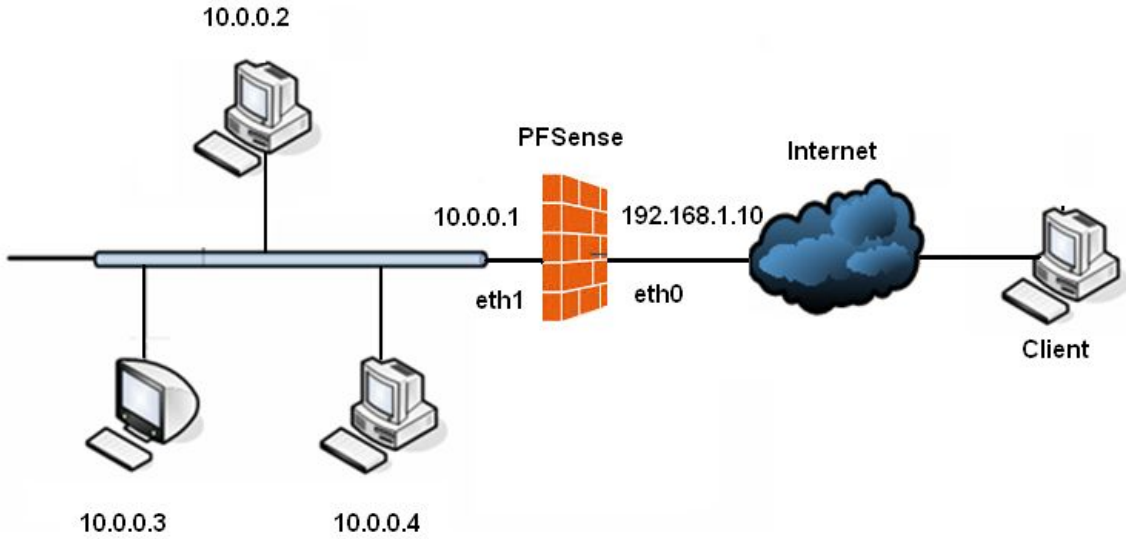
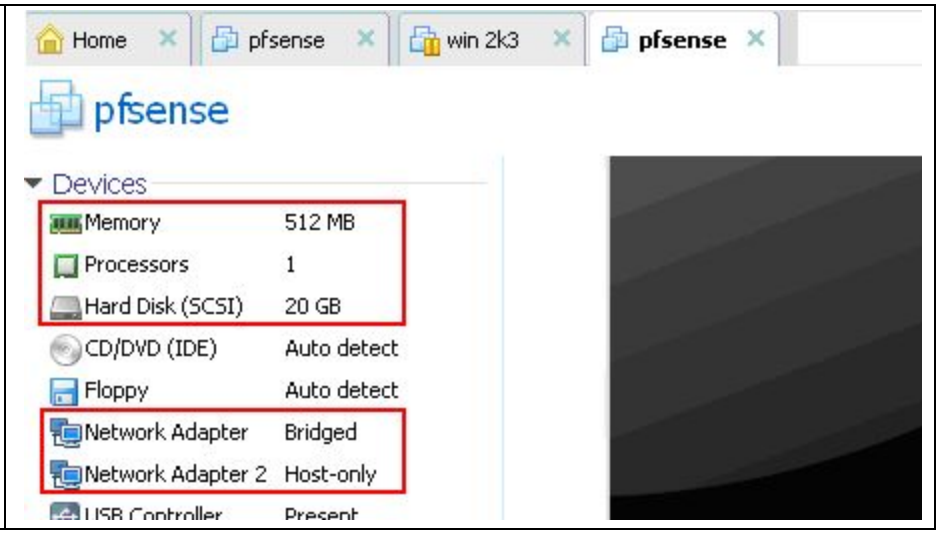
Đỗ Quang Ngọc

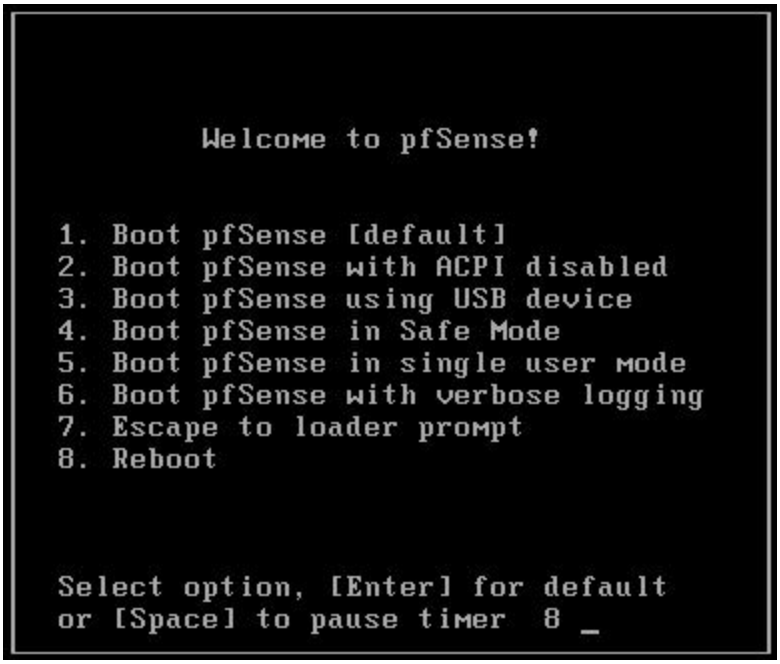
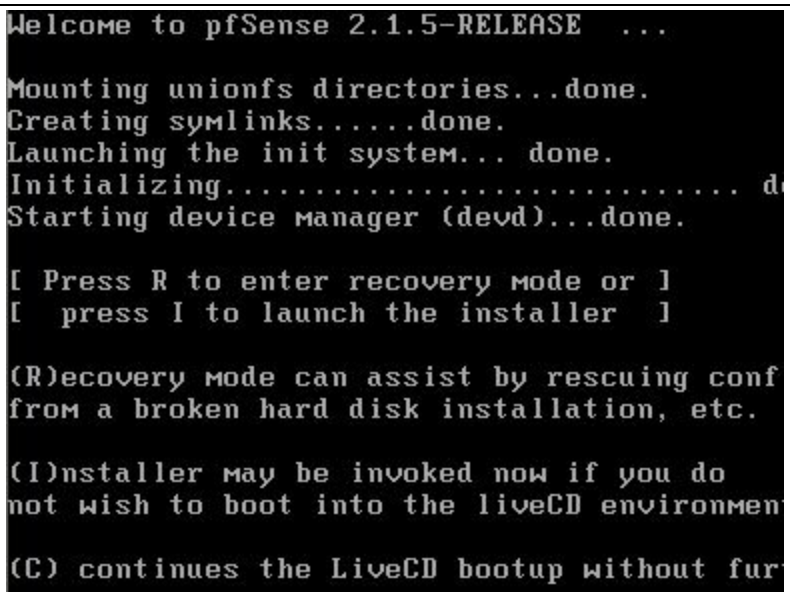
Cài đặt Pfsense

Mô hình mạng

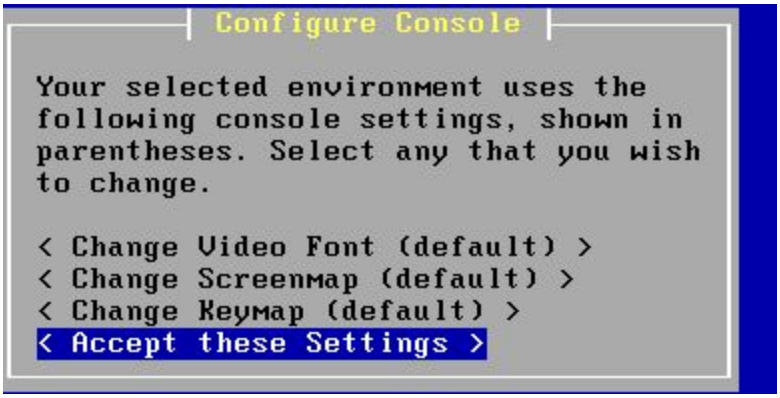


1. Cài máy PFsense

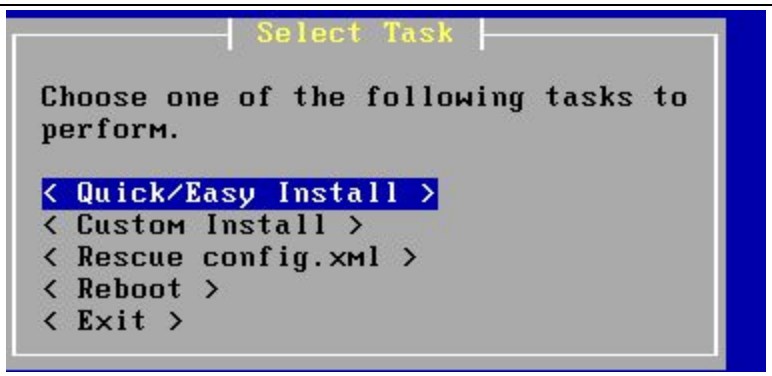
B1. Trên VMWare, Tạo máy ảo có cấu hình như sau	

B2. Nhấn Enter	
B3. Nhấn I để cài đặt (press I to launch the installer)	

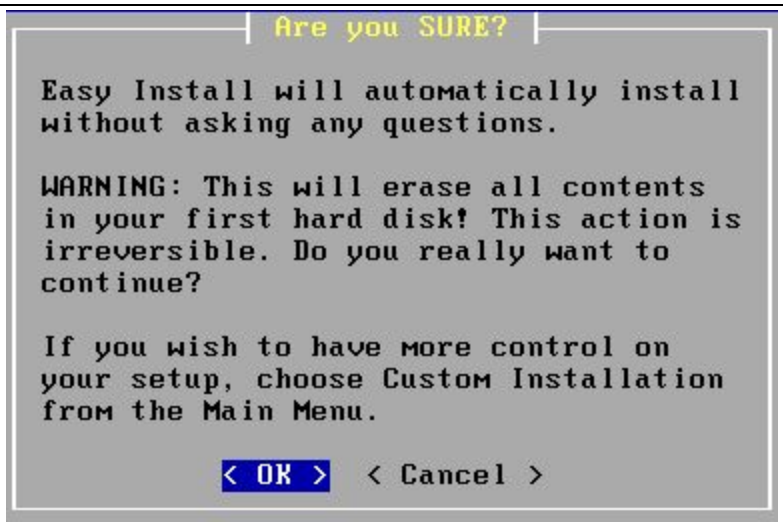
B4. Chọn **Accept these settings** ,chấp nhận các tham.



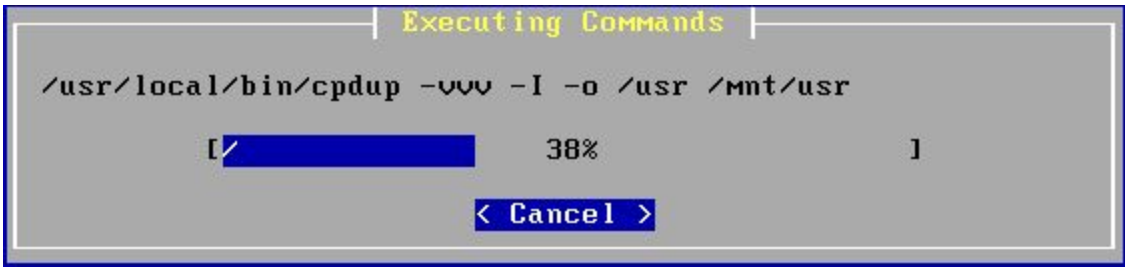
B5. Chọn Quick/Easy Install



B6. Nhấn OK để bắt đầu cài đặt



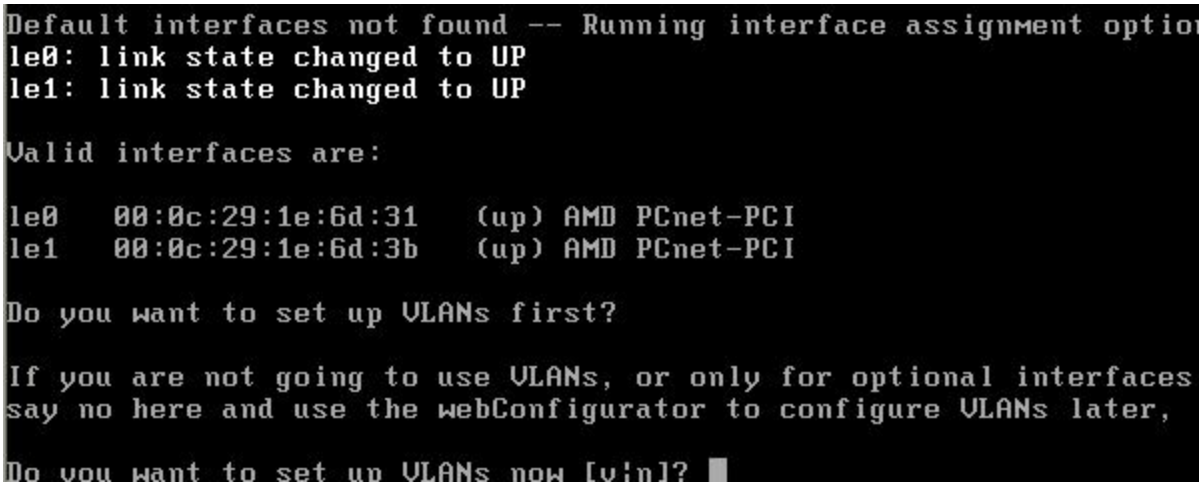
Quá trình cài đặt bắt đầu



B7. Chọn Standard Kernel

B8. Chọn Reboot để khởi động máy

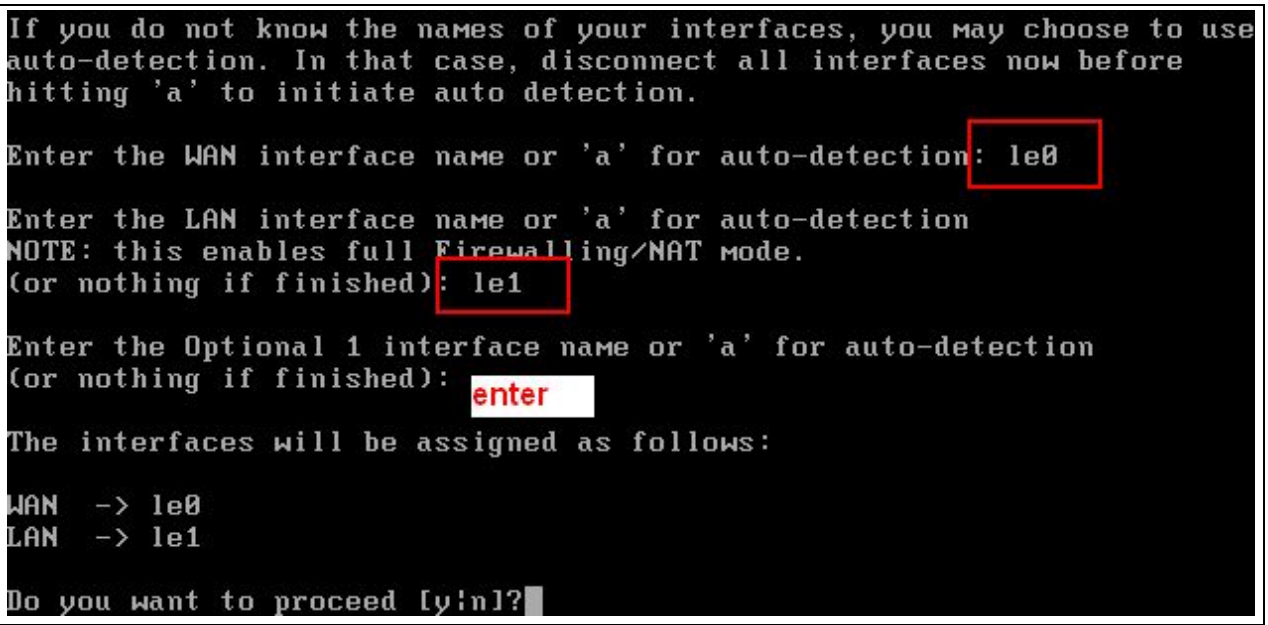
B9. Chọn N, không cấu hình VLAN



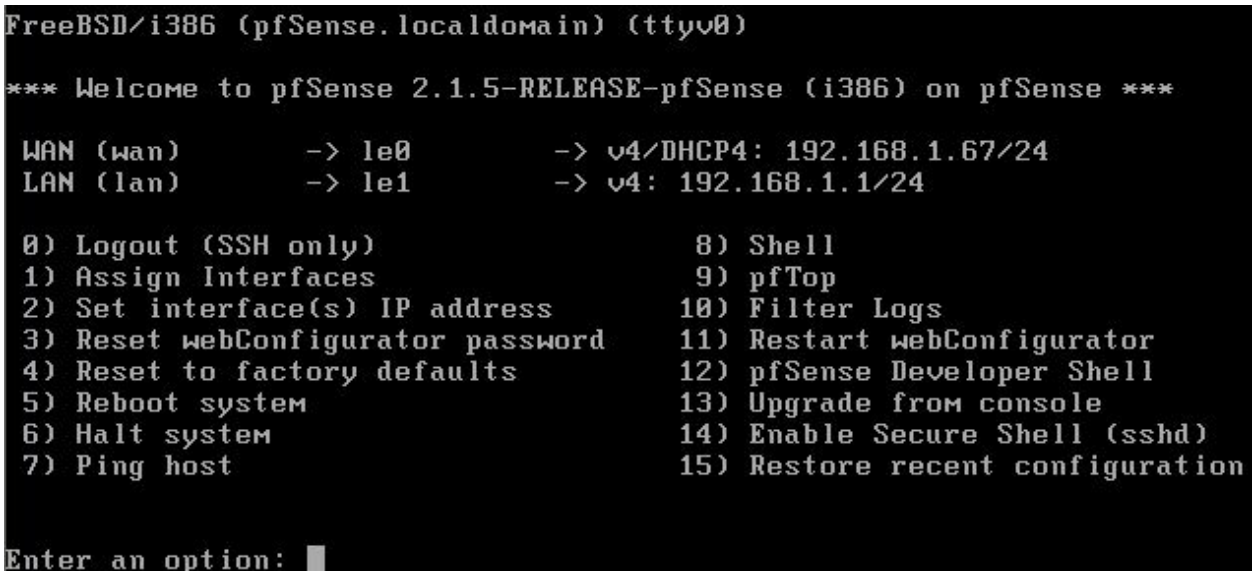
B10. Nhập tên Lan card:

kết nối WAN, nhập le0,

kết nối LAN, nhập le1. Nhấn Enter, chọn Y



B11. Chọn mục 2 để gán IP cho Lan card



B12. Chọn 1, Nhấn N.
- Nhập IP 192.168.1.10 cho WAN interface
- Nhập 24 cho độ dài Subnet
- Nhập IP 192.168.1.254, khai báo default gateway
- Chọn N, bỏ qua Ipv6 cho WAN interface

```
Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP?  [y|n]
> n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count:
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254
Configure IPv6 address WAN interface via DHCP6?  [y|n]
> n
```

B13. Chọn mục 2 để gán IP cho Lan card

```
FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on pfSense ***

 WAN (wan)       -> le0        -> v4: 192.168.1.10/24
 LAN (lan)       -> le1        ->

 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                         15) Restore recent configuration


Enter an option:
```

B14. Chọn 2,
- Nhập IP 10.0.0.1 cho LAN interface
- Nhập 24 cho độ dài Subnet
- Nhấn Enter

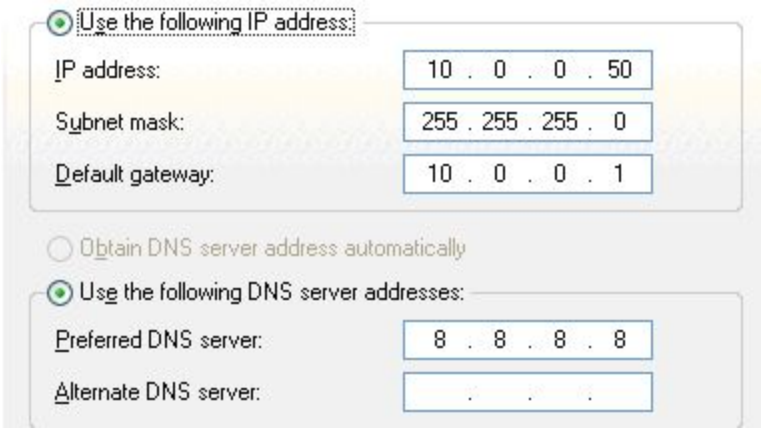
```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - static)
2 - LAN (le1)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count:
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> Enter
```

B15. Nhấn Enter, Chọn N, nhấn Enter để kết thúc

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> Enter

Enter the new LAN IPv6 address.  Press <ENTER> for none:
> Enter

Do you want to enable the DHCP server on LAN? [y|n]  n
Disabling DHCPD...Done!
Disabling DHCPD...Done!

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

The IPv4 LAN address has been set to 10.0.0.1/24
You can now access the webConfigurator by opening the following URL in
browser:
                http://10.0.0.1/

Press <ENTER> to continue.
```

2. Quản trị Pfsense

B1. Máy client trong mạng LAN, đặt IP như hình

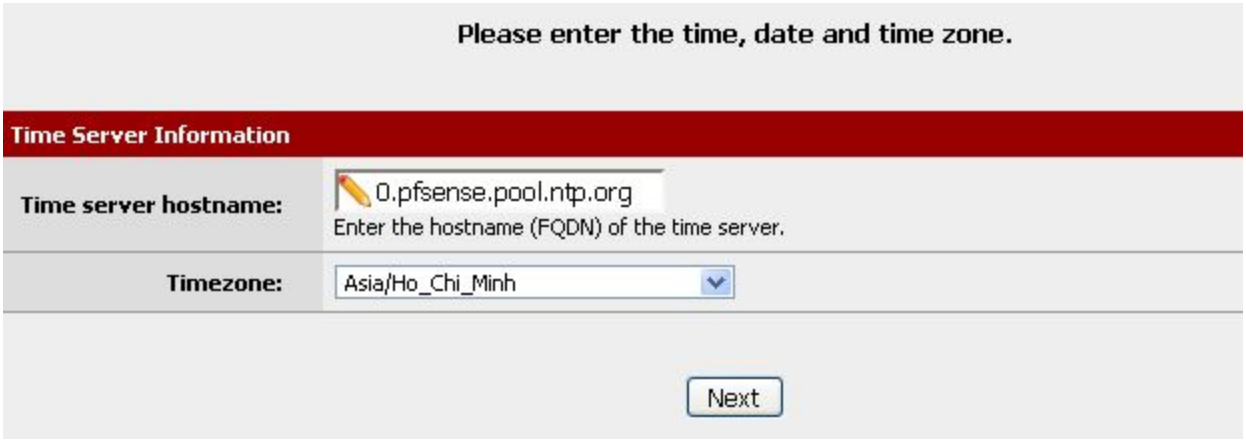


B2. Nhập username: admin
Password: pfsense

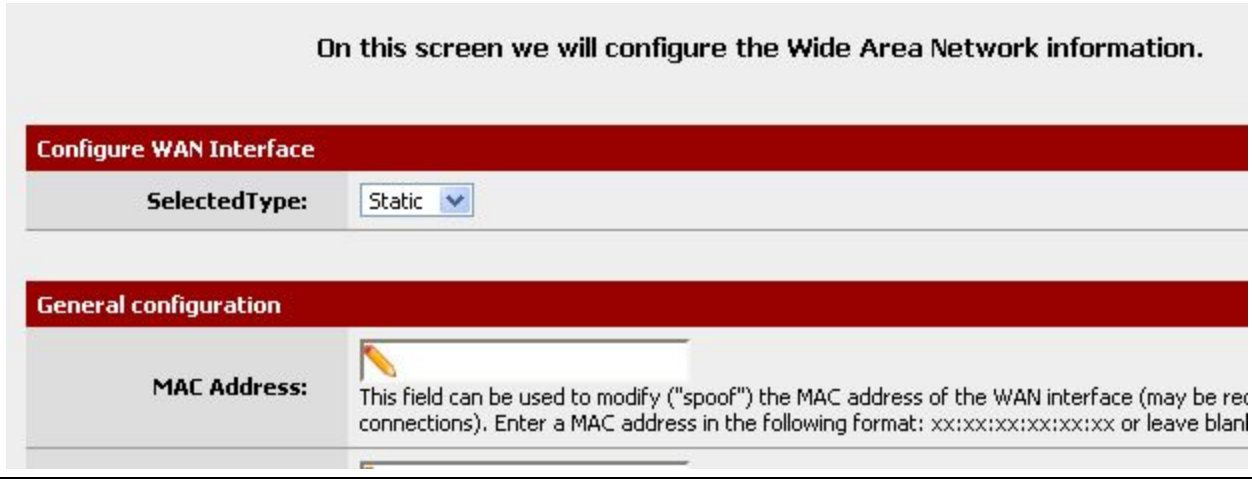
B3. Nhấn Next, Next

B4. Nhập tên máy, tên domain và DNS
Nhấn Next

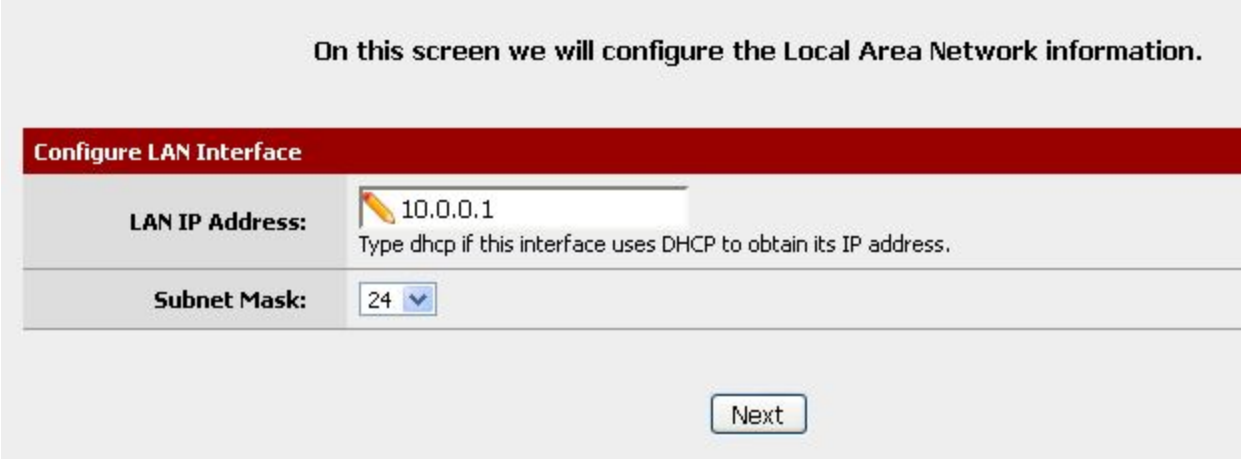
B5. Nhập Timezone, Nhấn Next



B6. Khai báo thông tin cho WAN interface, nhấn Next đẻ bỏ qua

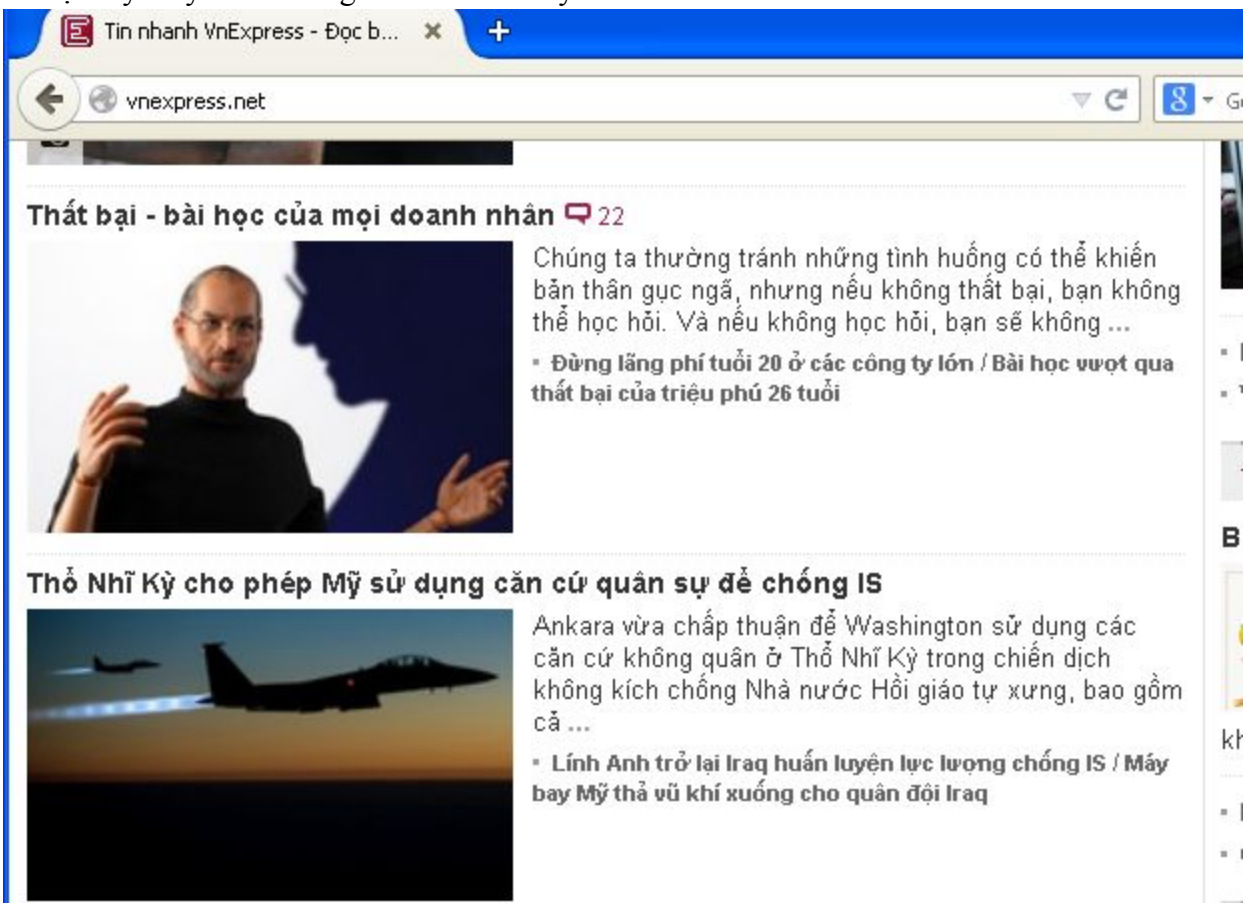


B7. Khai báo thông tin cho LAN interface, nhấn Next đẻ bỏ qua



B8. đổi password cho user admin, nhấn Reload

B9. tại đây máy client trong LAN có thể truy xuất Internet theo cơ chế NAT



Proxy server

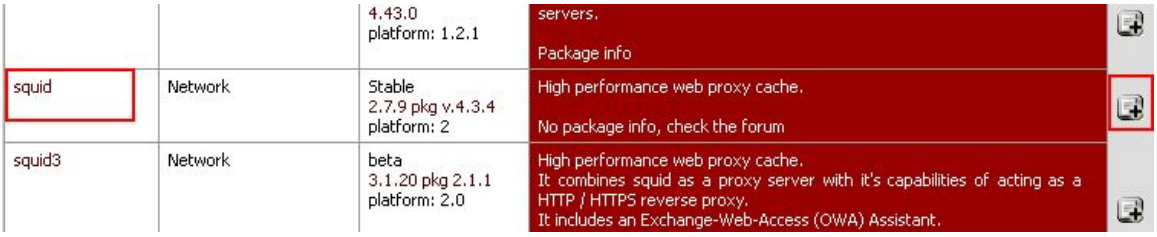
Quản lý, giám sát truy cập internet

1. Chuẩn bị

Cài các gói cần thiết

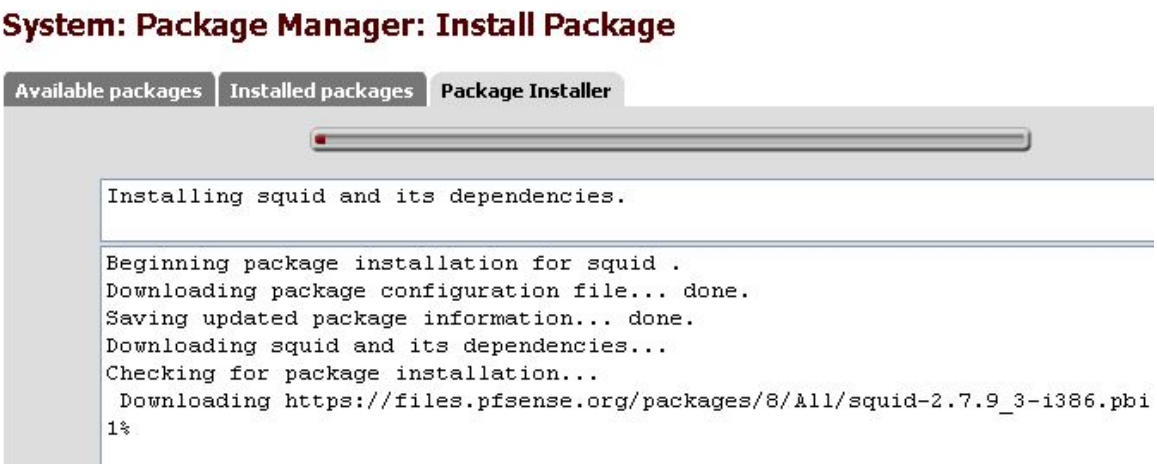
1.1 cài gói squid

System, Packages, chọn squid, nhấn dấu +

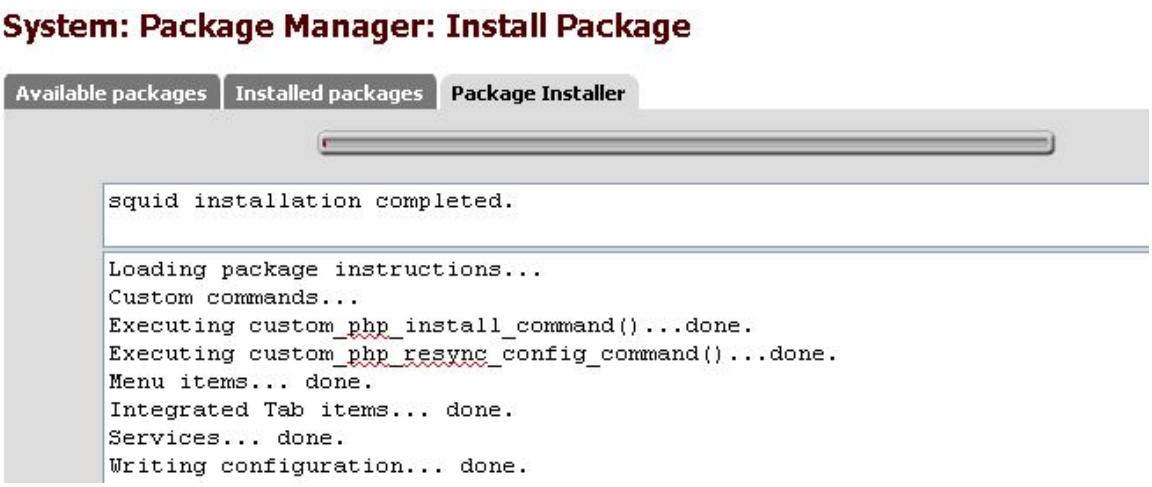


Chọn Confirm

Quá trình cài bắt đầu



Quá trình cài kết thúc

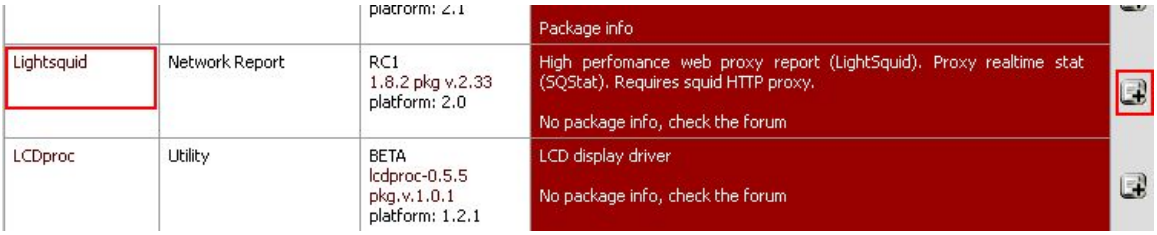


1.2 cài gói squidGuard

System, Packages, chọn squidGuard, nhấn dấu +

1.3 cài gói Lightsquid

System, Packages, chọn Lightsquid, nhấn dấu +



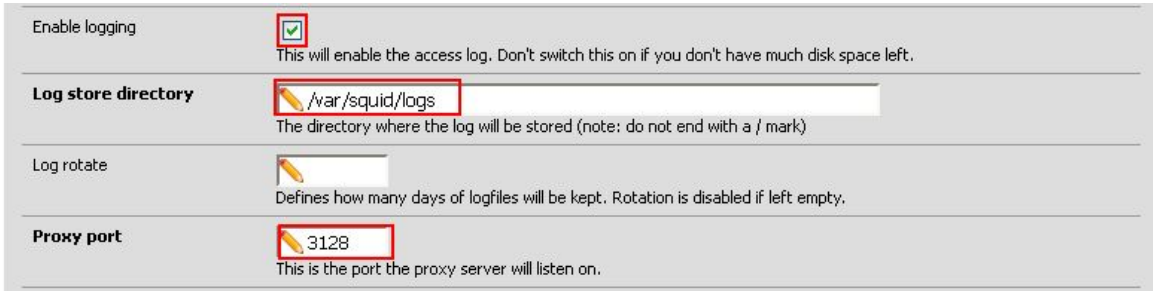
2. Cấu hình Proxy server:

2.1. Cấu hình chung

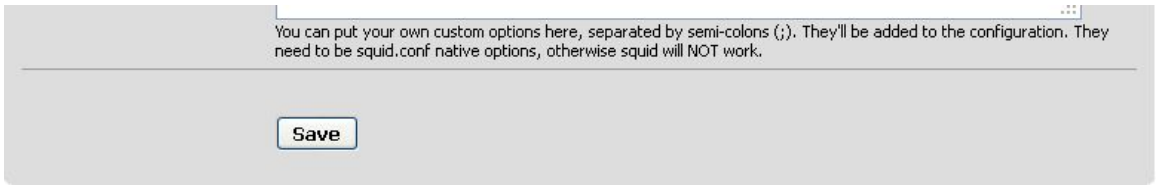
Service, chọn Proxy server, General

Proxy interface: chọn LAN
Allow users on interface: check
Transparent proxy: check

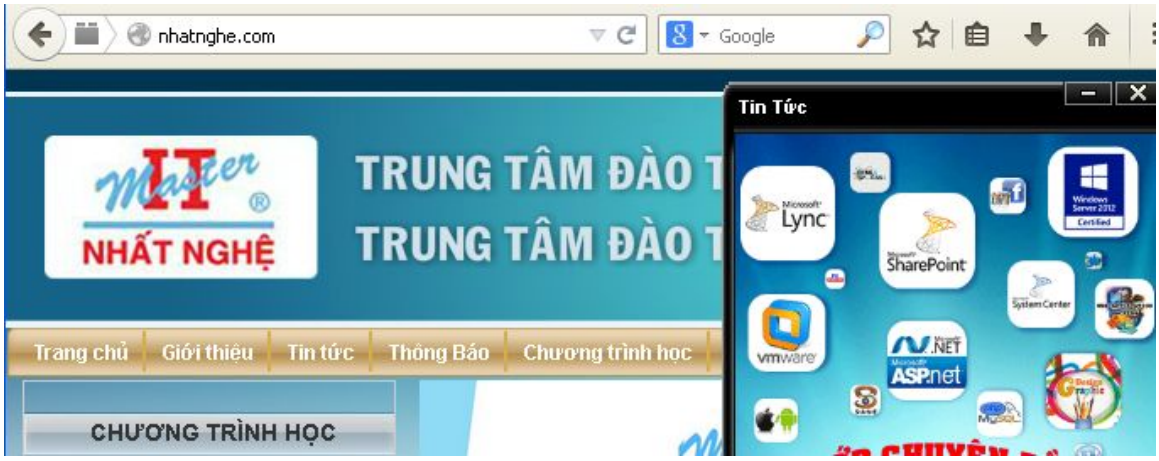
Enable logging: check
Log store directory: /var/squid/logs



Chọn **Save**



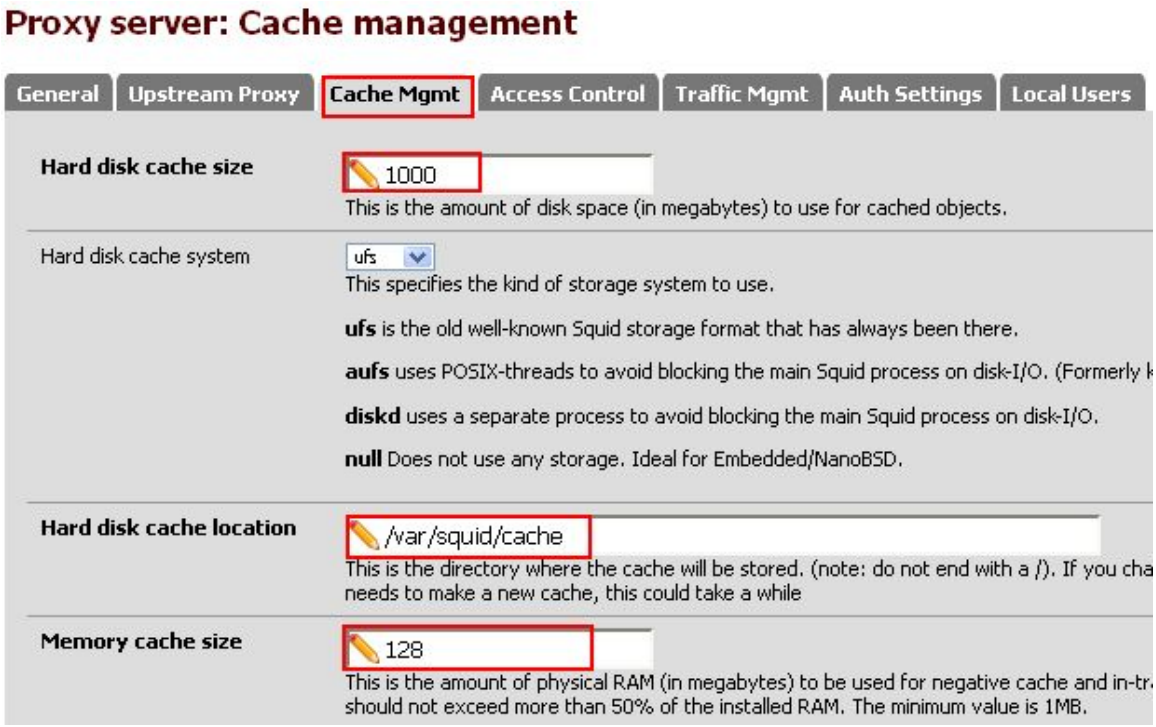
Tại máy client có thể truy cập Internet (không cần phải cấu hình proxy tại client)



2.2. Cấu hình Cache - Tăng tốc độ truy cập web

Service, chọn Proxy server, Cache mgmt

Hard disk cache size: dung lượng ổ cứng làm cache
Hard disk cache location: vị trí cache lưu trữ trên ổ cứng
Memory cache size: dung lượng RAM lách cache



Chọn save

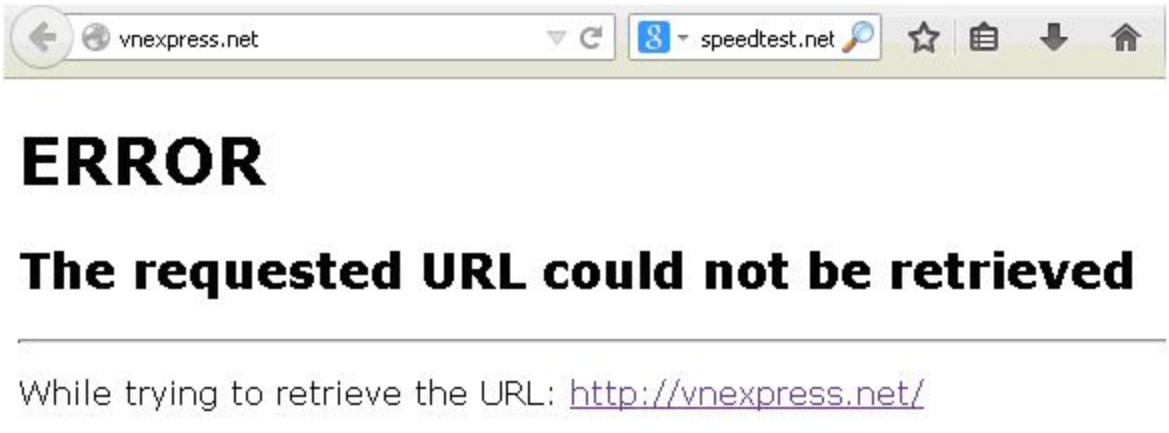
3. Giới hạn truy cập

Service, chọn Proxy server, Access control

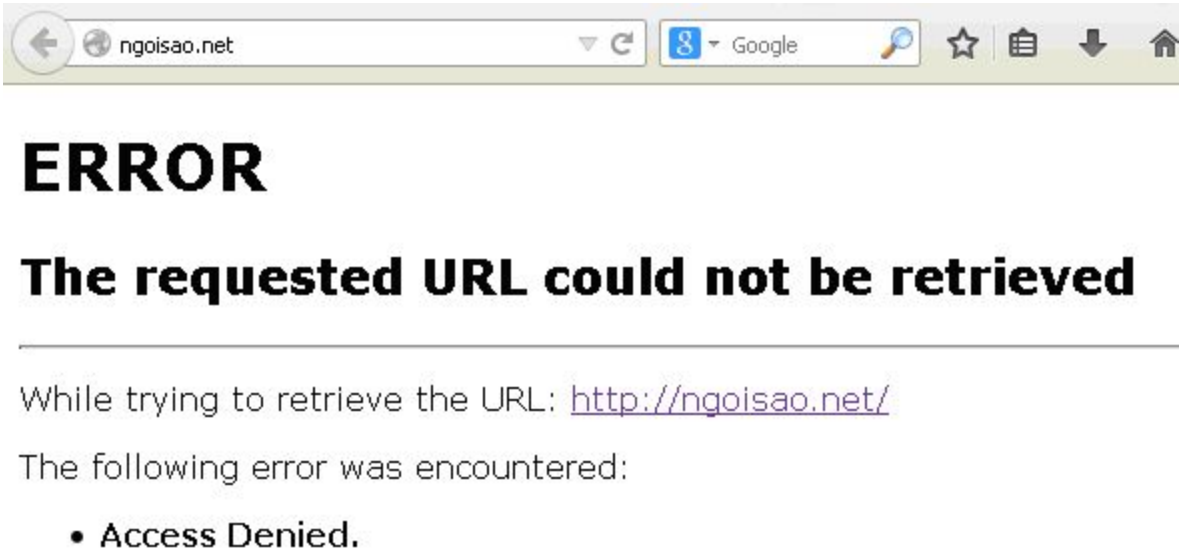
Banned host addresses: Nhập danh sach địa chỉ IP cấm truy cập
Blacklist : Danh sach web site cấm truy cập

Chọn **Save**

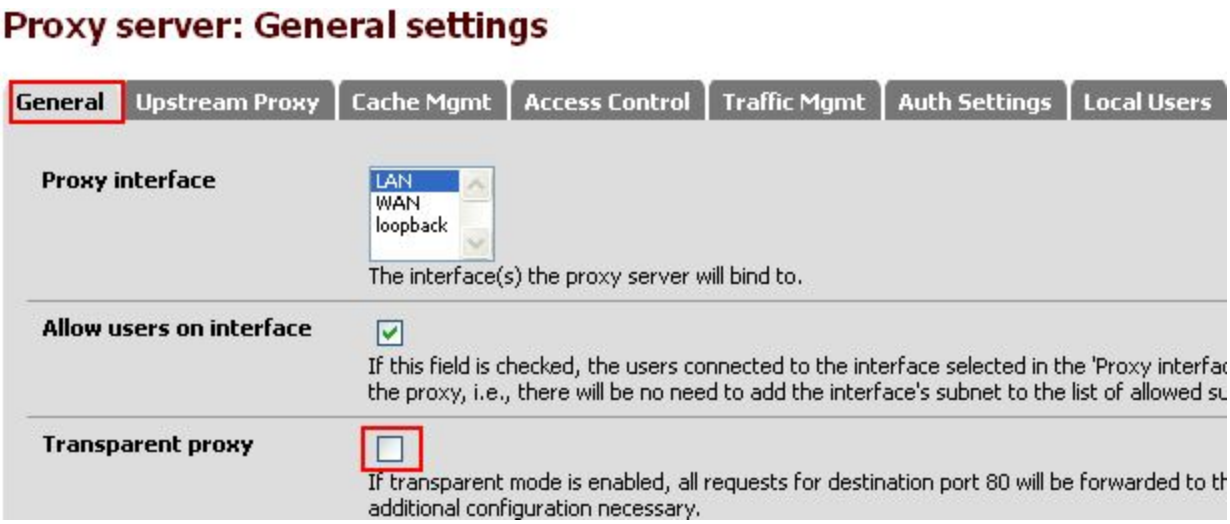
Tại máy 10.0.0.50 truy cập web sẽ báo lỗi



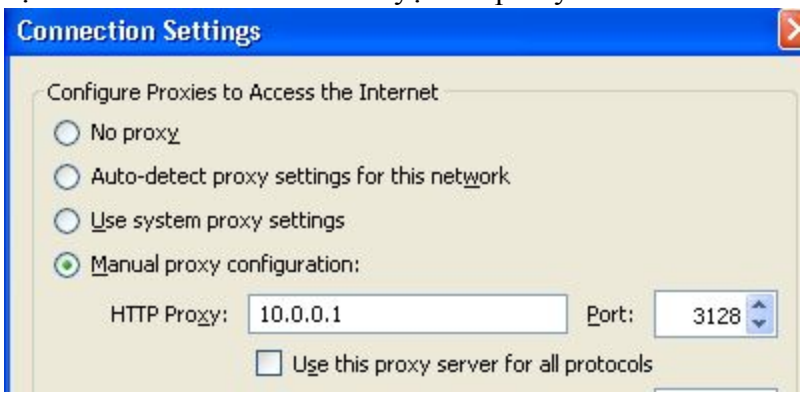
Tại máy 10.0.0.51 truy cập ngoisao.net sẽ báo lỗi



4. Chứng thực user truy cập web
Service, chọn Proxy server, General
Transparent proxy: bỏ check
Chọn **Save**



Tại client cấu hình chỉ trình duyệt đến proxy server

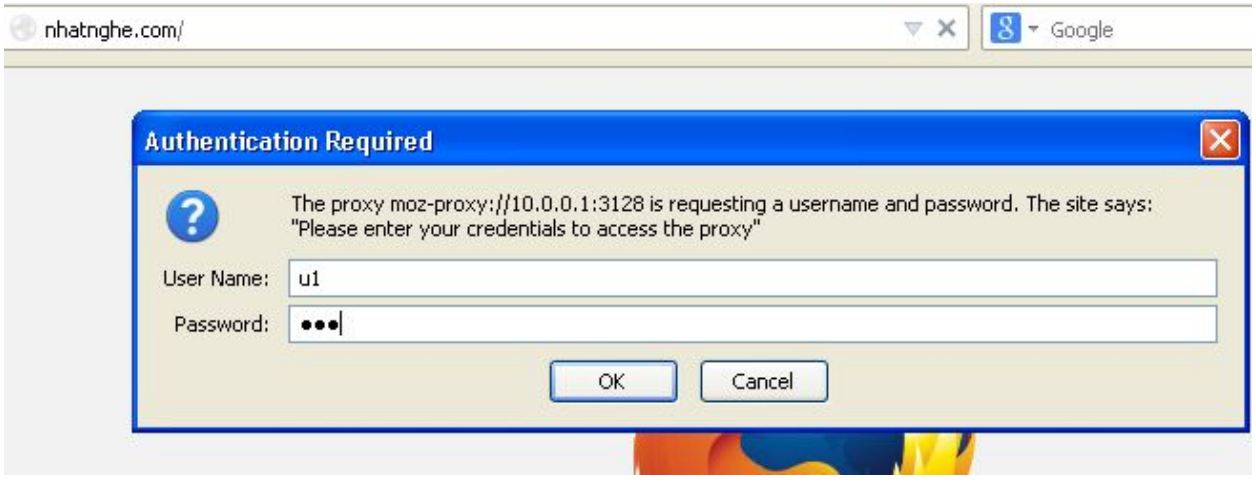


4.1 Chứng thực Local user
B1. Service, chọn Proxy server, Local user
Add user

User name: u1
Password: 123
Chọn **Save**

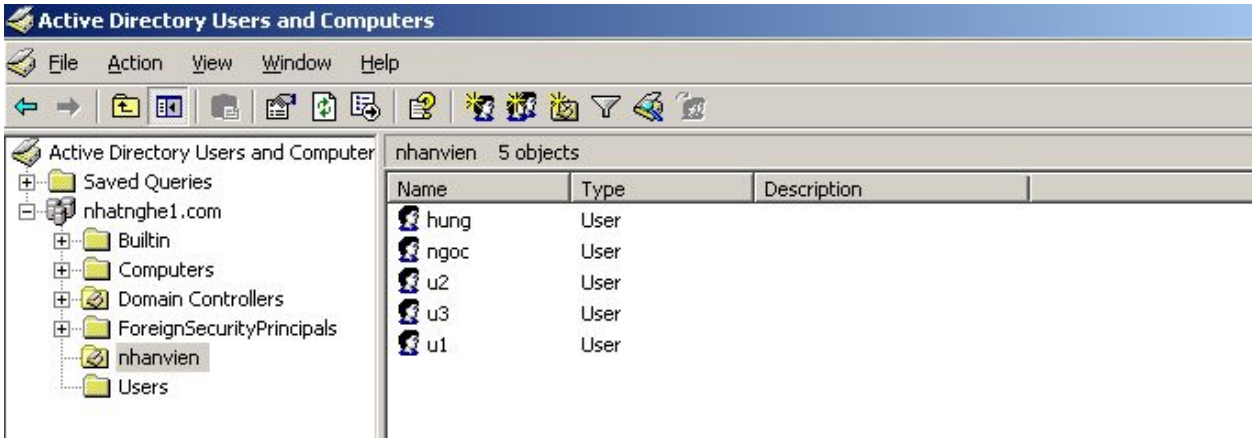
B2. **Service, chọn Proxy server, Auth Settings**
Authentication method: chọn **Local**
Chọn **Save**

B3**.** Máy client truy cập web phải nhập username và password



4.2 Chứng thực DC user

B1. Tại máy DC 10.0.0.150 tạo các user u1, u2, u3



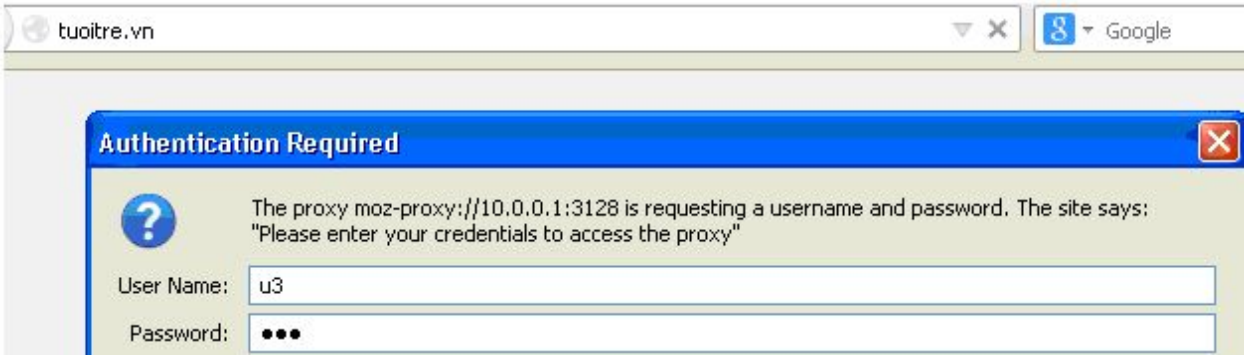
B2. **Service**, chọn **Proxy server**, **Auth Settings**

Nhập các thông tin:

Authentication method:	LAP
LDAP version:	3
Authentication server:	10.0.0.150
Authentication server port:	389
LDAP server user DN:	cn=u1,ou=nhanvien,dc=nhatnghe1,dc=com
LDAP password:	123
LDAP base domain:	dc=nhatnghe1,dc=com
LDAP username DN attribute:	uid
LDAP search filter:	sAMAccountName=%s

Chọn **Save**

B3. Máy client truy cập web nhập username u3, password: 123



Truy cập thành công

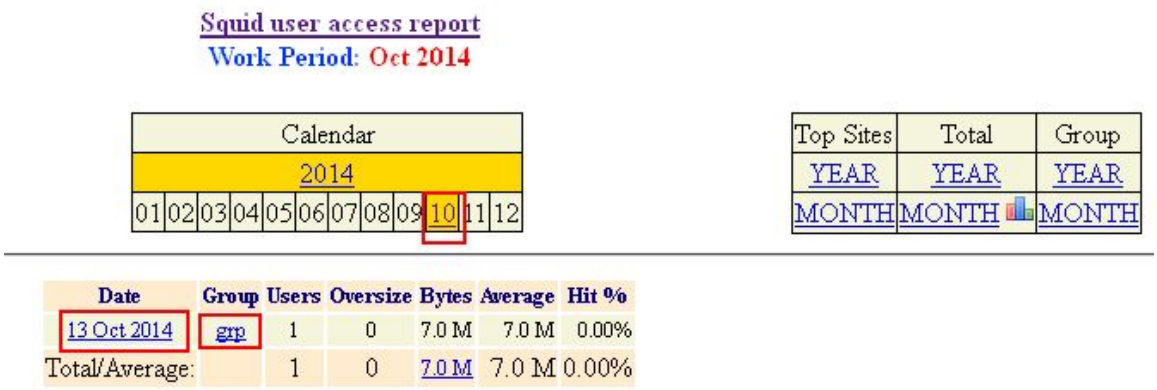
5. Thống kê truy cập

5.1 Cấu hình chung
Status, Proxy reports, settings

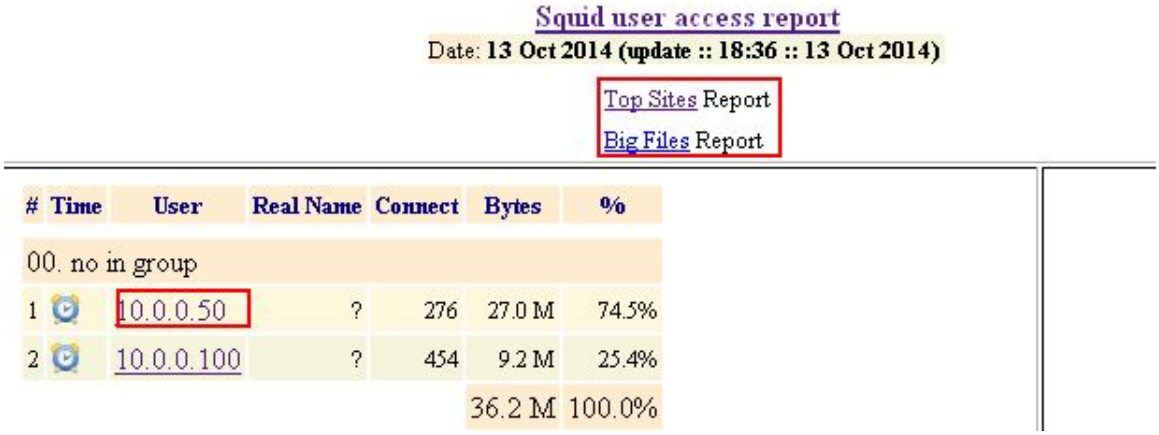
Language: chọn English
Refresh sheduler: chọn 10min
Nhấn: Refresh
Chọn **Save**

5.2 Xem báo cáo truy cập

Status, Proxy reports, Lightsquid Report
Chọn tháng, ngày, Group cần xem báo cáo



Thống kế theo **User** hoặc **Top sites**, **Big files**



Thống kê theo User

Squid user access report

User: 10.0.0.50 (?)
Group: ?
Date: **13 Oct 2014**

Total **7.0 M**

#	Accessed site	Connect	Bytes	Cumulative	%
1	c0.f21.img.vnecdn.net	29	5.6 M	5.6 M	80.1%
2	st.polyad.net	12	495 564	6.1 M	6.7%
3	st.eclick.vn	22	432 016	6.5 M	5.9%
4	c0.f23.img.vnecdn.net	6	248 524	6.7 M	3.4%
5	c0.f24.img.vnecdn.net	3	102 640	6.8 M	1.4%
6	ngoisao.net	3	57 966	6.9 M	0.7%
7	c0.f22.img.vnecdn.net	1	26 982	6.9 M	0.3%

6. Squid Guard

Lọc web nâng cao

SquidGuard can be used to

- limit the web access for some users to a list of accepted/well known web servers and/or URLs only.
- block access to some listed or blacklisted web servers and/or URLs for some users.
- block access to URLs matching a list of regular expressions or words for some users.
- enforce the use of domainnames/prohibit the use of IP address in URLs.
- redirect blocked URLs to an info page.
- redirect banners to an empty GIF.
- have different access rules based on time of day, day of the week, date etc.

Service, Proxy filter, General Setting

Check **Enable**, chọn **apply**

Chọn Common ACL, nhắp **click here**

Default access [all]: chọn allow

chọn: Save

Các máy client truy cập web bình thường

6.1 Blacklist

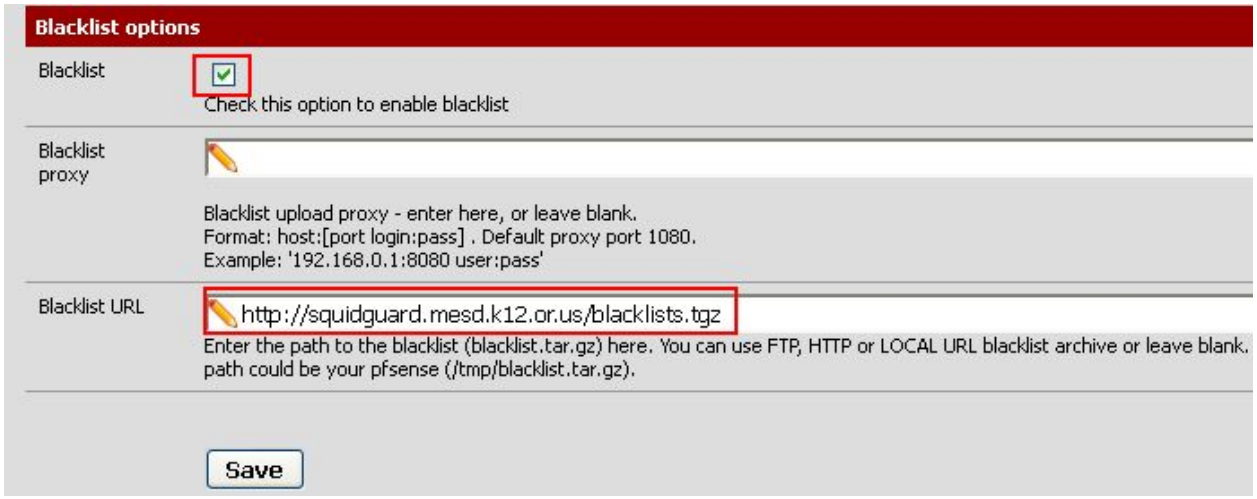
Service, Proxy filter, General Setting

Blacklist URL:

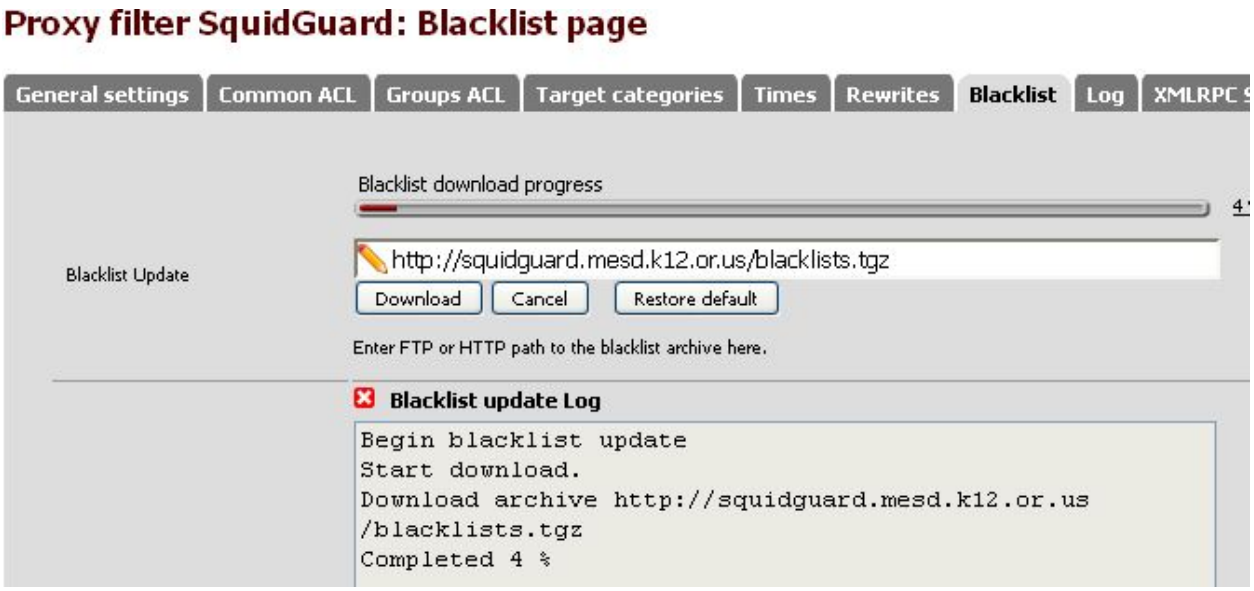
Nhập http://squidguard.mesd.k12.or.us/blacklists.tgz

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

Chọn **Save**



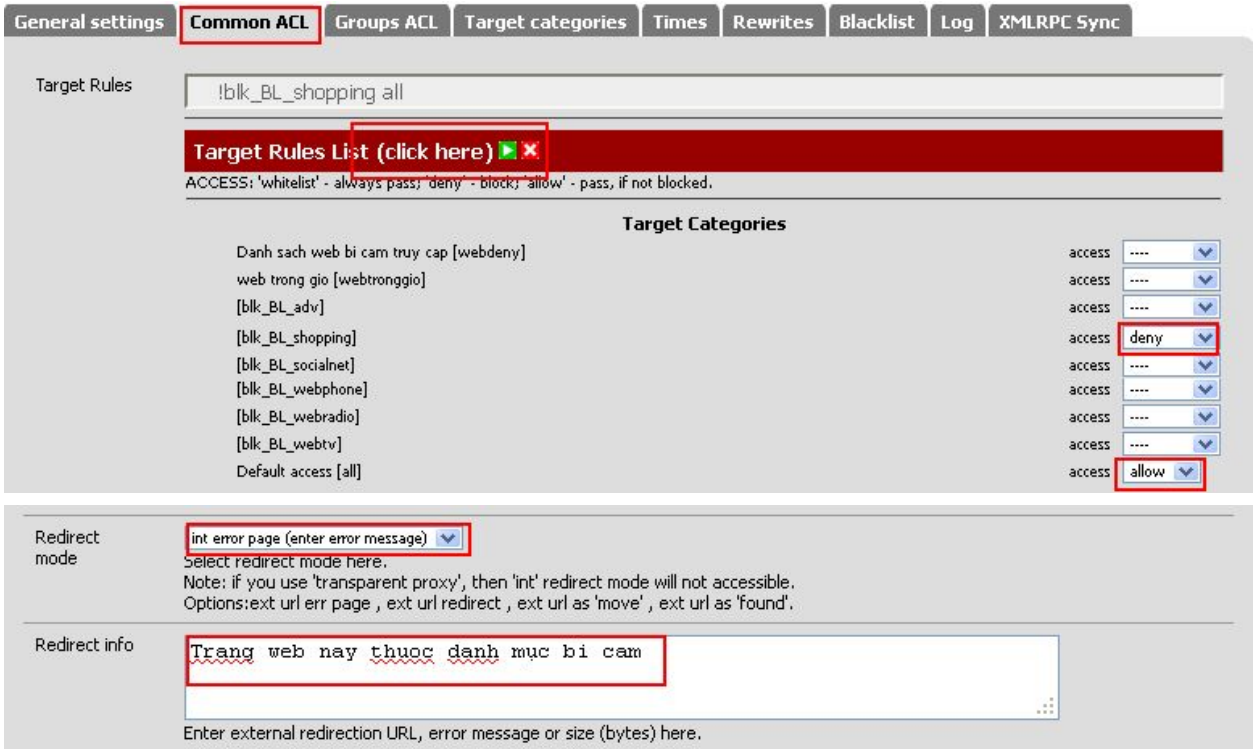
Chọn thẻ **Blacklist,** nhấn **download**



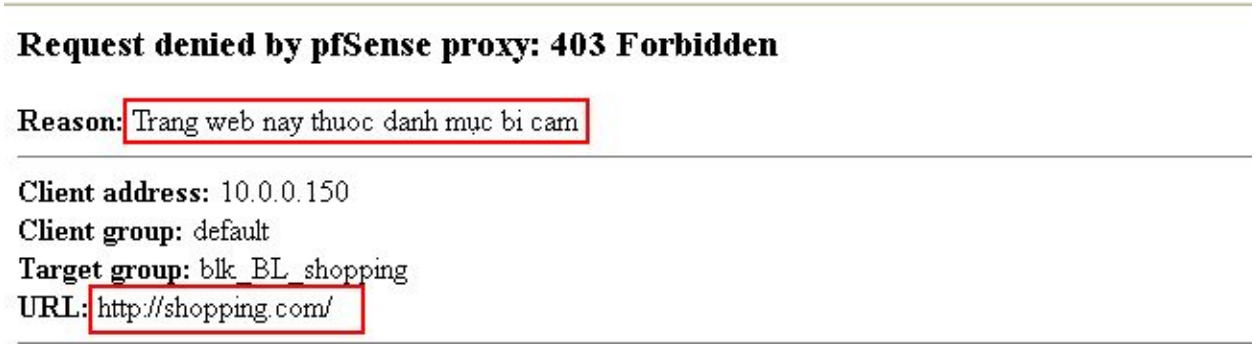
Khi download kết thúc, chọn **Common ACL**

[blk_BL_shopping]	Chọn Deny
Default access [all]	Chọn Allow

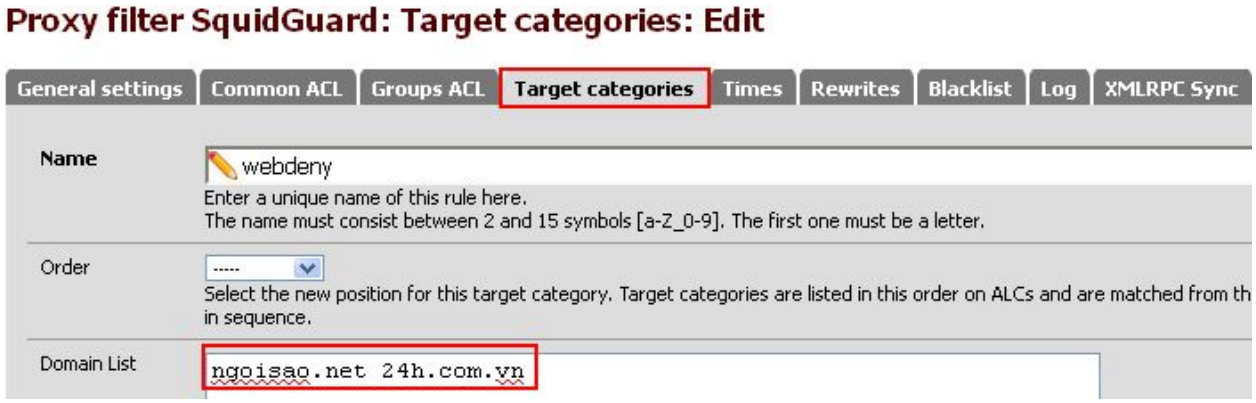
Redirect mode: int error page
Redirect info: Nhập thông báo lỗi



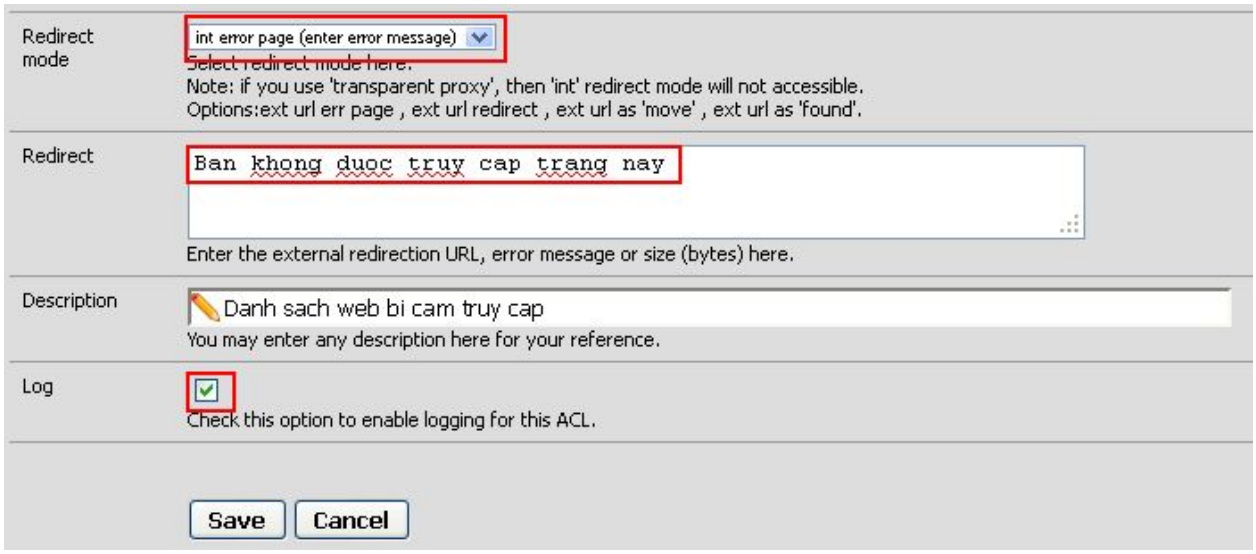
Chọn **Save**, **Apply**
Tại máy client truy cập trang shopping.com



6.2 Cấu truy cập web
Tất cả các PC trong LAN không được truy cập:
ngoisao.net
24h.com.vn
Service, Proxy filter, General Setting, Target categories
Name: nhập webdeny
Domain List: ngoisao.net 24h.com.vn



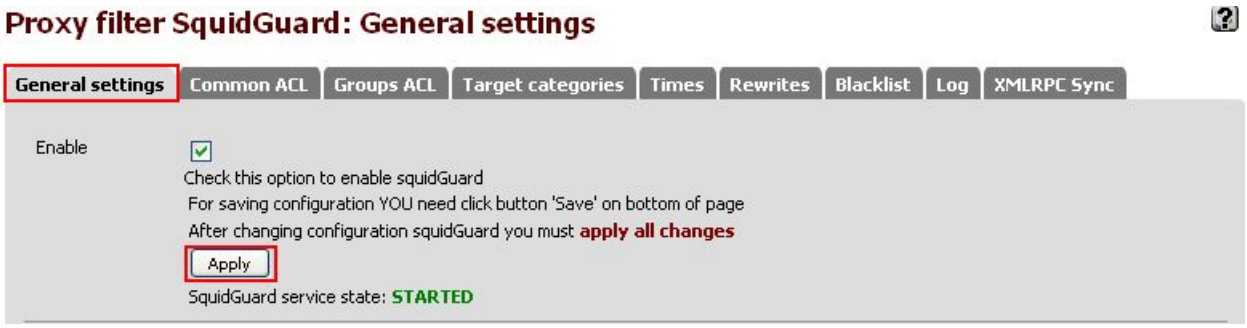
Redirect mode: int error page(enter error message)
Nếu chọn "ext err page(enter URL)" sẽ chuyển hướng đến web site khác Redirect: http://nhatnghe.com
Redirect: "Ban khong duoc truy cap trang nay"
Chọn **Save**



Chọn **Common ACL**

Danh sach web bi cam truy cap [webdeny] chọn **deny**

Chọn **General settings**, **Apply**



Mở trình duyệt , truy cập trang ngoisao.net sẽ báo lỗi

Chú ý: xóa cache trình duyệt nếu cần

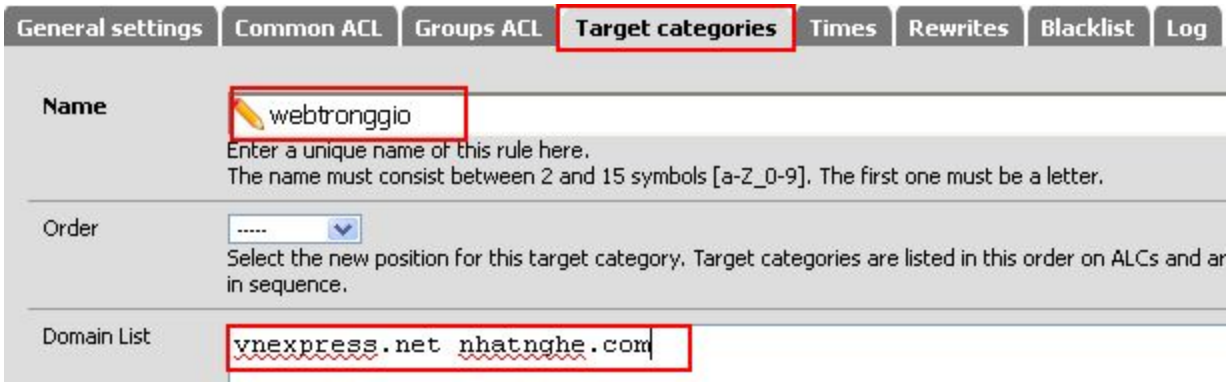
6.2 Giới hạn giờ truy cập web
Chú ý: deny tất cả các rule trong common ACL

Rule1.Các pc 10.0.0.10-10.0.0.100
Trong giờ làm việc
Chỉ được truy cập trang web: vnexpress.net nhatnghe.com
Ngoài giờ truy cập không giới hạn

Rule 2: Các pc 10.0.0.101-10.0.0.254 truy cập web không giới hạn ở bất kỳ thời đểm nào

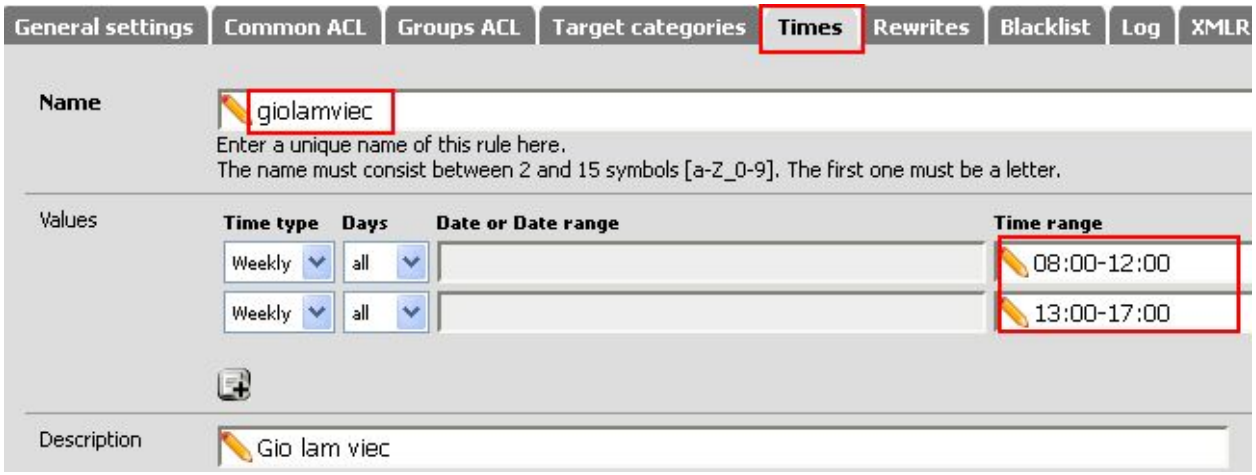
B1**. Service, Proxy filter, General Setting, Target categories**
Nhấn + tạo rule mới

Name: nhập webtronggio
Domain List: nhập vnexpress.net nhatnghe.com
Chọn **Save**



B2**. Service, Proxy filter, General Setting, Times**
Name: giolamviec

Values: weekly 08:00-12:00
weekly 13:00-17:00
Description: Gio lam viec
Chọn **Save**

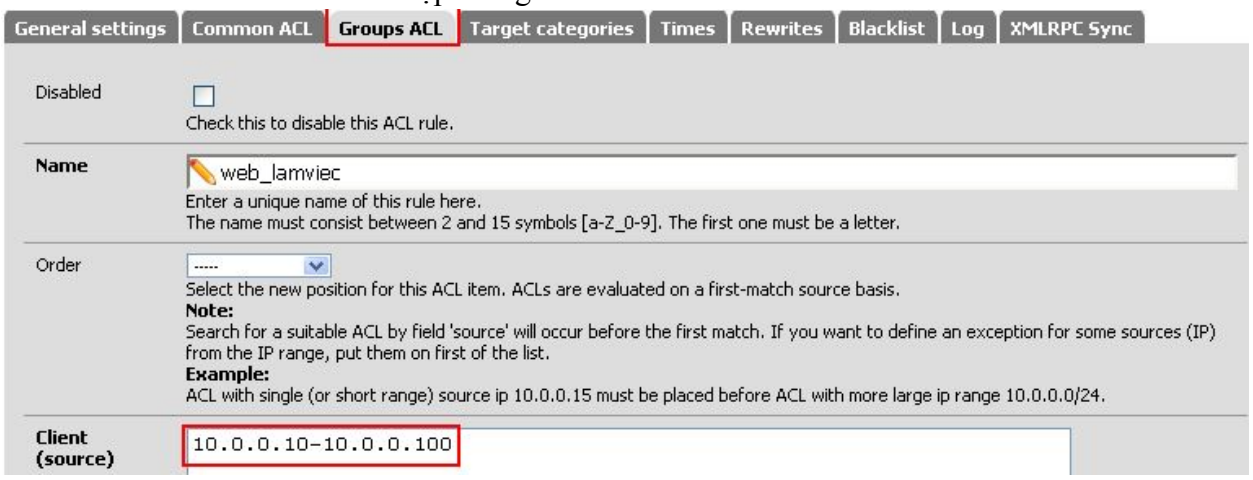


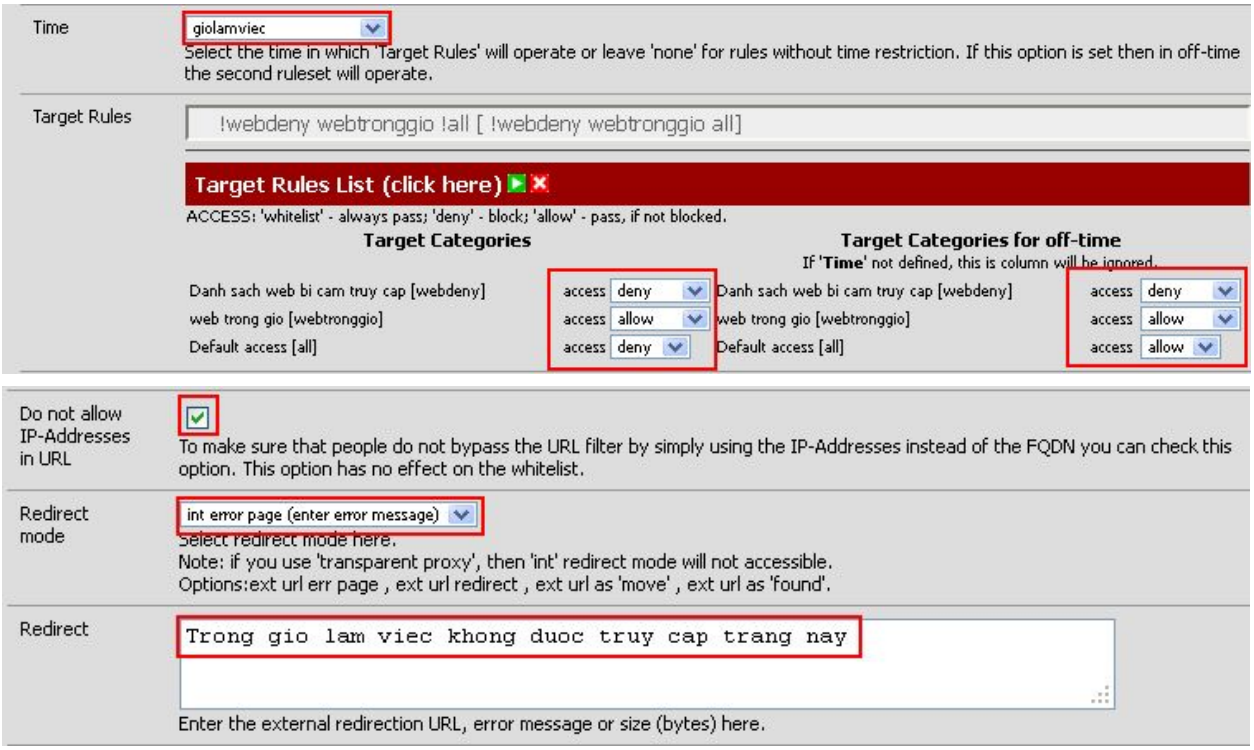
B.3 **Service, Proxy filter, General Setting, Groups ACL**

Name: web_lamviec
Client (source) 10.0.0.10-10.0.0.100
Time giolamviec
Target Rules chọn

Danh sach web bi cam truy cap [webdeny]	deny	deny
web trong gio [webtronggio	allow	allow
Default access [all]	deny	deny

Redirect Nhập thông báo lỗi

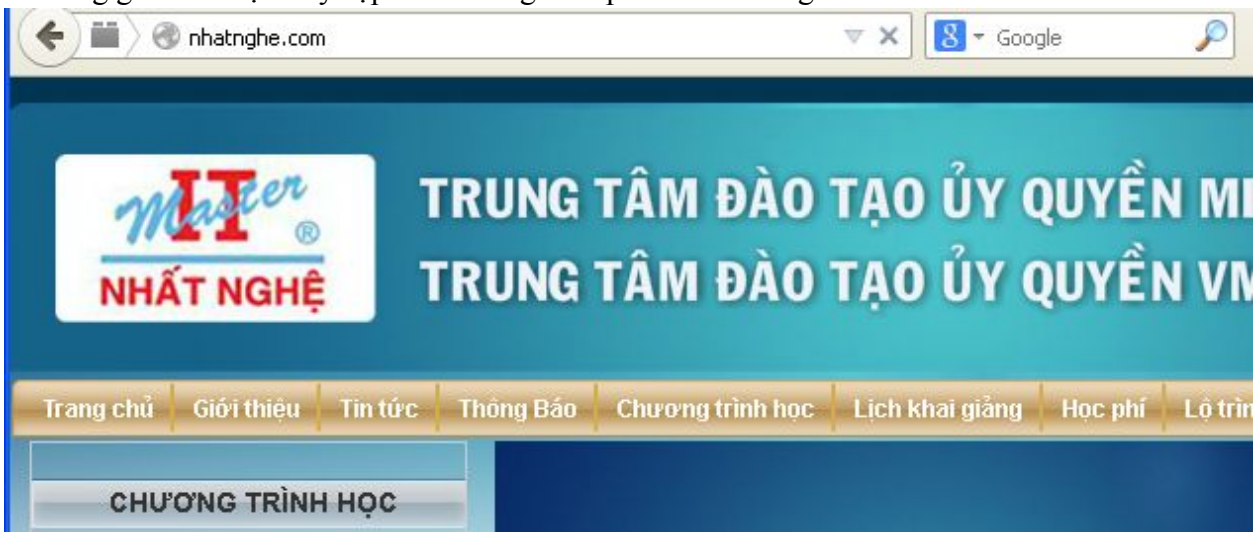




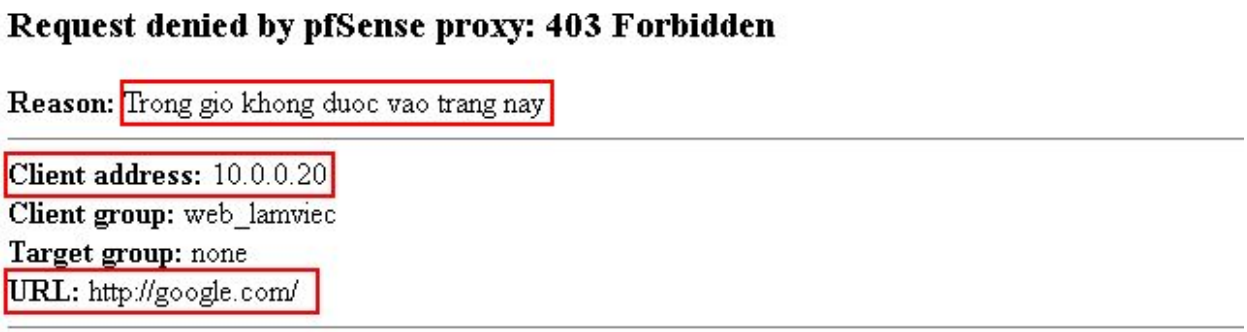
Chọn **Save**

B4. Kiểm tra

a. Trong giờ làm việc truy cập thành công vnexpress.net nhatnghe.com



b. Trong giờ làm việc truy cập không được google.com và các trang khác.



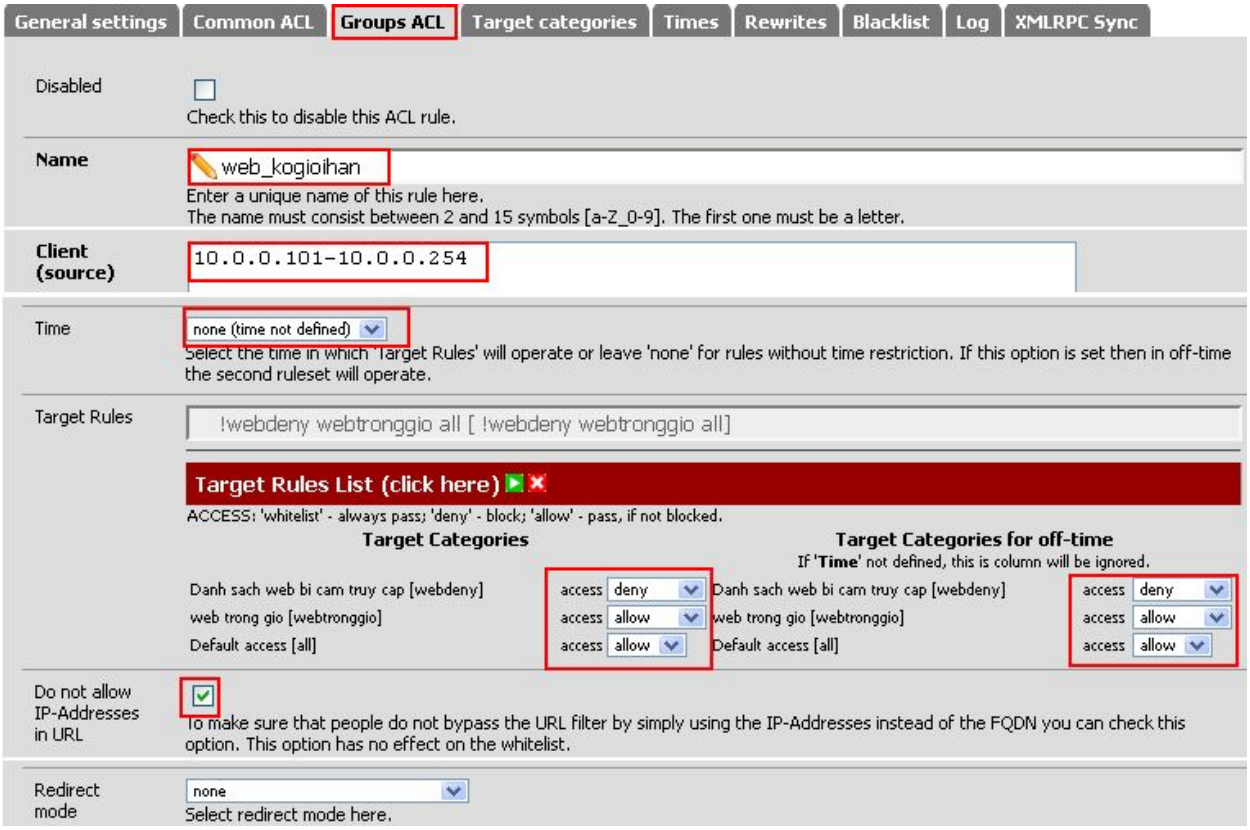
c. Ngoài giờ làm việc, truy cập bất cứ trang web nào

d. Máy client không thuộc dải IP 10.0.0.10-10.0.0.100 cũng không truy cập web do chưa được phép

B5. Các pc 10.0.0.101-10.0.0.254 truy cập web không giới hạn ở bất kỳ thời đểm nào

Service, Proxy filter, General Setting, Groups ACL
Nhấn + tạo rule mới
Name: web_kogioihan

Client (source)	10.0.0.101-10.0.0.254		
Time	none		
Target Rules	chọn		
	Danh sach web bi cam truy cap [webdeny]	deny	deny
	web trong gio [webtronggio	allow	allow
	Default access [all]	allow	allow
Redirect	none		

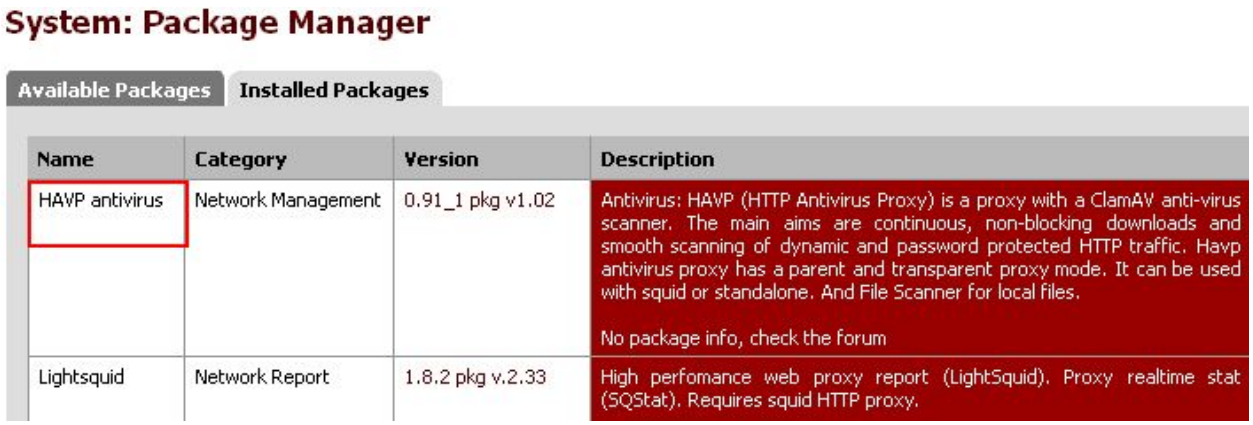


Chọn **Save**

Kết quả có 2 rule được tạo

Kiểm tra: tại pc có ip thuộc dải 10.0.0.101-10.0.0.254 truy cập web thành công ở bất kỳ thời gian nào

7. *HAVP* (HTTP Antivirus Proxy)
System, Packages, cài gói *HAVP* Antivirus



Scheme: {internet}->[HAVP]->[Squid cache]->{clients}

Setup

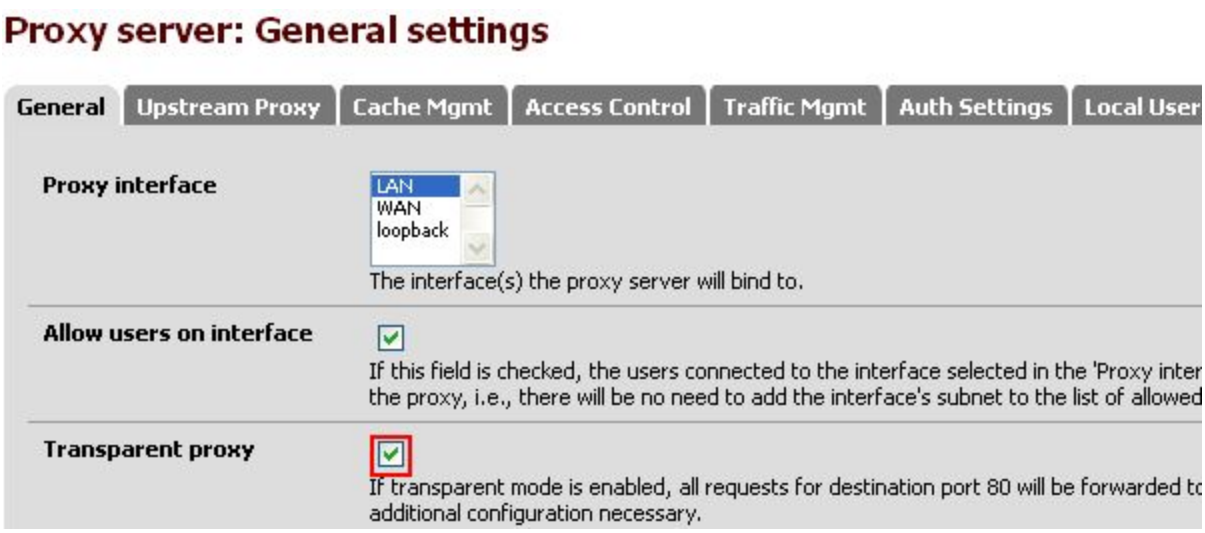
Squid:

- Disable upstream proxy (also will auto-disabled by HAVP)

HAVP:

- Select *Proxy mode* field as *Parent for Squid* and Save
- Scan Squid cache with *Antivirus: File scanner* for removing cached viruses.
- If you are planning to use Transparent Proxy mode: Squid transparent on

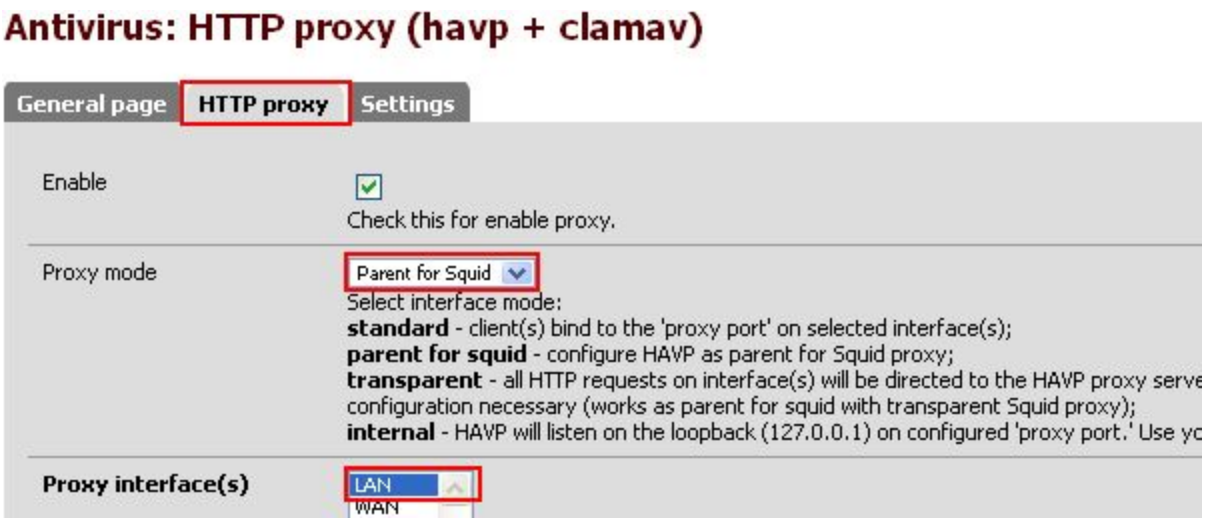
B1. Kiểm tra Proxy server đamh ở chế độ *Transparent proxy*

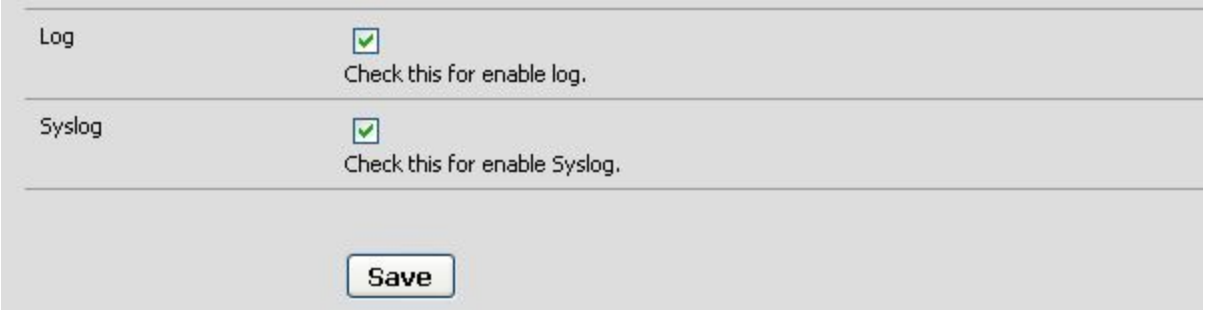


B2. Cấu hình **HTTP proxy**

Service, Antivirus, chọn **HTTP proxy**

Enable	check
Proxy mode	**parent for squid** ;HAVP đứng trước Squid proxy)
	(Chọn **transparent nếu** HAVP đứng sau Squid proxy)
Proxy interface(s)	chọn Lan



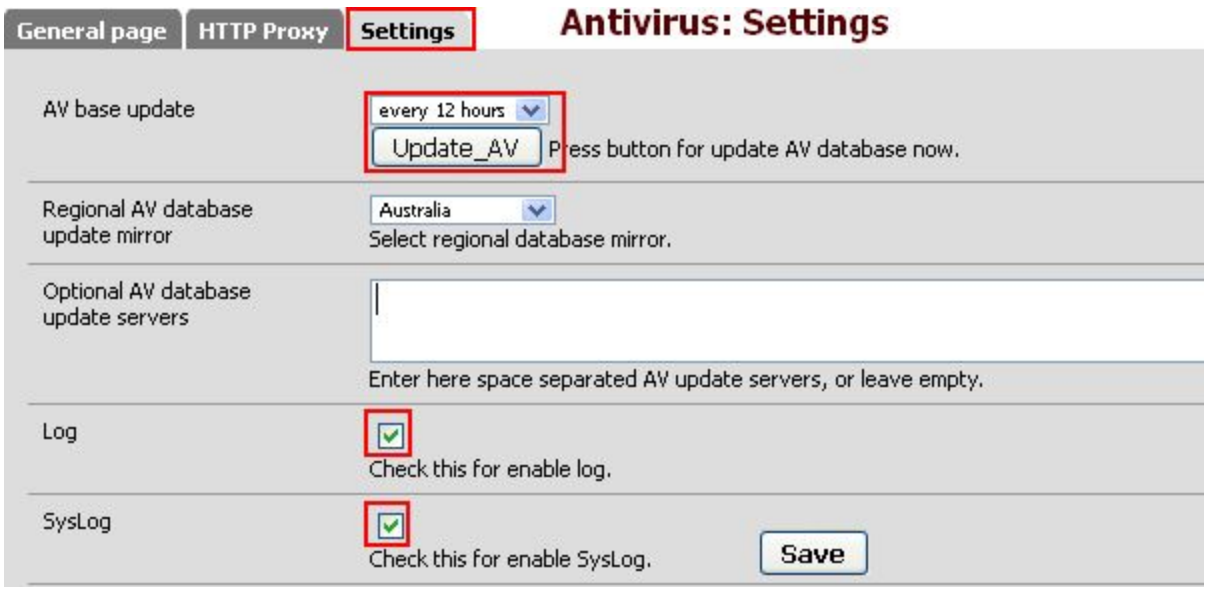


Log check
Syslog check
Chọn **Save**

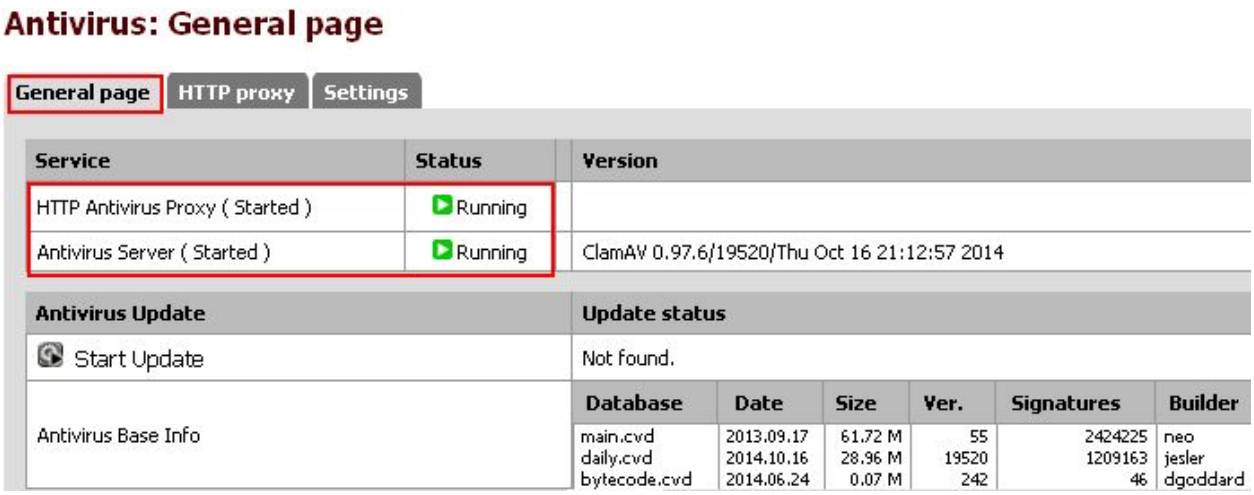
B3. Cấu hình cập nhập ClamAV

Service, **Antivirus**, chọn **Setting**

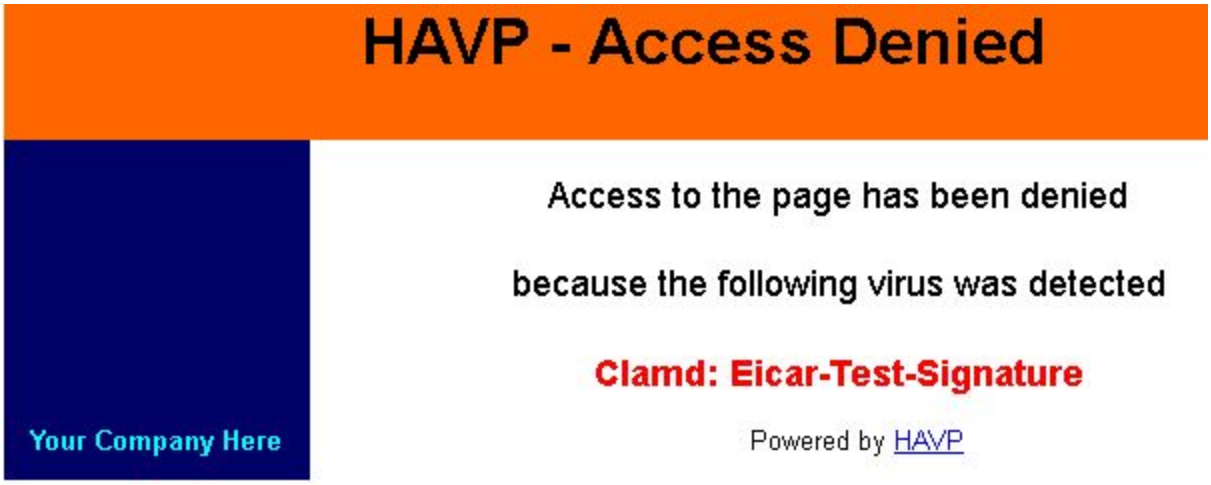
AV base update Chọn thời gian cập nhật
Regional AV database Nơi cập nhật
Log check
Syslog check
Chọn **Save**



B4. Kiểm tra các dịch vụ đã chạy



B5. Kiểm tra
Tại máy client truy cập trang http://www.eicar.org
Chọn download (http)

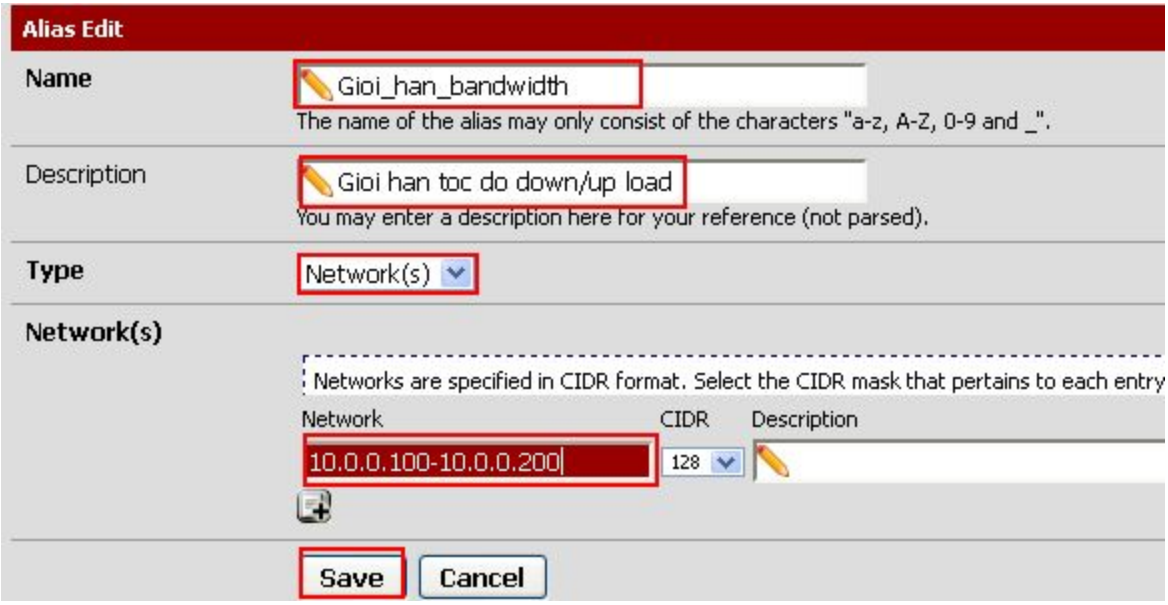


Khi download các file nhiễm virus sẽ gặp báo lỗi như trên

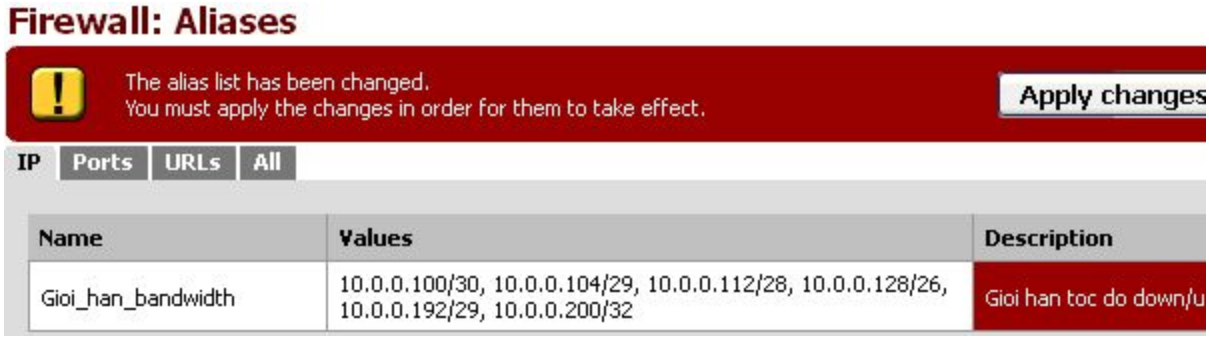
8. Limit bandwidth
Giới hạn các pc 10.0.0.100 – 10.0.0.200 có bandwidth
Download: max 1024 Kps
Upload: max 100 Kbp
Ngoài giờ làm việc thì không giới hạn download

B1. **Firewall**, **liases, IP,** nhắp dấu +

Name: Nhập Gioi_han_bandwidth
Description: Gioi han toc do down/up load
Type: chọn Network
Network Nhập 10.0.0.100-10.0.0.200
Nhấn **Save**



Nhấn Apply Change

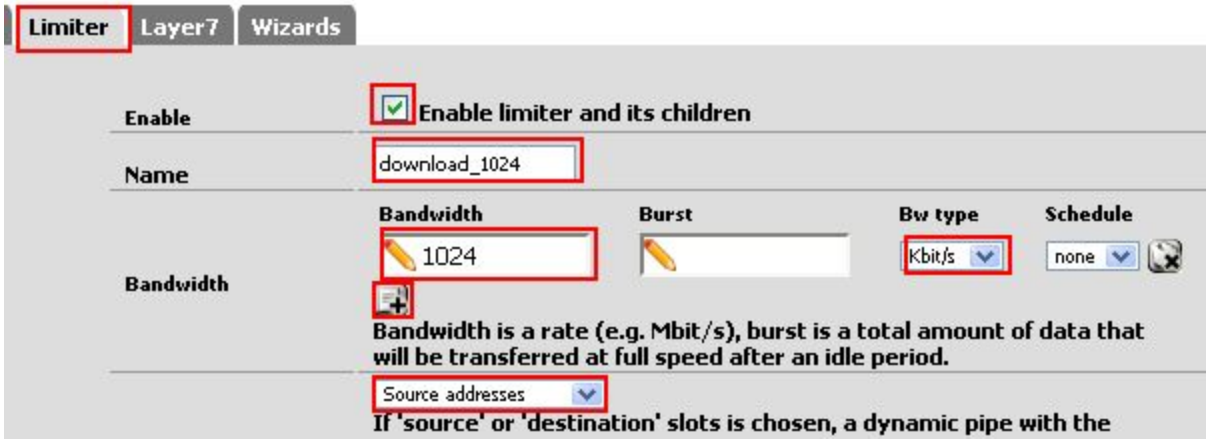


B2. **Firewall**, **Traffic Shaper**, **Limiter**

Chọn **Create new limiter**

Enable	Check	
Name	download_1024	
Bandwidth	1024 Kbps	
Mask	Source address	(chọn des sẽ giới hạn được IDM)
Description	Gioi han download	

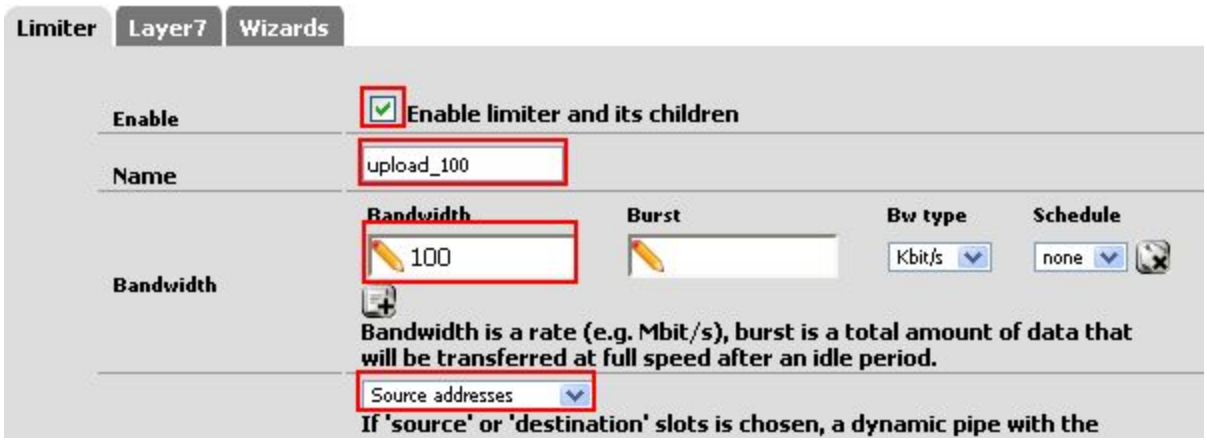
Chọn **Save**



Tương tự, chọn **Create new limiter** để giới hạn tóc độ upload

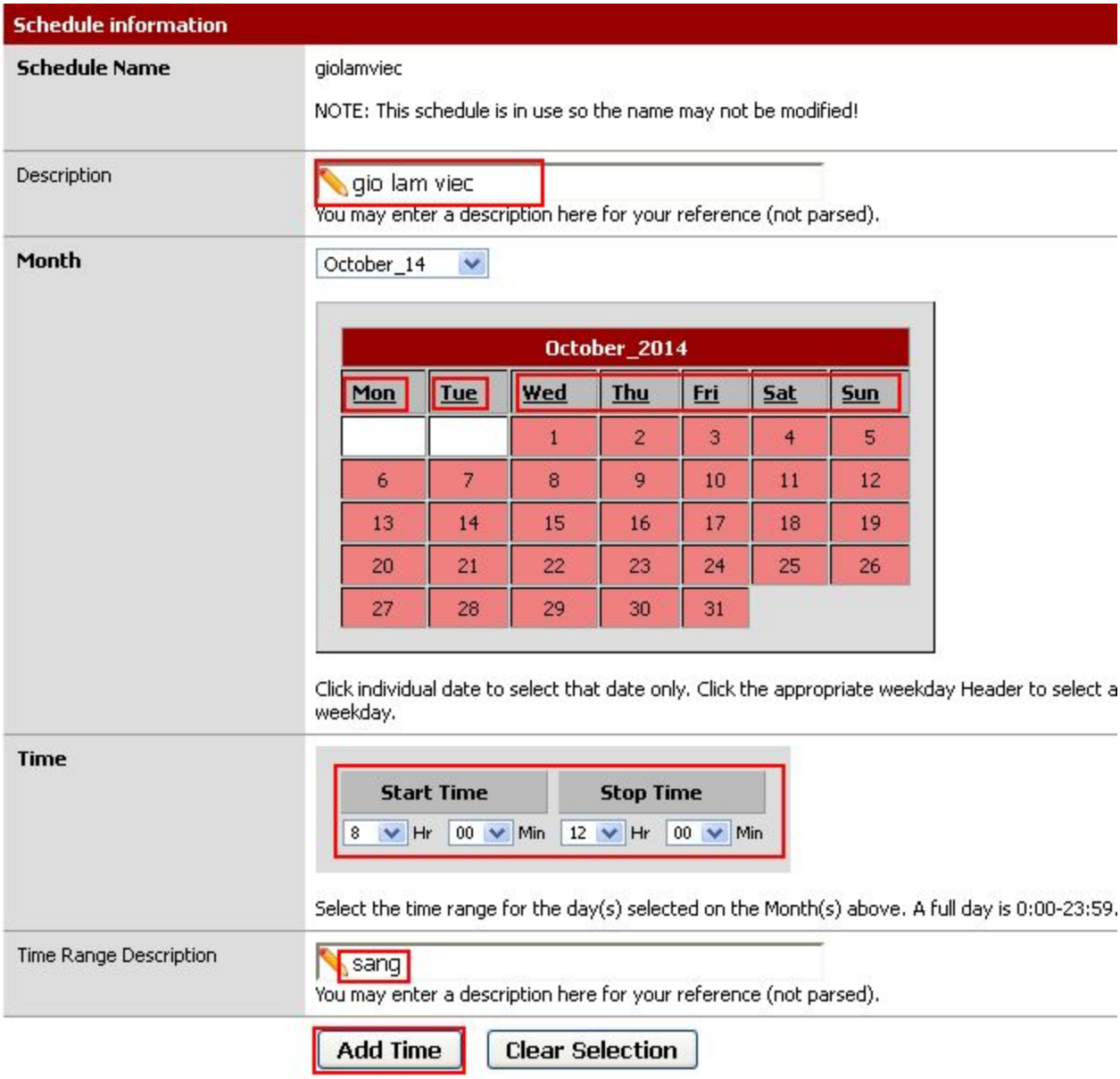
Enable	Check	
Name	upload_100	
Bandwidth	100 Kbps	
Mask	Source address	(chọn des sẽ giới hạn được IDM)
Description	Gioi han upload	

Chọn **Save**

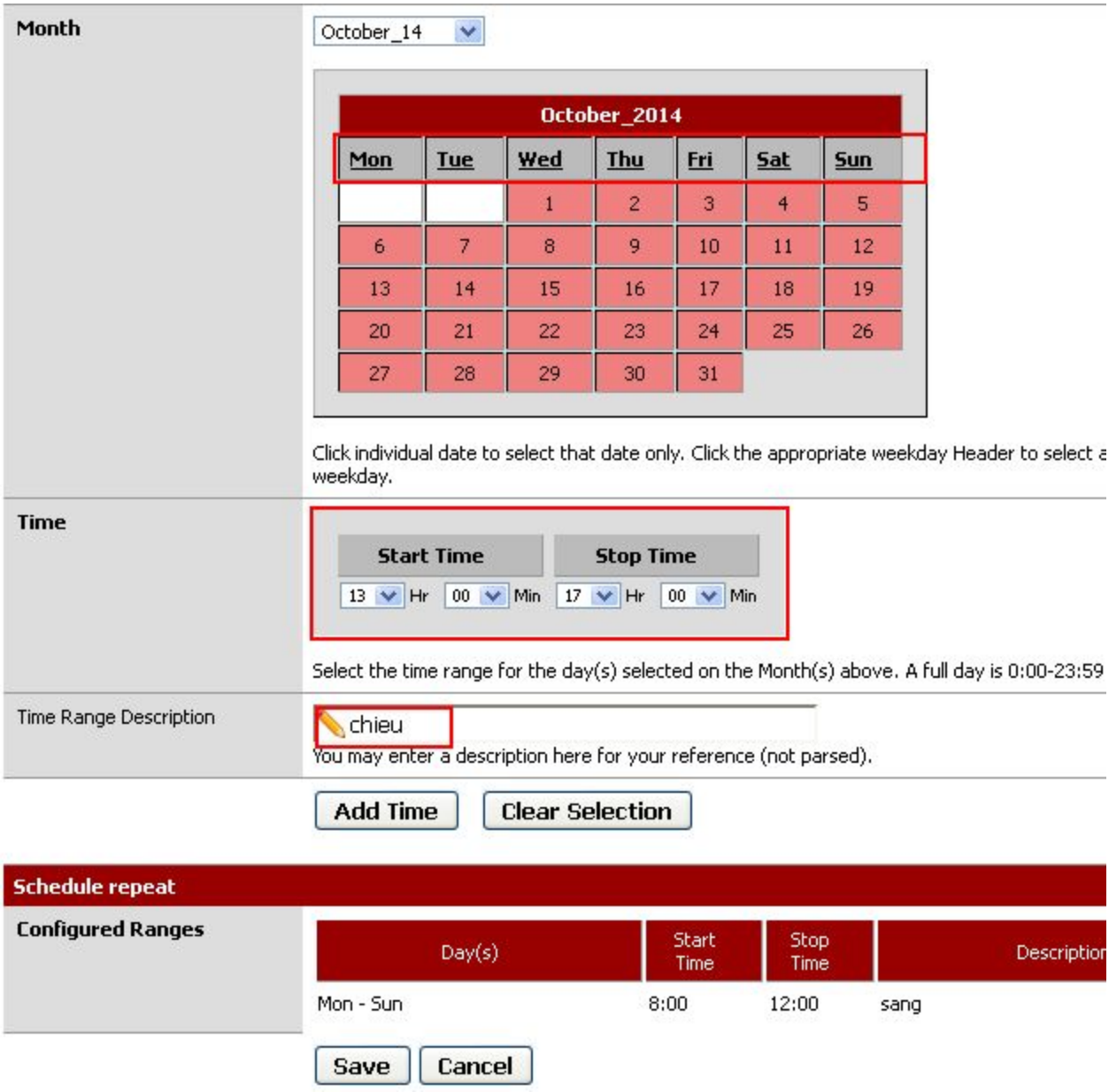


Nhấp Apply changes

B3. Khai báo giờ làm việc
Firewall, **Schedules**, nhắp +



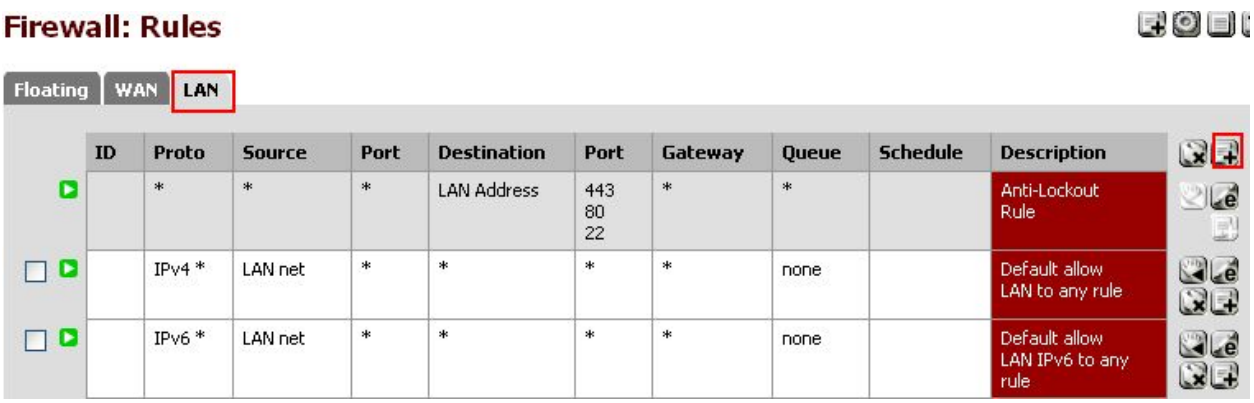
Khai báo thông tin như hình, chọn **Add Time**
Nhập thôn tin buổi chiều


Month
October_14
October_2014
Mon Tue Wed Thu Fri Sat Sun
1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31
Click individual date to select that date only. Click the appropriate weekday Header to select a weekday.
Time
Start Time
Stop Time
13 Hr 00 Min 17 Hr 00 Min
Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59
Time Range Description
chieu
You may enter a description here for your reference (not parsed).
Add Time
Clear Selection
Schedule repeat
Configured Ranges
Day(s)
Start Time
Stop Time
Description
Mon - Sun
8:00
12:00
sang
Save
Cancel

Chọn **save**


Firewall: Schedules
Name
Time Range(s)
Description
giolamviec
Mon - Sun 8:00-12:00 sang
Mon - Sun 13:00-17:00 chieu
gio lam viec
Note:
Schedules act as placeholders for time ranges to be used in Firewall Rules.

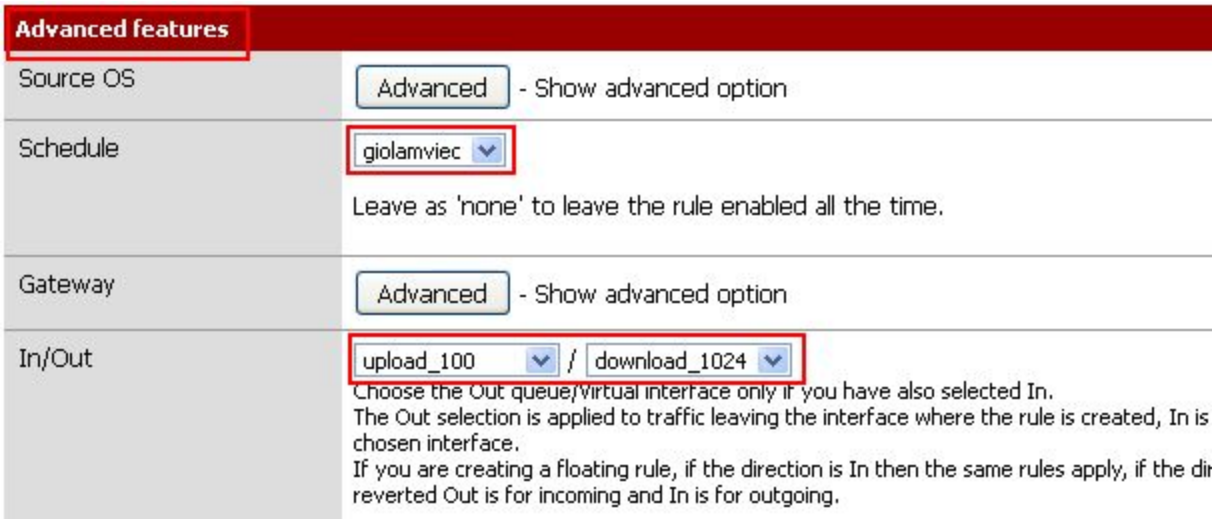
B4. Tạo rules
Firewall, **Rules**, **LAN,** nhắp +



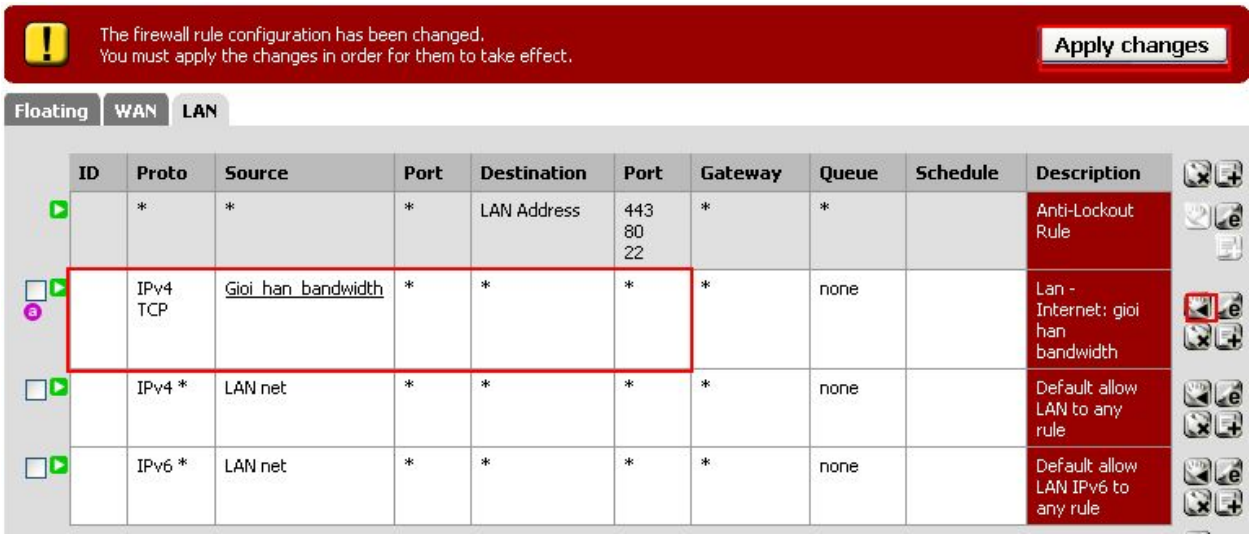
Khai báo các thông tin sau:

Action	Pass
Interface	Lan
TCP/IP Version	Ipv4
Protocol	TCP
Source	Sigle host or alias
	Nhập Address: *Gioi_han_bandwidth*
Destination	any
Description	Lan - Internet: gioi han bandwidth

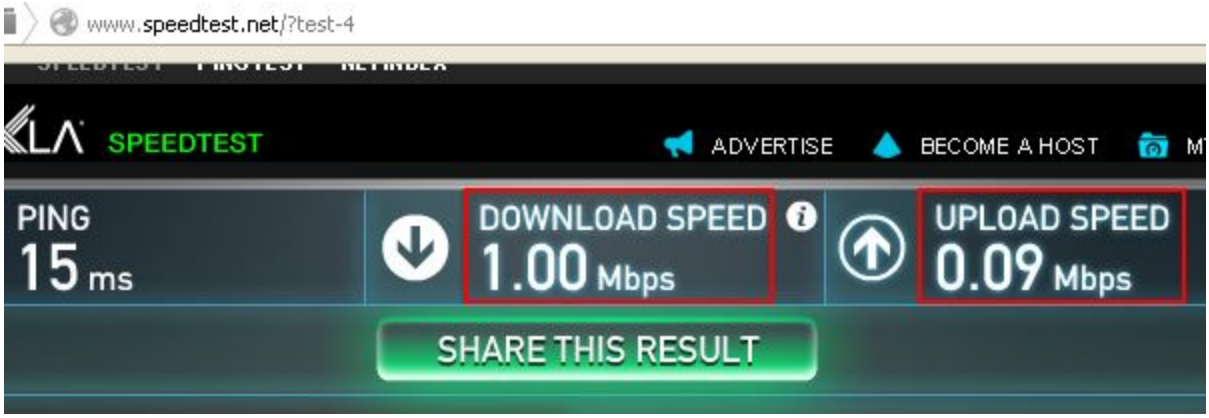
Schedule giolamviec
In: upload_100
Out: download_1024



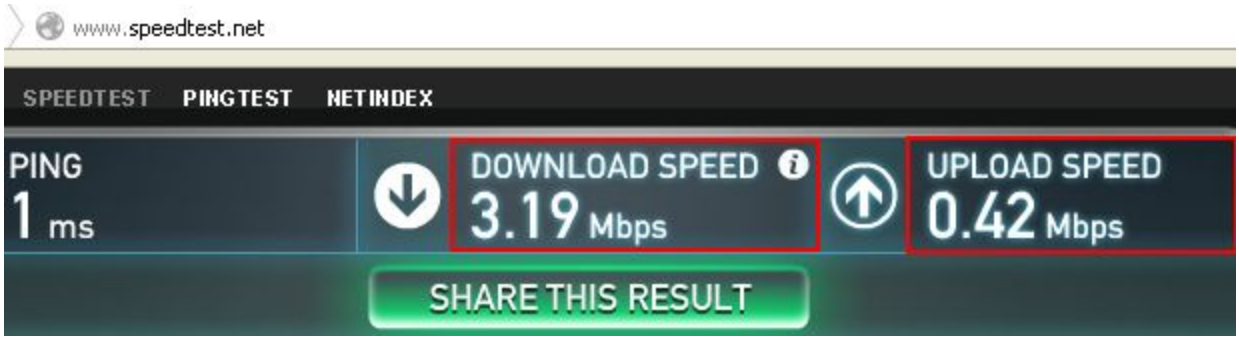
Chọn **save**
Rule vừa tạo phải di chuyển lên trên cùng



B4. Kiểm tra các máy thuộc dải IP 10.0.0.100-100.0.0.200 (*chú ý giờ trên firewall*)



Kiểm tra các máy không thuộc dải IP 10.0.0.100-100.0.0.200
Các máy nà không bị ảnh hưởng bởi chính sách giới hạn download/uoload



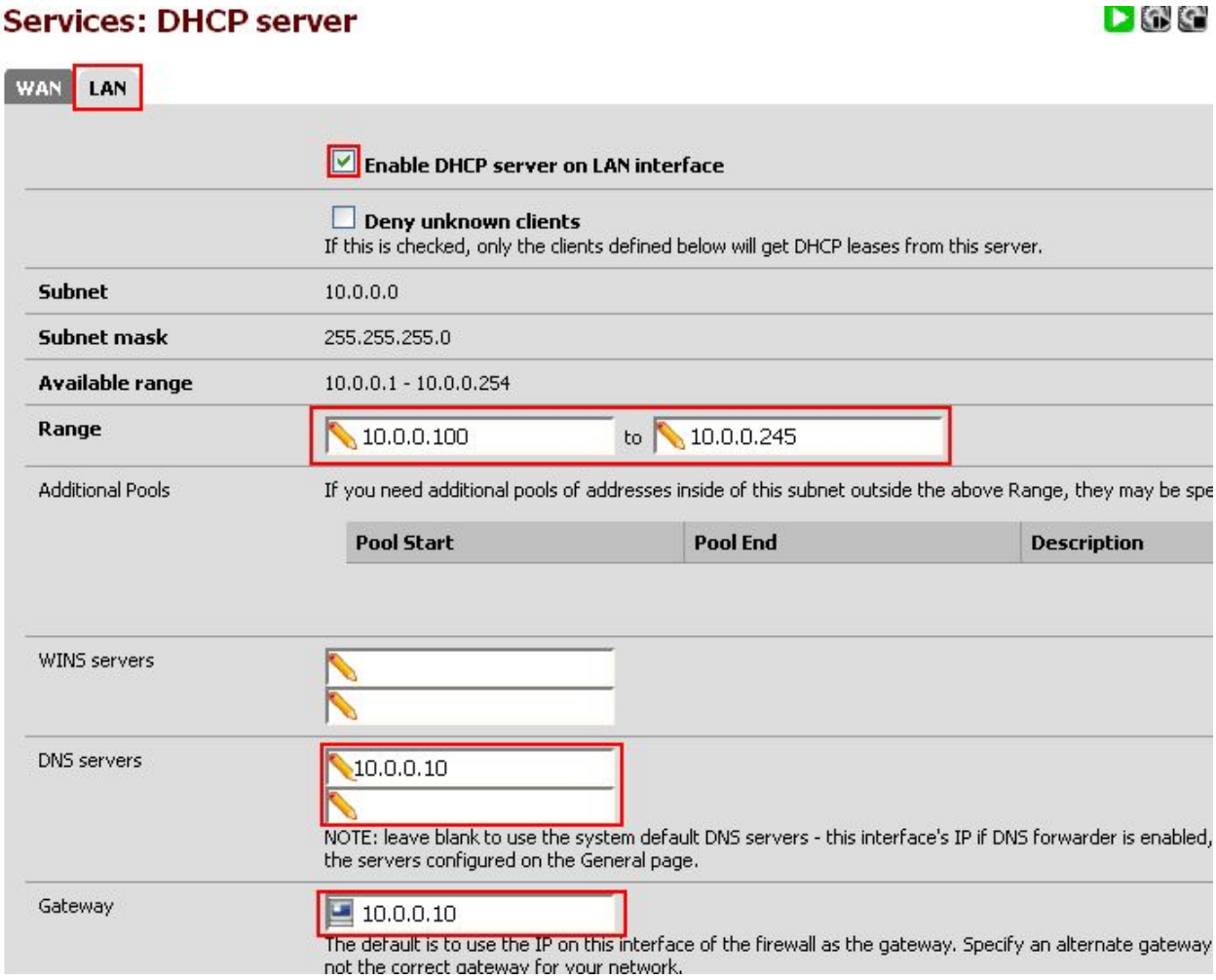
Captive portal

Captive portal là kỹ thuật buộc người dùng phải chứng thực qua 1 giao diện web trước khi kết nối vào internet. Kỹ thuật này thường áp dụng cho các điểm truy cập wifi, mạng có dây. Người dùng muốn truy cập vào, phải có một account chứng thực.

Chuẩn bị: - Cấu hình transparent Proxy để các client có thể truy cập web
- Các client phải sử dụng DNS của FW

B1. cấu hình DHCP
Services,DHCP server, chọn thẻ **LAN**

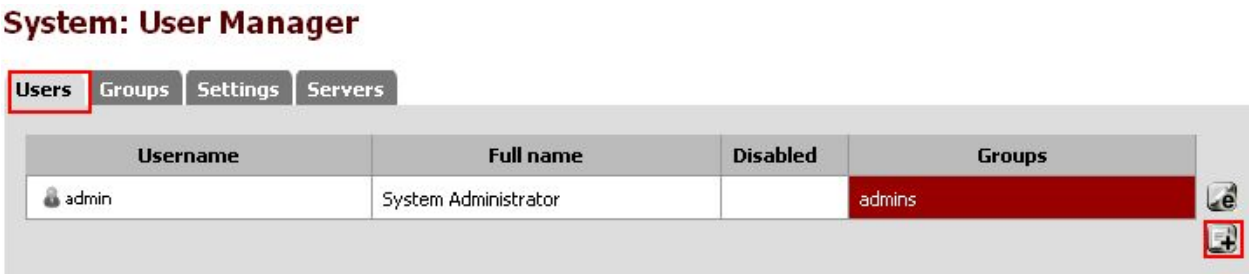
Enable DHCP server on LAN interface	check
Range	Nhập 10.0.0.100 - 10.0.0.245
DNS servers	Nhập 10.0.0.10 (dns của pfsense)
Gateway	10.0.0.10
Chọn **Save**	



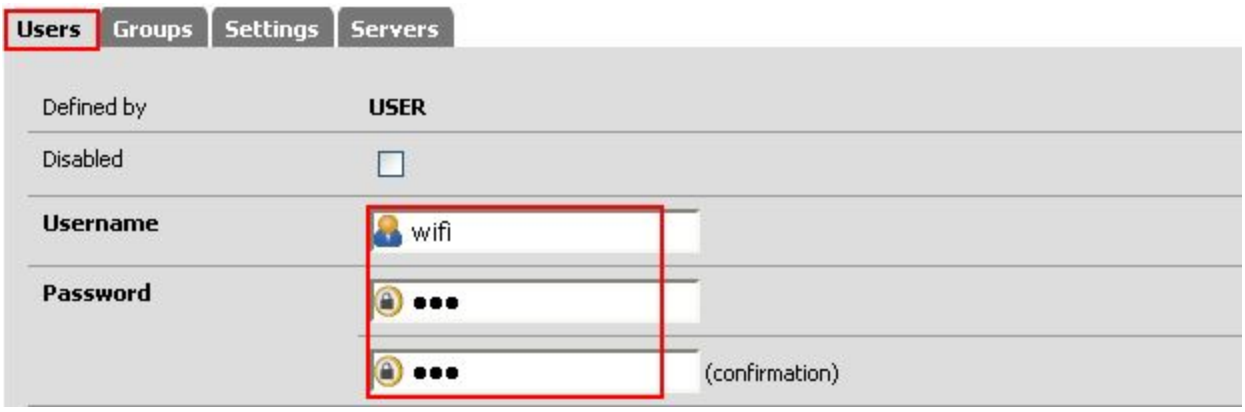
B2. client xin IP

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : client1
        Primary Dns Suffix  . . . . . . . : nhatnghe1.com
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : nhatnghe1.com

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapt
 #2
        Physical Address. . . . . . . . . : 00-0C-29-26-1A-7A
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.0.0.123
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . : 10.0.0.10
        DNS Servers . . . . . . . . . . . : 8.8.8.8
                                            208.67.222.222
```

B3. Tạo user
System, User Manager, nhấn +

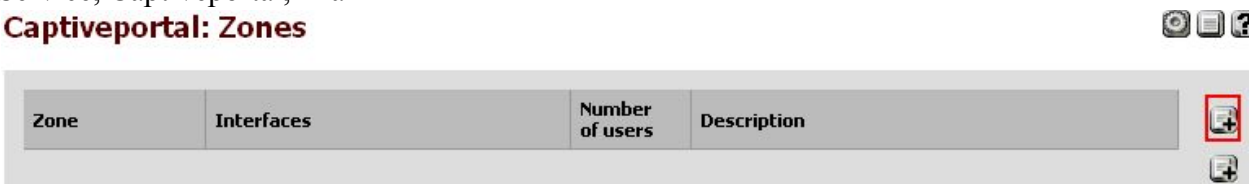


Username Nhập wifi
Password Nhập 123
Chọn **Save**

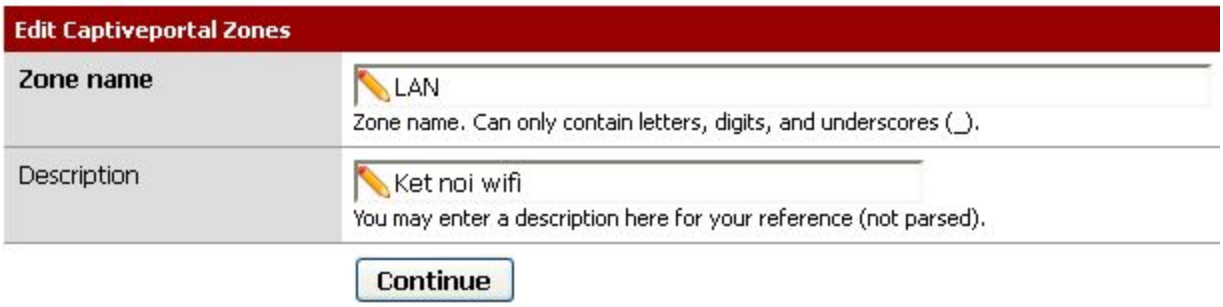


B4. Cấu hình Captiveportal

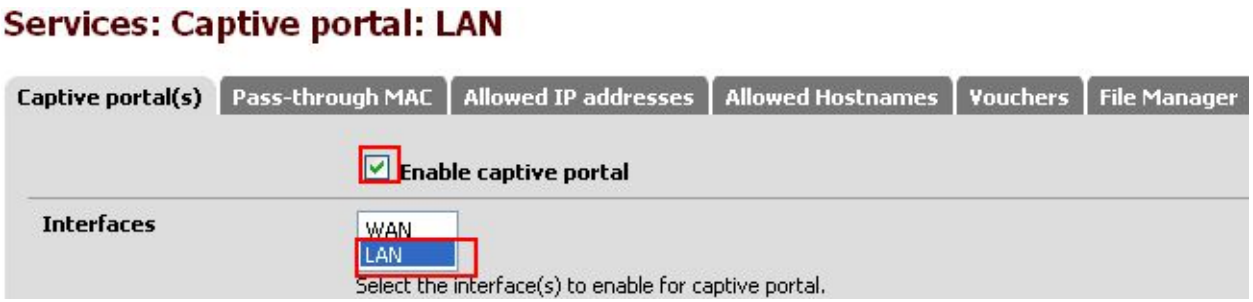
Service, Captiveportal, nhấn +



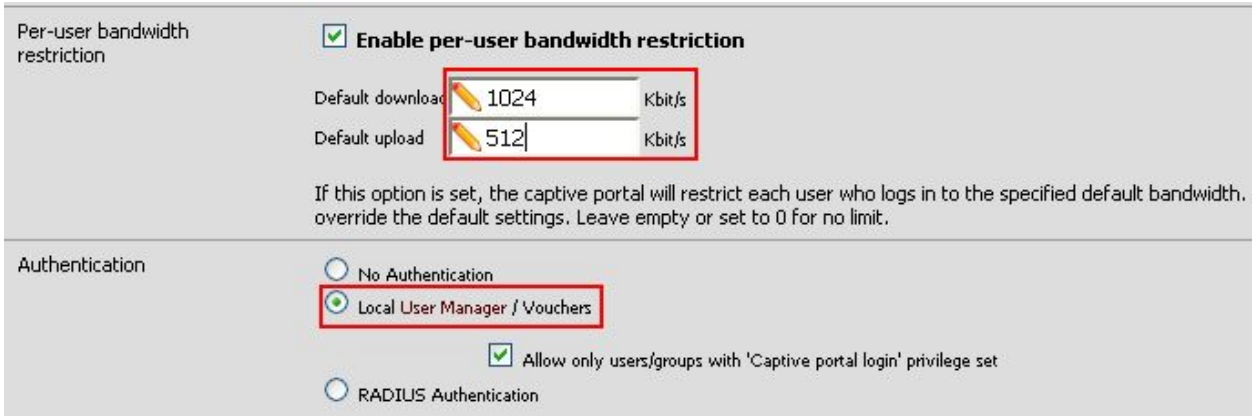
Zone name Nhập LAN
Description Ket noi wifi
Nhấn **continue**



B5. Cấu hình Captiveportal
Enable captive portal check
Interfaces chọn LAN



Per-user bandwidth restriction Giới hạn bandwidth cho mỗi user
Authentication chọn Local User Manager /
Vouchers



Khai báo file chứa code trang web login

Login.html

```
<h1>Thank you for connecting to our network.</h1>
<h3>Please enter your username and password to access the Internet</h3>
<form action="$PORTAL_ACTION$" method="post">
<p>Username:<input name="auth_user" type="text" /></p>
<p>Password:<input name="auth_pass" type="password" /></p>
<p><input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$" /></p>
<p><input name="accept" type="submit" value="Login" /></p>
</form>
```

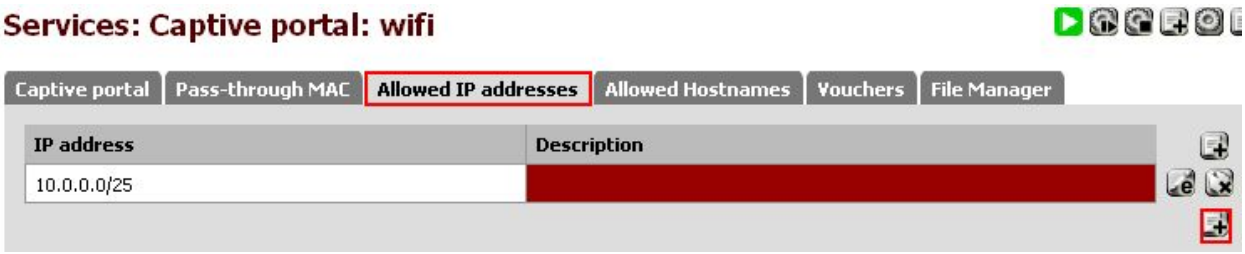
Chọn **Save**

B6. client truy cập

Máy client khi truy cập web sẽ phải nhập user name và password

Chú ý: nếu máy client không chỉ DNS về FW (10.0.0.10) thì sẽ không thể truy cập web

B7. Không yêu cầu chứng thực với 1 dải IP
Services,Captive portal, Chọn **Allowed IP address**, nhấn +



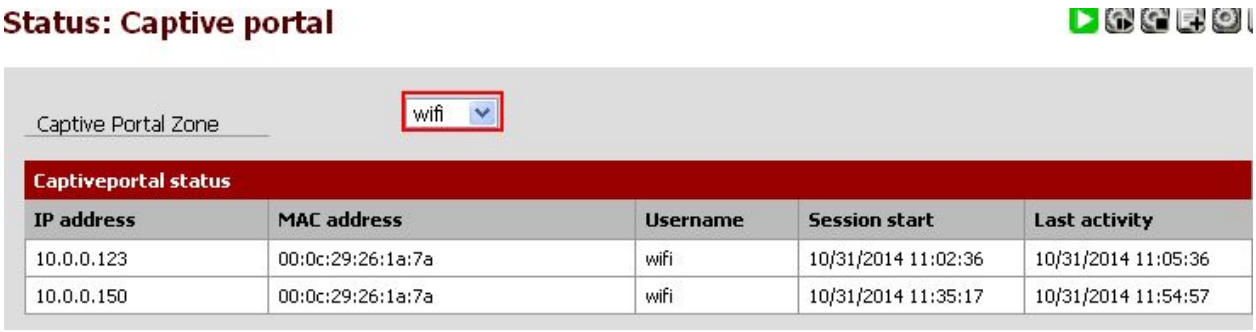
IP address: nhập 10.0.0.0/25 (dải IP 10.0.0.1-10.0.0.126)
Chọn **Save**

Kết quả:

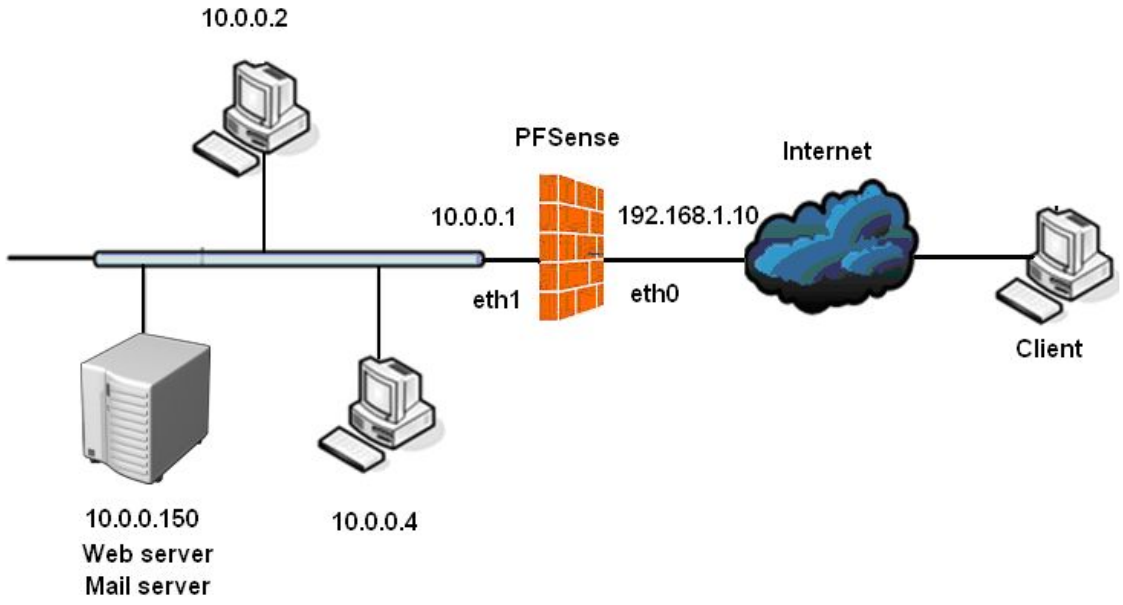
Máy client đặt ip thuộc dải ip 10.0.0.1-10.0.0.126 sẽ không phải nhập user/pass

Tương tự có thể không yeu cầu nhập user/pass với các MAC address hoặc hostname chỉ định trong các mục: pass-through MACs, allowed Hostnames.

B8.
Status, Captive portal, chọn wifi xem thông tin các client đã kết nối



SERVER PUBLISHING



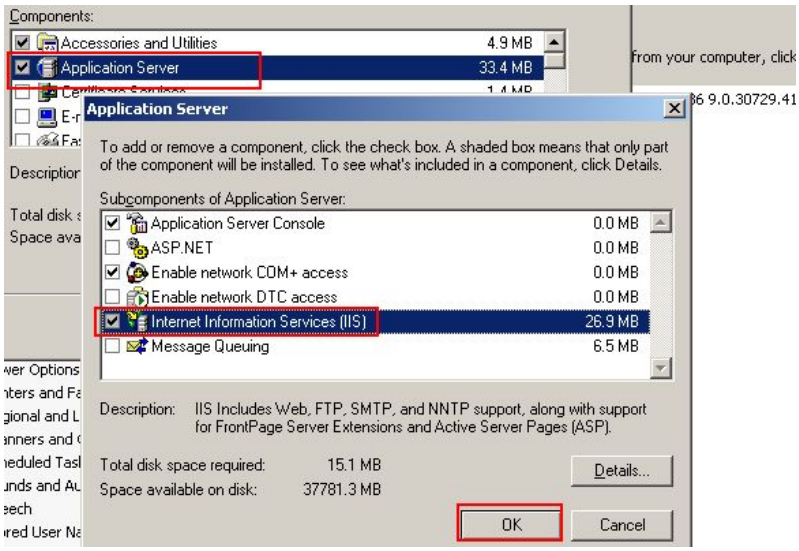
1. Publish Web server

B1. Máy 10.0.0.150 cài IIS và tạo trang web

Control Panel, Add/Removw Program, Application Server, IIS, OK

Tạo file C:\Inetpub\wwwroot\ default.htm có nội dung:

<h1> Web dat ben trong mang LAN



B2. Tạo rules

Firewall, **NAT**, chọn **Port Forward WAN**, nhấn +

Khai báo các thông số:

Interface	WAN
Protocol	TCP
Source	Any
Destination	Wan address
Redirect target port	http
Redirect target IP	10.0.0.150
Redirect target port	http
Description	Publish Web server

Firewall: NAT: Port Forward: Edit

Edit Redirect entry	
Disabled	☐ **Disable this rule** Set this option to disable this rule without removing it from the list.
No RDR (NOT)	☐ Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	WAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	☐ **not** Use this option to invert the sense of the match. Type: any Address: / 31
Source port range	from: any to: any Specify the source port or port range for this rule. **This is usually *random* and almost destination port range (and should usually be 'any').** Hint: you can leave the *'to'* field empty if you only want to filter a single port.
Destination	☐ **not** Use this option to invert the sense of the match. Type: WAN address Address: / 31
Destination port range	from: HTTP to: HTTP Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the *'to'* field empty if you only want to map a single port
Redirect target IP	10.0.0.150 Enter the internal IP address of the server on which you want to map the ports. e.g. *192.168.1.12*
Redirect target port	HTTP Specify the port on the machine with the IP address entered above. In case of a port rang the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	Publish Web server You may enter a description here for your reference (not parsed).

Chọn **Save**
Nhấp **Apply changes**

Firewall: NAT: Port Forward

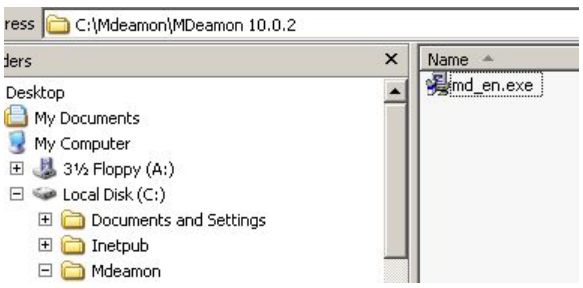
Port Forward | 1:1 | Outbound | NPt

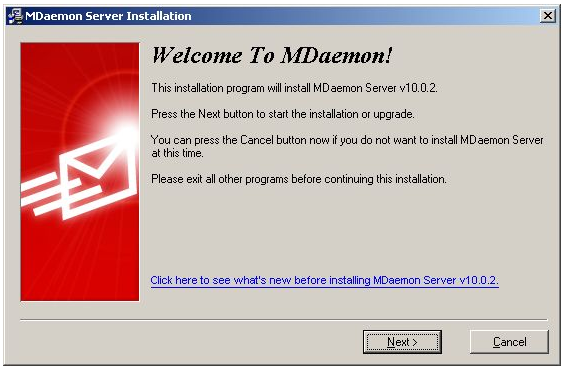
	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
☐	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.150	80 (HTTP)	Publish Web server

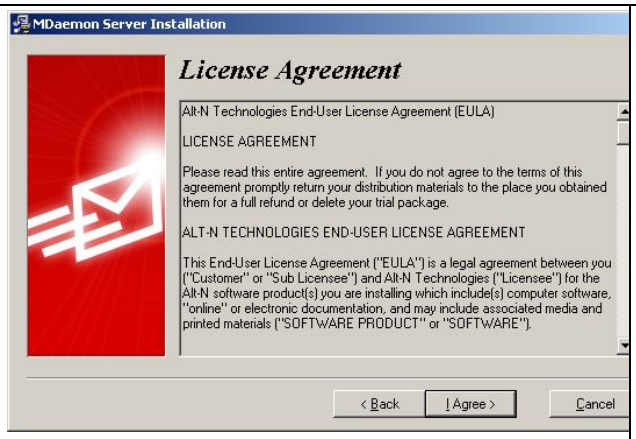
B3. Tại máy client từ bên ngoài Internet, mở IE, truy cập vào IP mặt ngoài của Firewall

2. Publish Mail server (POP3 & SMTP)
Máy 10.0.0.150 cài Mdaemon làm mail server
B1.

Cài Mdeaon 10.0.2	Chọn Next
Chọn I Agree	Chọn thư mục cài đặt

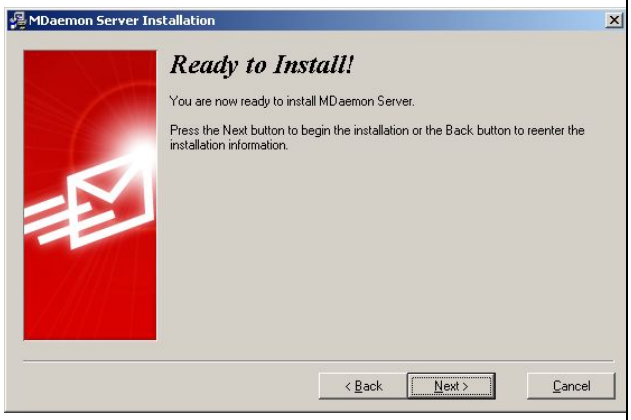






Nhấn Next bắt đầu cài đặt

Nhập tên domain: nhatnghe1.com

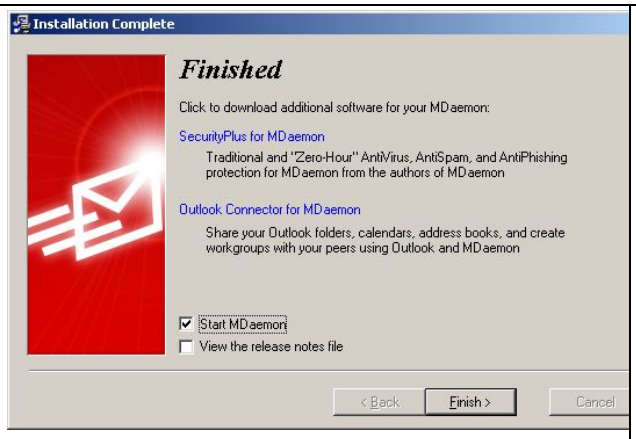


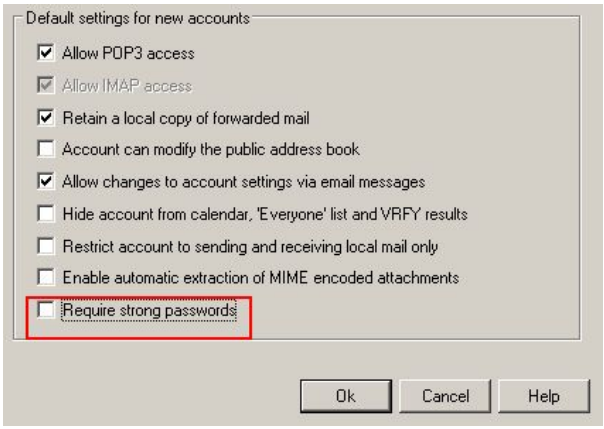
Tạo mailbox admin

Khai báo DNS

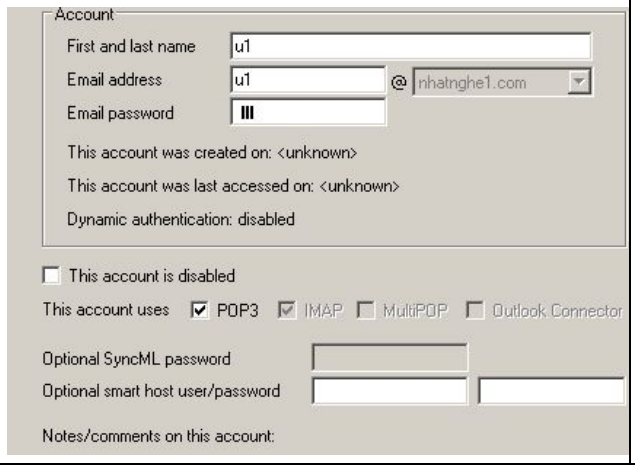
Nhấn Finish

Account, Account setting, bỏ check yêu cầu password phức tạp



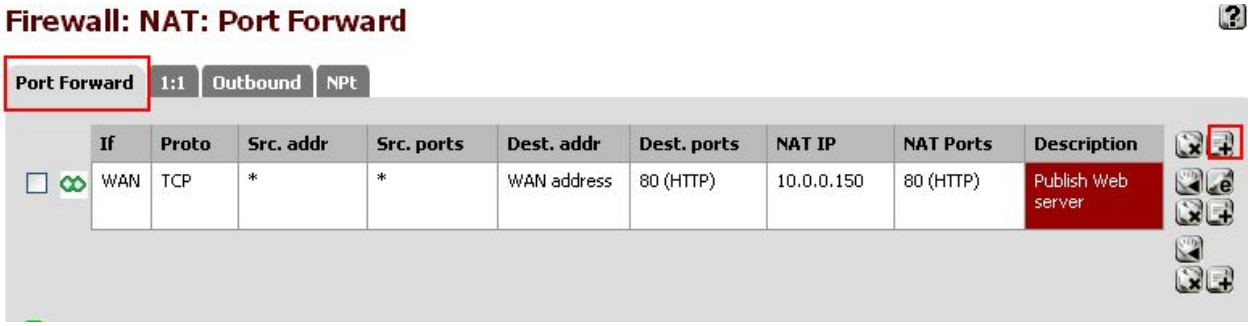


Account, Account Manage, Tạo mailbox u1



B2. Tạo rule

Firewall, **NAT**, chọn **Port Forward WAN**, nhấn +



Firewall: NAT: Port Forward: Edit

Edit Redirect entry	
Disabled	☐ **Disable this rule** Set this option to disable this rule without removing it from the list.
No RDR (NOT)	☐ Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	WAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	☐ **not** Use this option to invert the sense of the match. Type: any Address: / 31
Source port range	from: any to: any Specify the source port or port range for this rule. **This is usually *random* and almos** **destination port range (and should usually be 'any').** Hint: you can leave the *'to'* field empty if you only want to filter a single port.
Destination	☐ **not** Use this option to invert the sense of the match. Type: WAN address Address: / 31
Destination port range	from: SMTP to: SMTP Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the *'to'* field empty if you only want to map a single port
Redirect target IP	10.0.0.150 Enter the internal IP address of the server on which you want to map the ports. e.g. *192.168.1.12*
Redirect target port	SMTP Specify the port on the machine with the IP address entered above. In case of a port rar the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	Publish mail smtp You may enter a description here for your reference (not parsed).

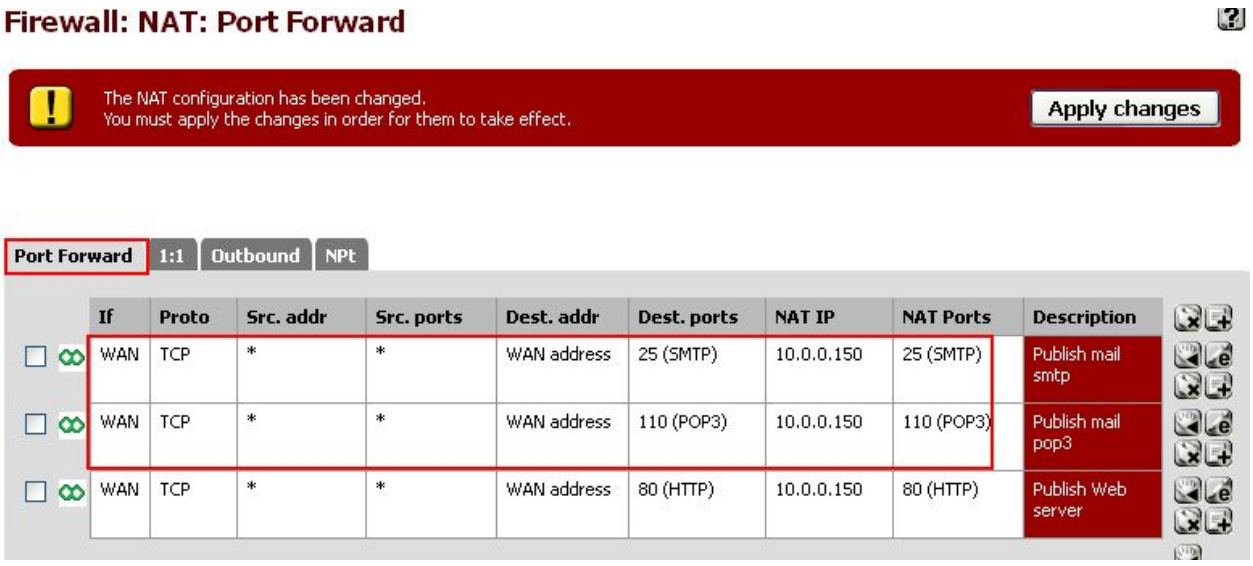
Khai báo các thông số:

Interface	WAN
Protocol	TCP
Source	Any
Destination	Wan address
Redirect target port	smtp
Redirect target IP	10.0.0.150
Redirect target port	smtp
Description	Publish mail smtp

B3. Lặp lại bước trên để nat trên port 110

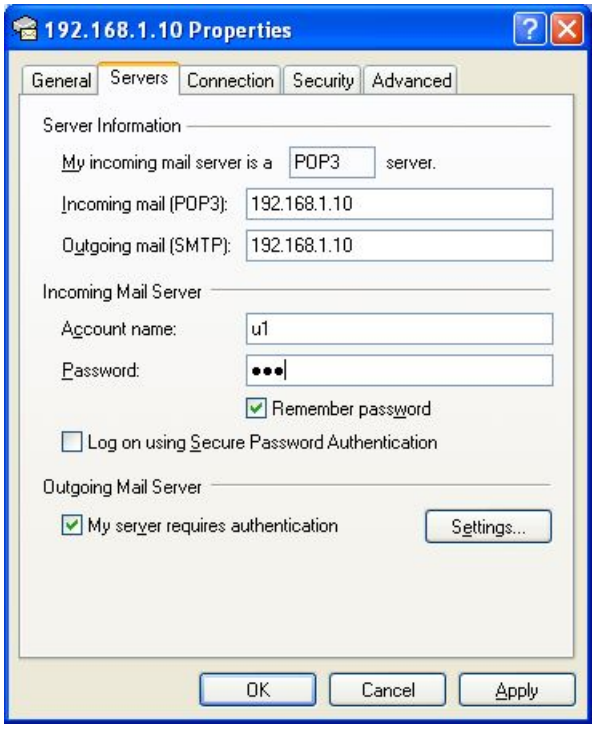
Khai báo các thông số:

Interface	WAN
Protocol	TCP
Source	Any
Destination	Wan address
Redirect target port	pop3
Redirect target IP	10.0.0.150
Redirect target port	pop3
Description	Publish mail pop3

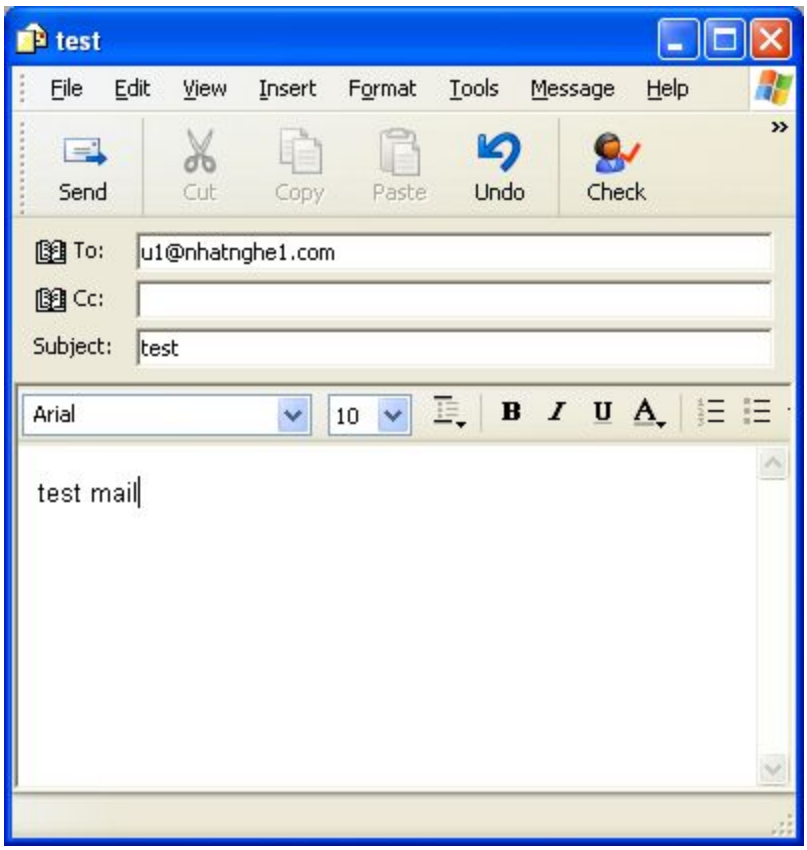


Nhấn Apply changes

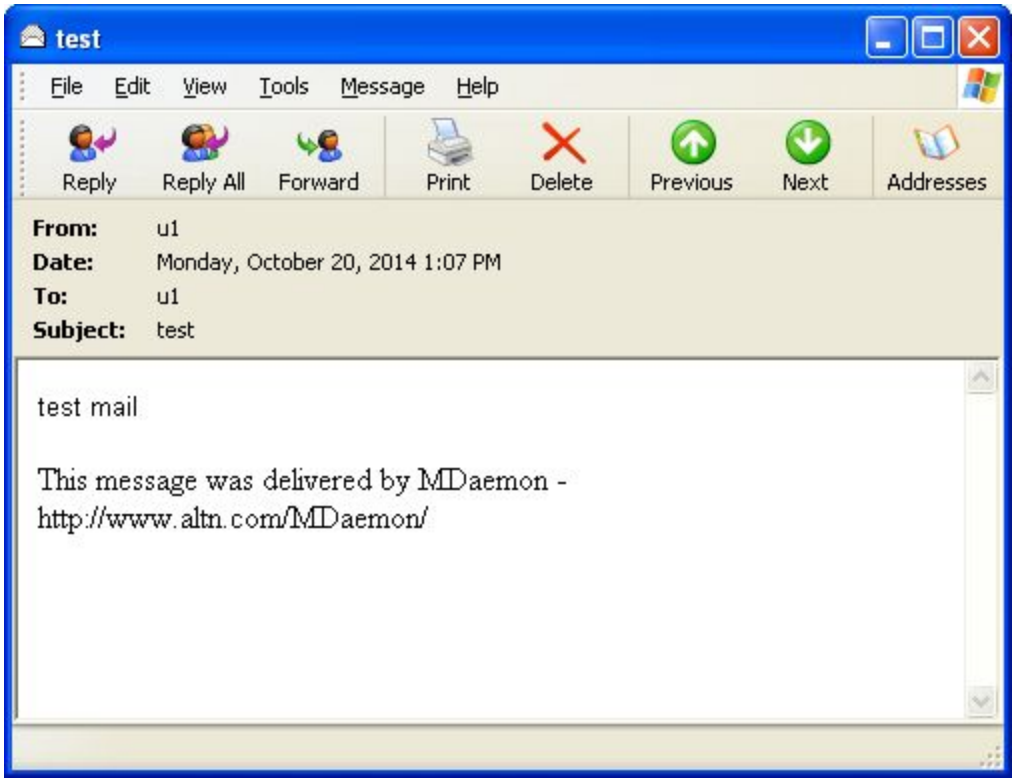
B4. Tại máy client từ bên ngoài Internet, mở Outlook Express
Cấu hình mail cho u1@nhatnghe1.com



Soạn email , nhấn send

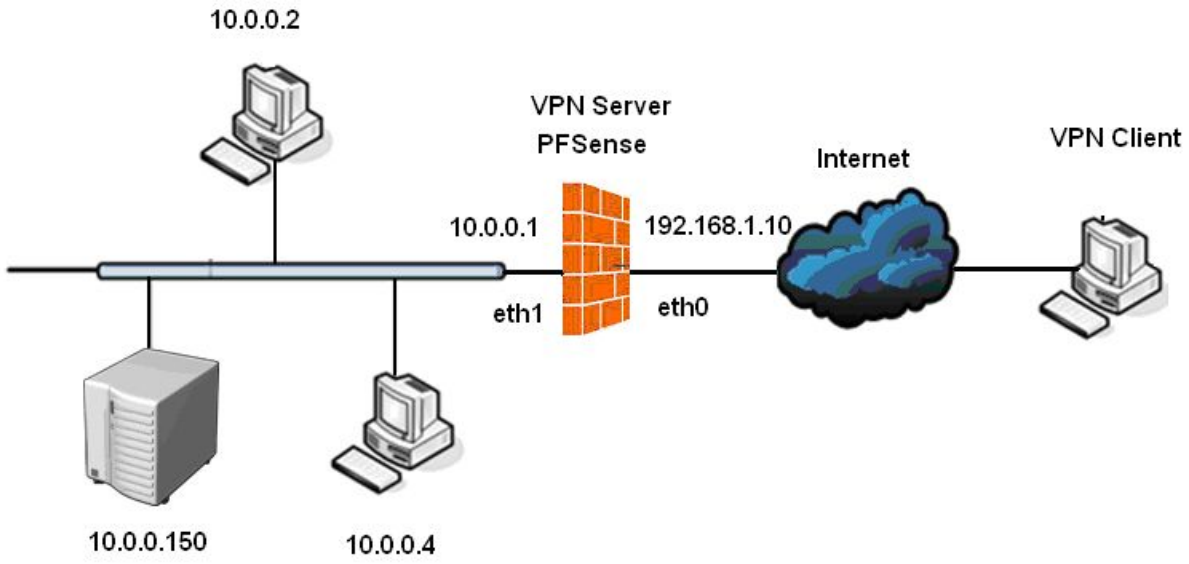


U1 nhận được mail do chính mình gởi

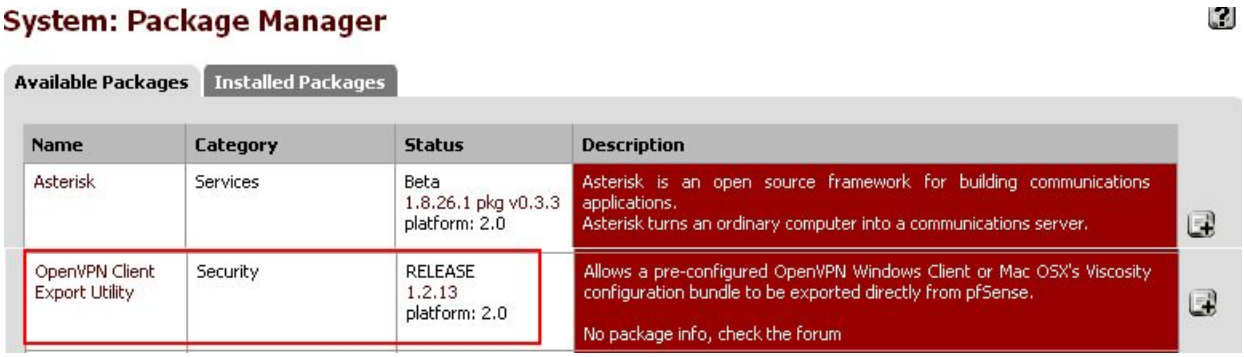


OPENVPN

1. client to site - OpenVPN with TLS and local User Authentication



B1. cài gói OpenVPN Client Export Utility
System, Package, chọn gói *OpenVPN Client Export Utility*, nhắp +

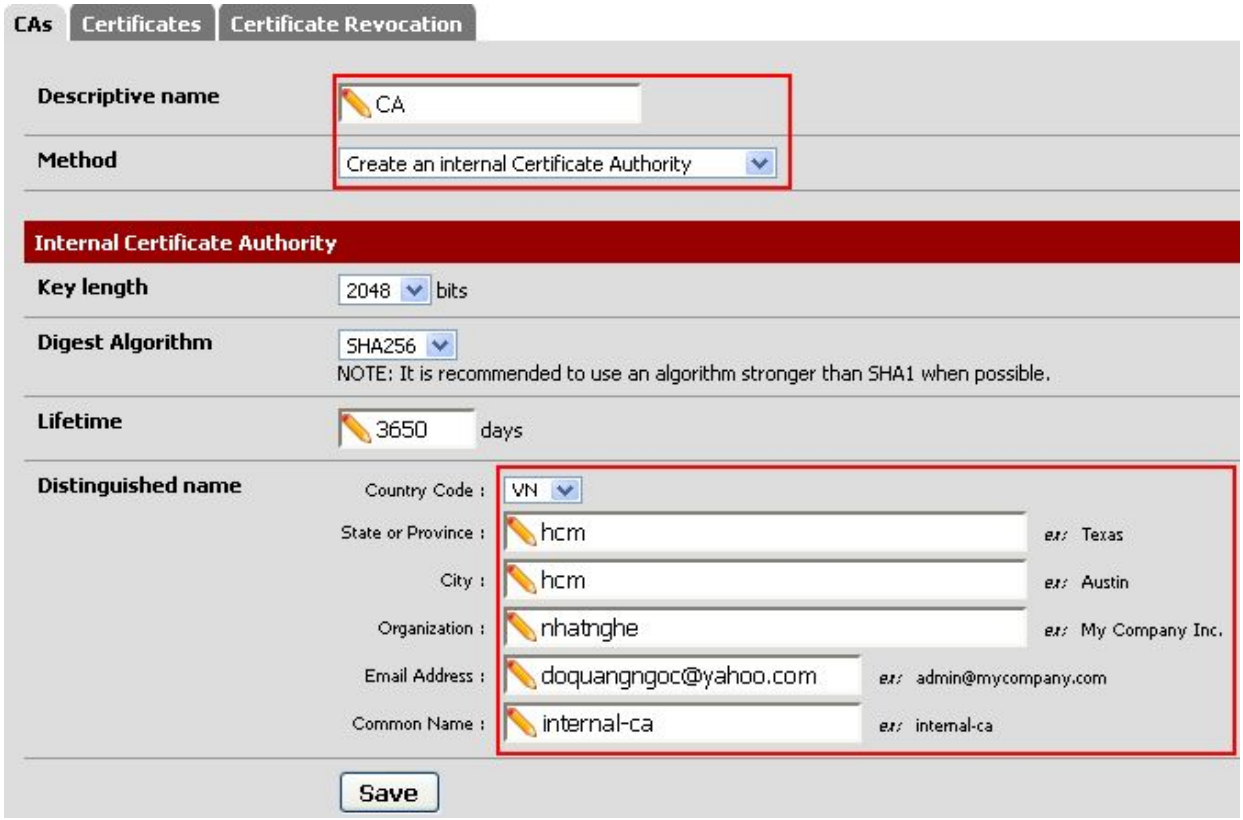


B2. Tạo chứng chỉ cho vpn server
System, **Cert Manager, CA,** nhắp +

Khai báo các thông tin cho CA:

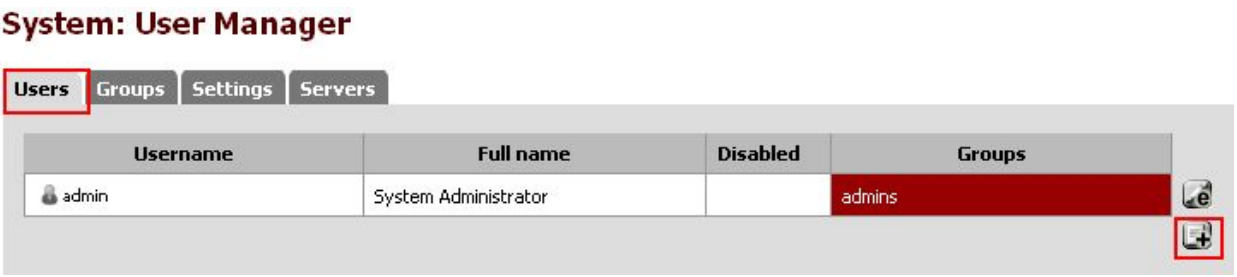
Descriptive name:	CA
Method:	Create an internal Certificate Authority
State or Province :	hcm
City :	hcm
Organization :	nhatnghe
Email Address :	doquangngoc@yahoo.com
Common Name :	internal-ca

Chọn **Save**



CA đã được tạo

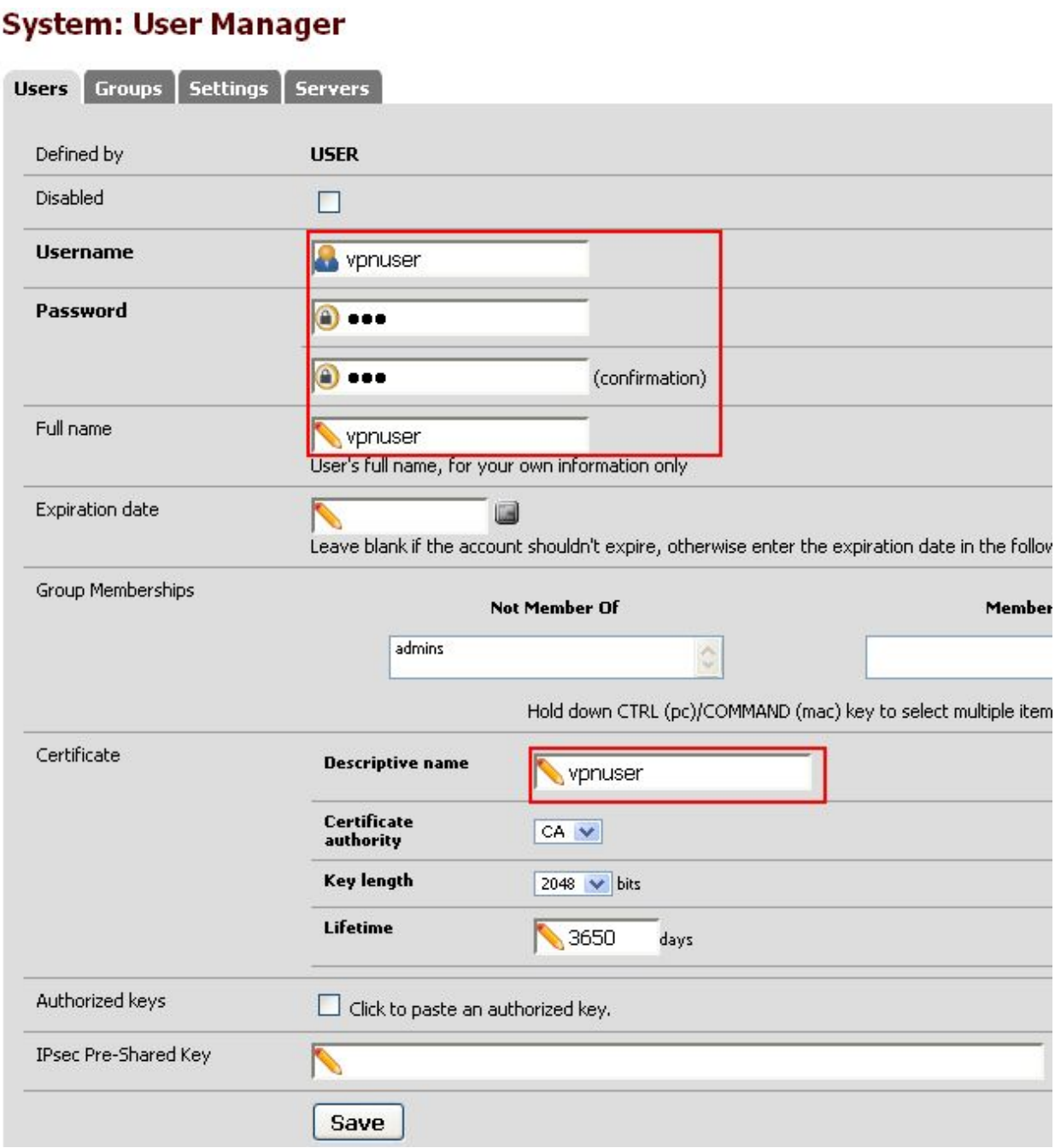
B3. tạo user
System, User Manager, Users, nhắp +



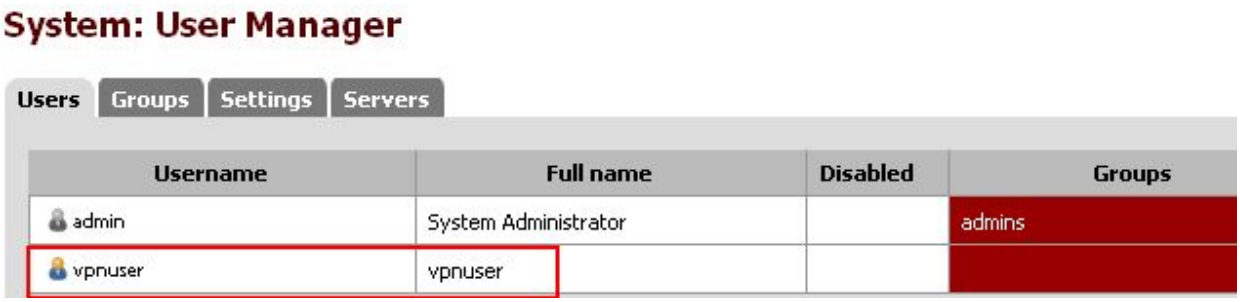
Khai báo các thông tin cho user:

Username	vpnuser
Password	123
Full name	vpnuser
Certificate	check, tạo cetificate cho user vpnuser nhập vpnuser

Chọn **Save**



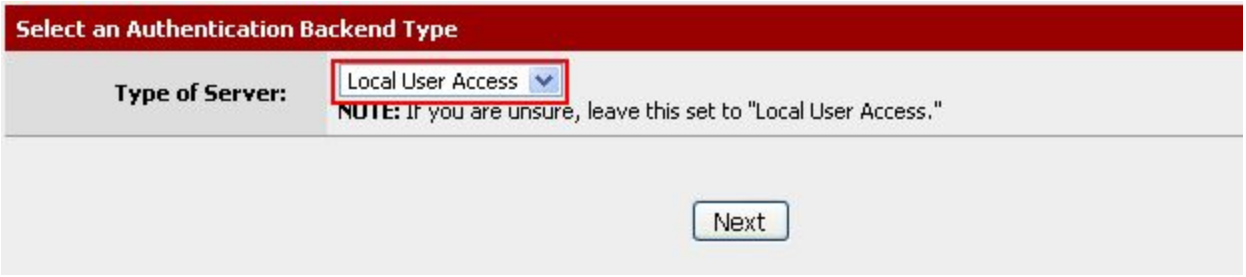
User vpnuser đã được tạo



B4. Cấu hình openvpn

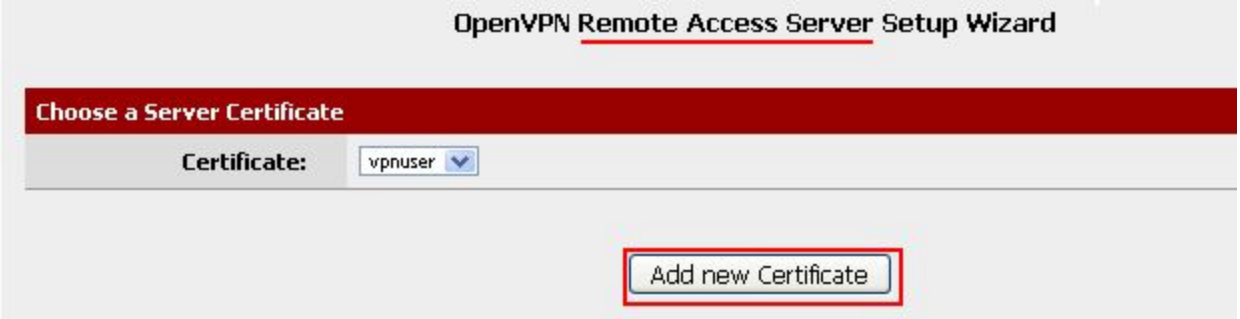
VPN, chọn **OpenVPN,** chọn **Wizard**

B5. chọn kiểu chứng thực
Type of Server: chọn **Local user Access**
Nhấn **Next**



B6. Chọn CA
Chọn CA, Nhấn **Next**

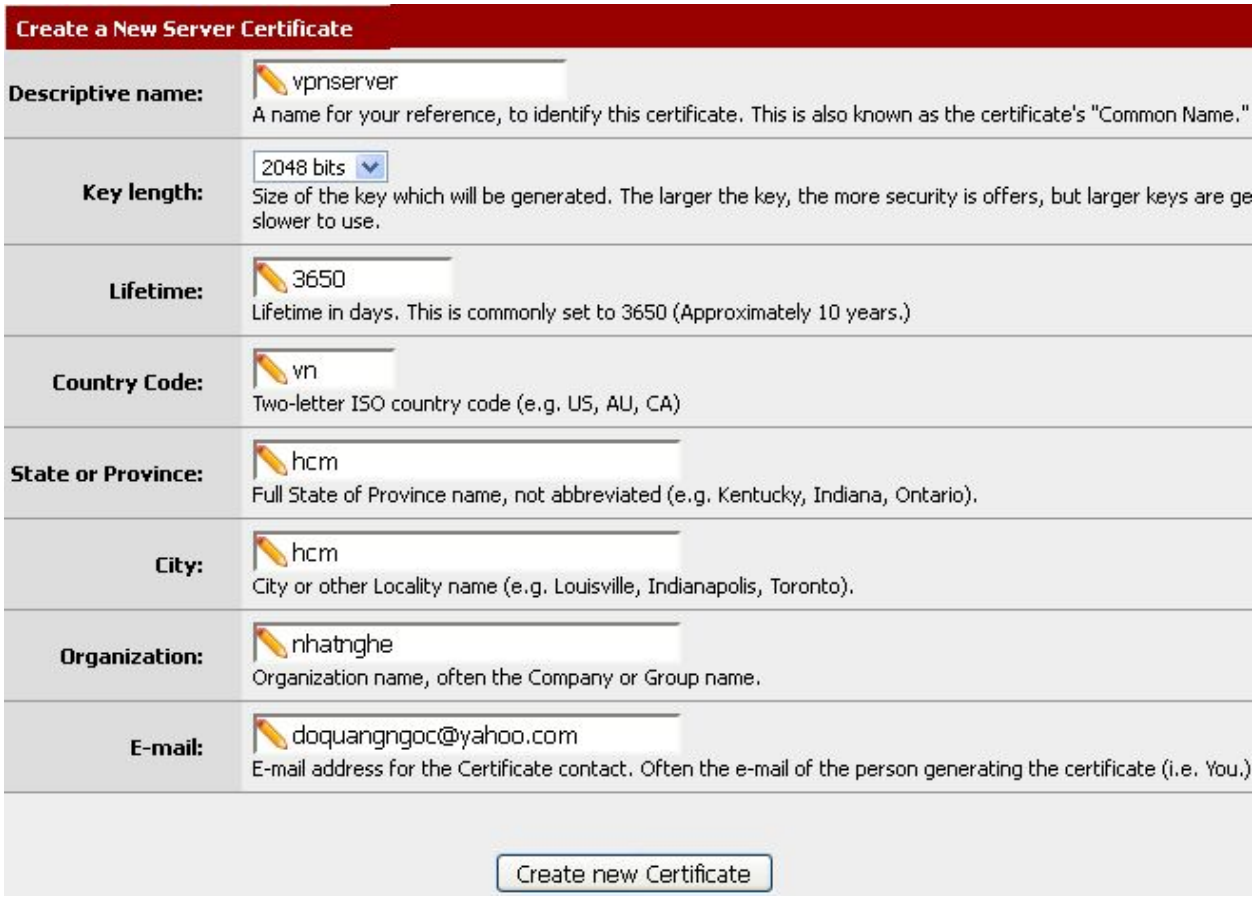
B7. Tạo chứng chỉ cho openvpn server
Nhấn **Add new Certificate**



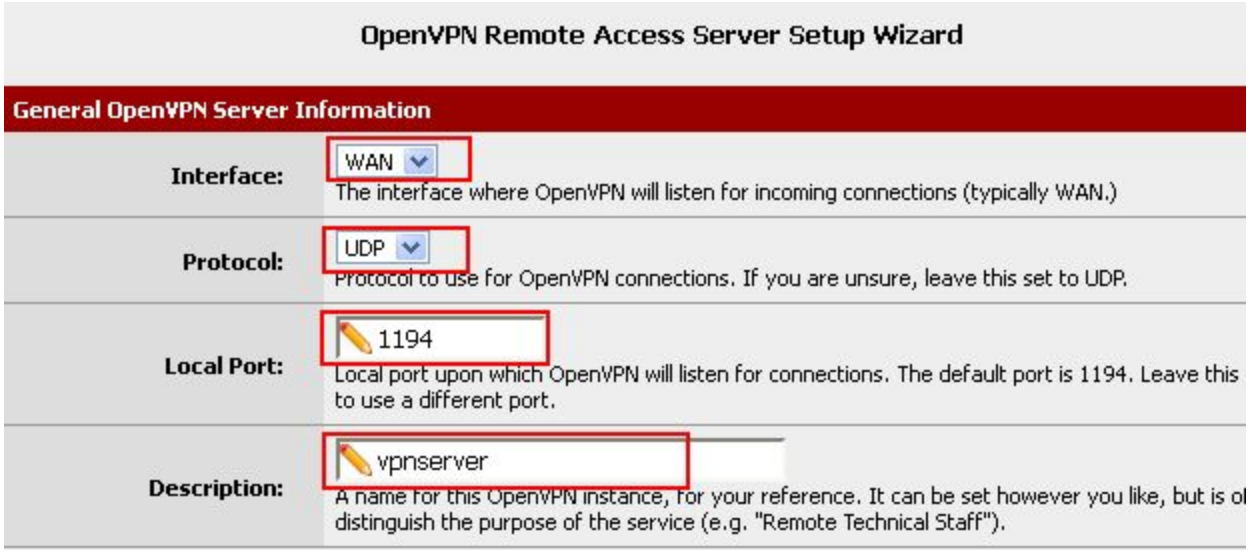
Nhập thông tin cho chứng chỉ

Descriptive name:	vpnserver
Country Code:	vn
State or Province:	hcm
City:	hcm
Organization:	nhatnghe

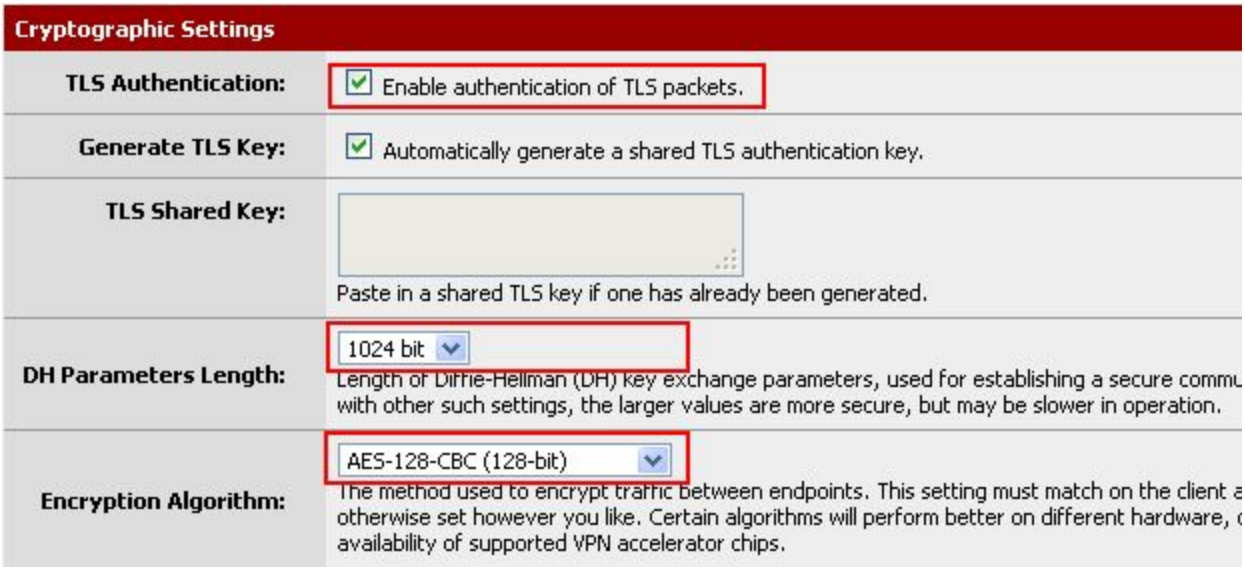
Nhấn **Create new Certificate**



B8. Cấu hình vpn
Chọn interface, giao thức, port cho kết nối VPN



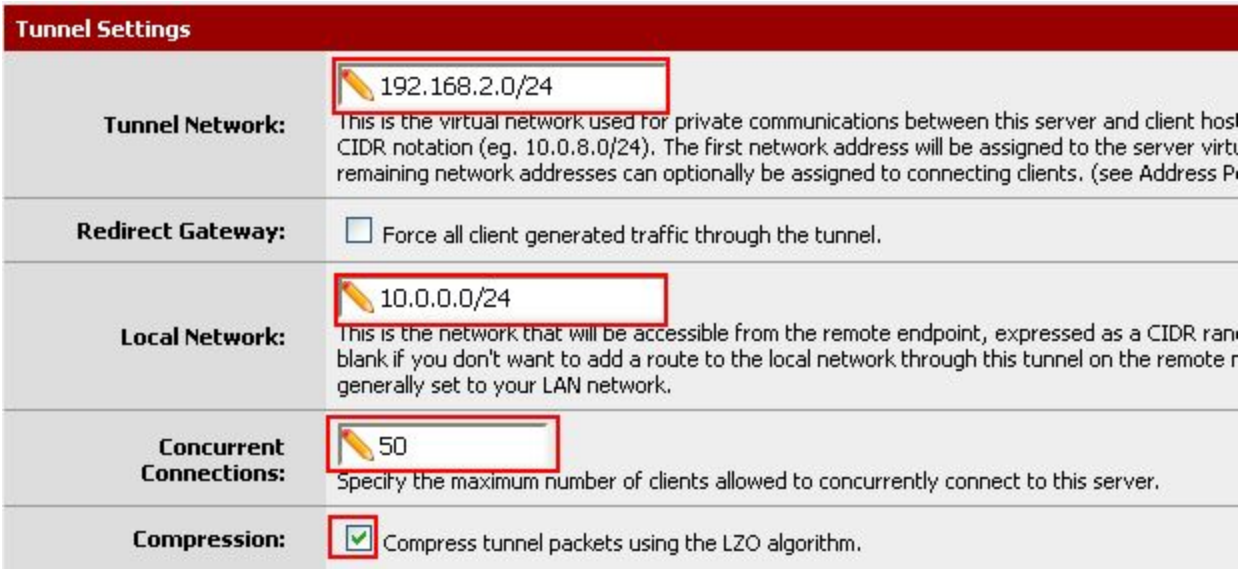
Chọn thuật toán mã hóa cho việc chứng thực và mã hóa data



Cấu hình tunnel:

Tunnel Network:	192.168.2.0/24	(vpn)
Local Network:	10.0.0.0/24	(internal network)
Concurrent Connections:	50	
Compression:	Check	

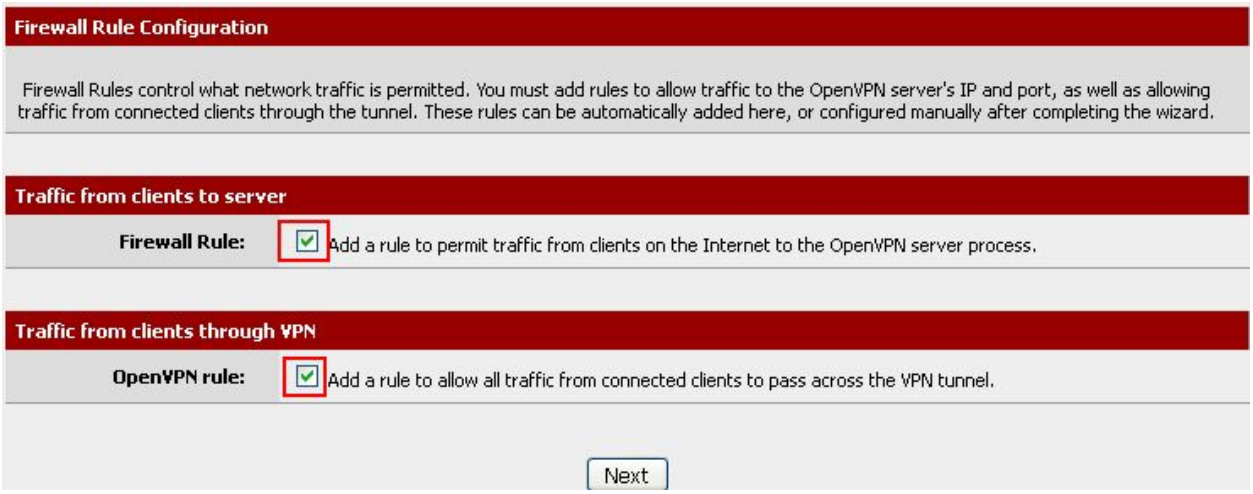
Nhấn **Next**



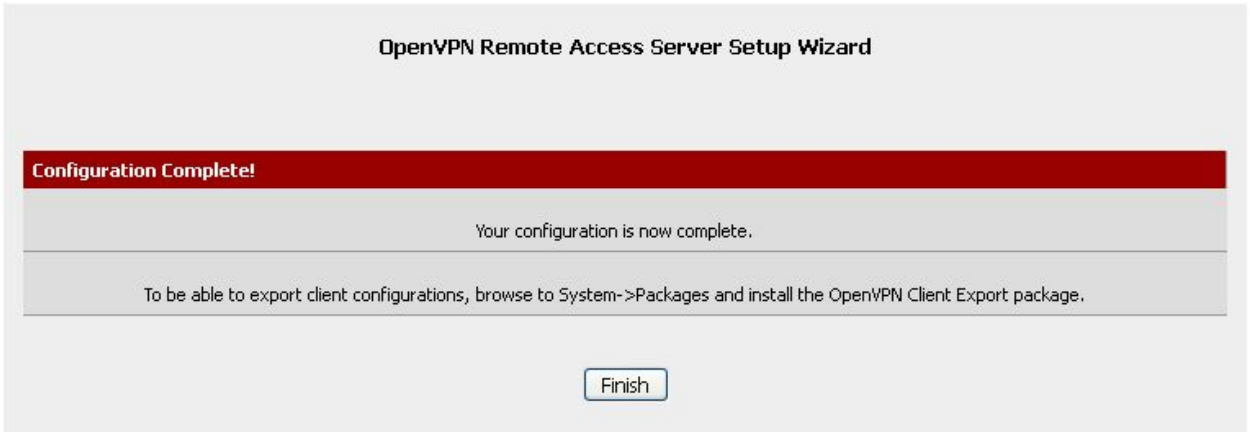
B9. Tạo rule cho phép liên lạc giữa mạng LAN và vpn client

Firewall Rule:	Check
OpenVPN rule:	Check

Nhấn **Next**



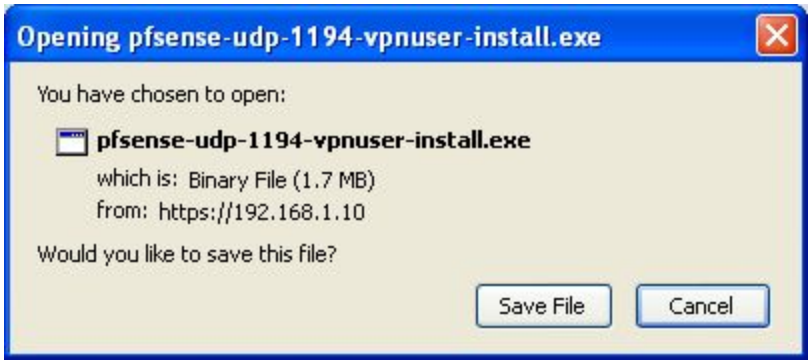
B10. Nhấn finish



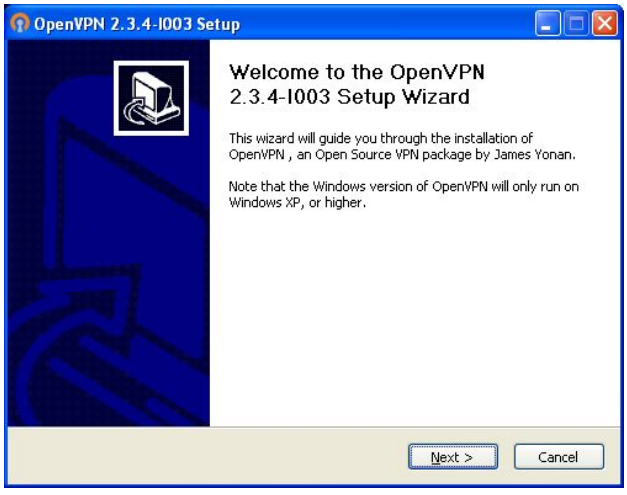
B11. Xuất file cài đặt và cấu hình cho client

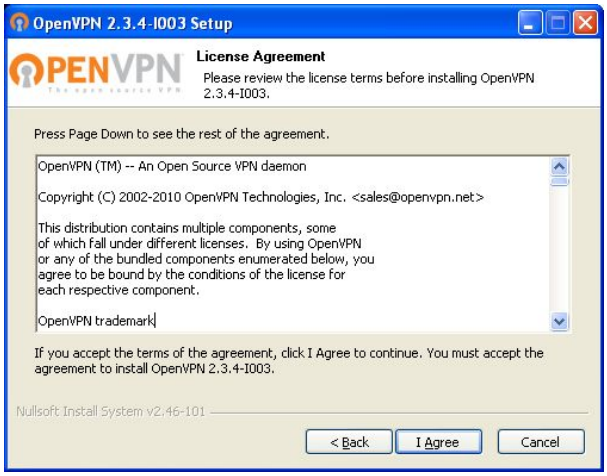
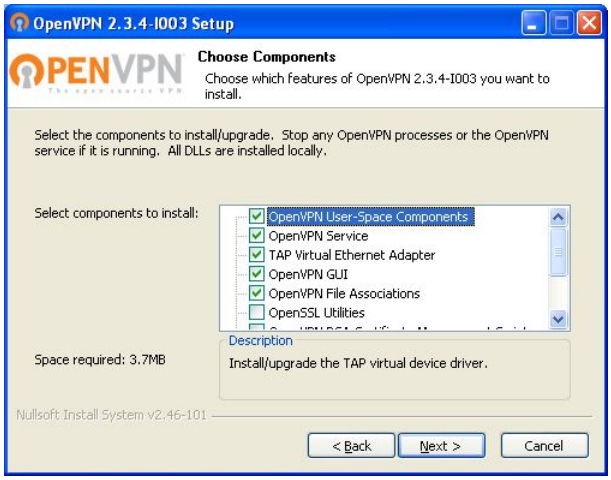
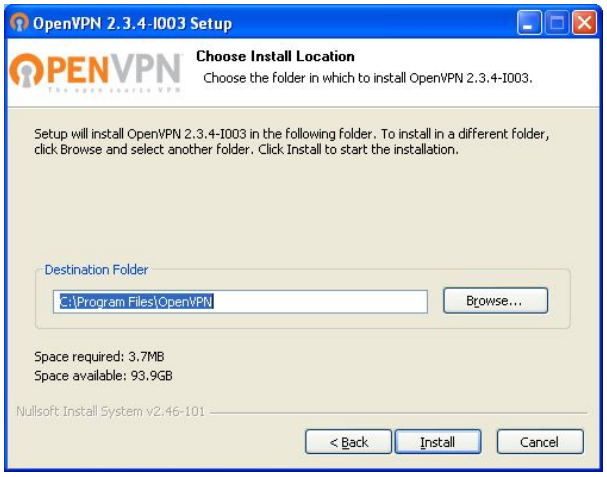
Chọn **2.3-x86**

Chọn **Save file**

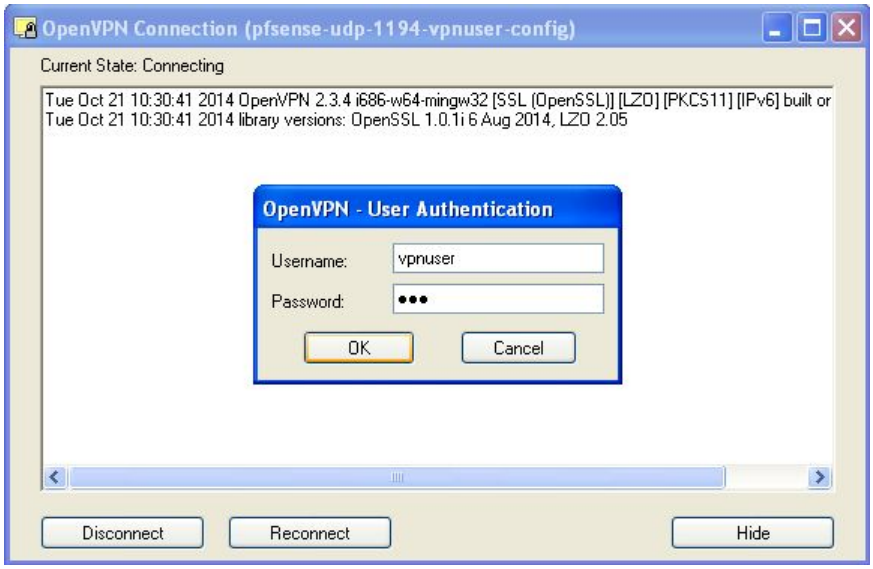


B12. Cài vpn client

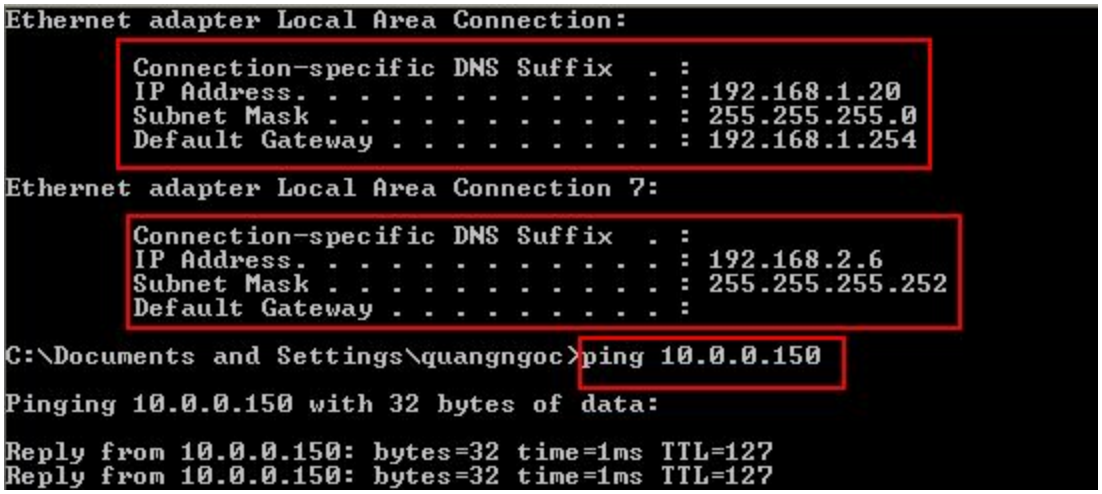
Thực thi file **pfsense-udp-1194-vpnuser-install.exe** vừa download 	Nhấn Next 

Chọn I Agree  	Nhấn Next 
Chọn Install  	Chọn continue Anyway 
Chọn start OpenVPN GUI Finish	

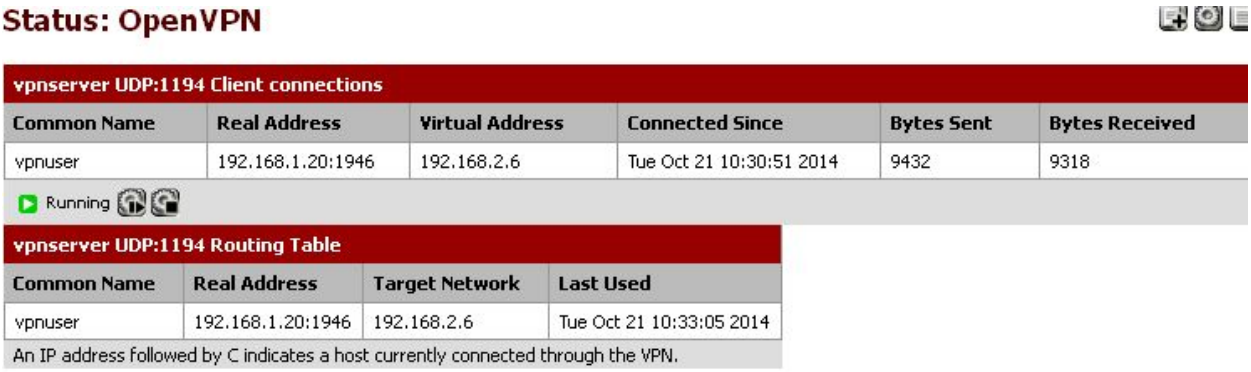
B13. kết nối VPN
Mở OpenVPN GUI, connect



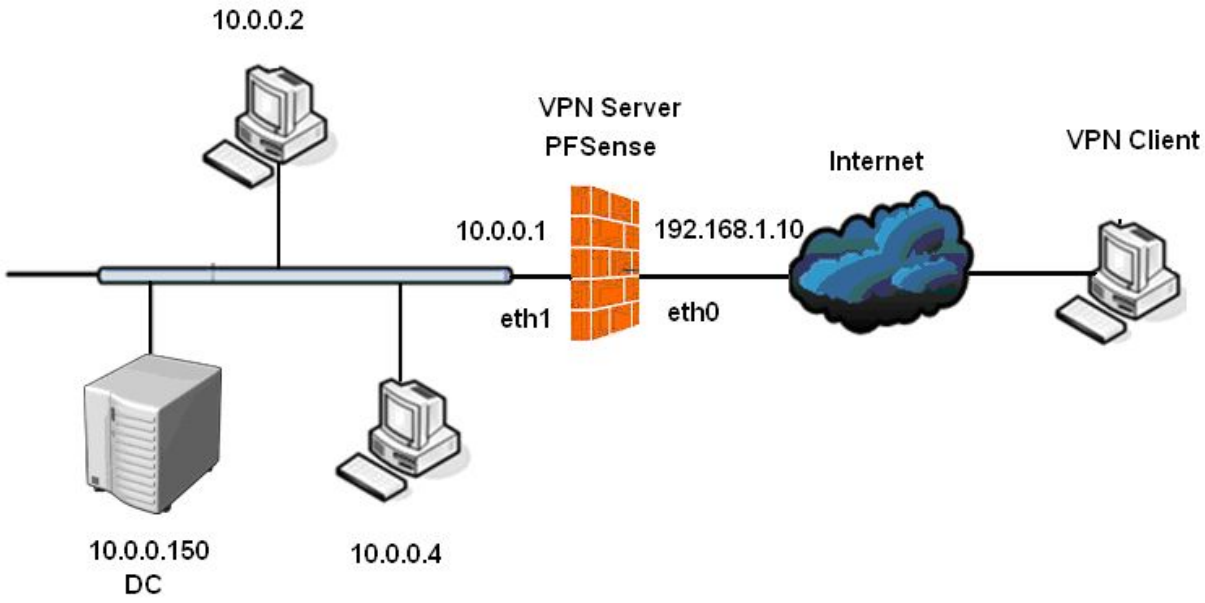
Kết nối thành công



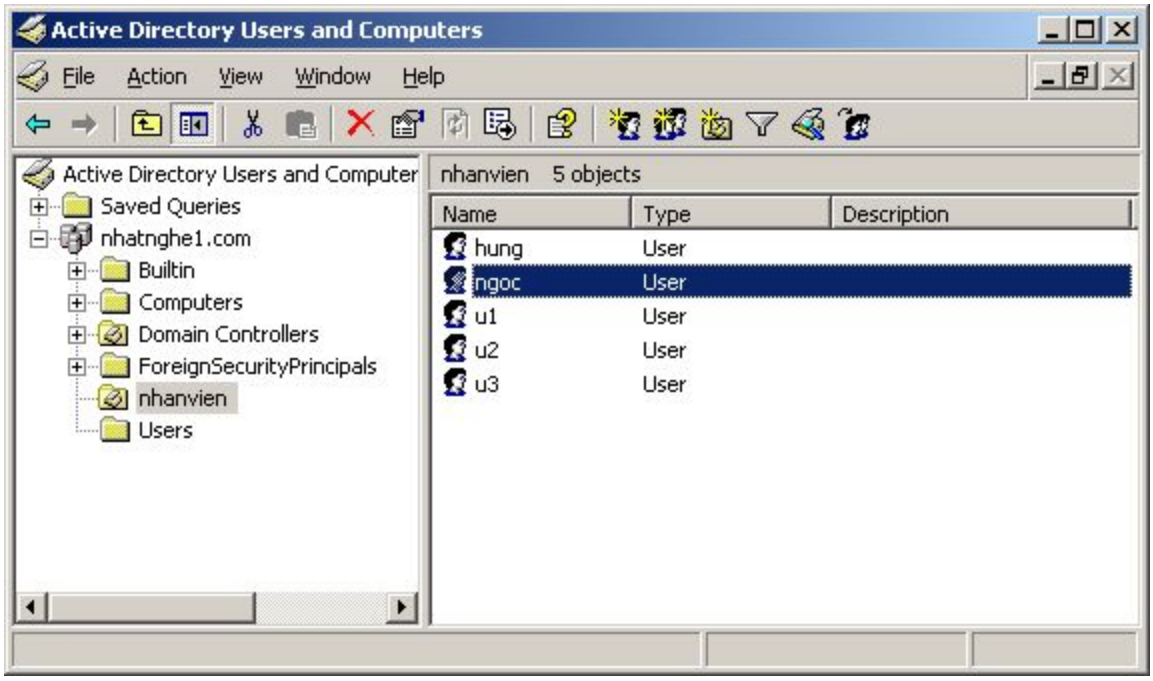
B14. Xem thông tin kết nối
Status, chọn **OpenVPN**



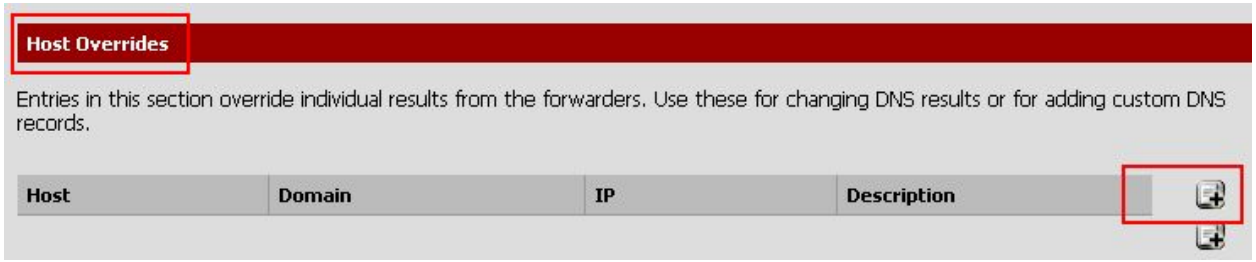
2. client to site - OpenVPN with TLS and AD User Authentication



B1. Trên máy DC tạo các user u1, u2, u3



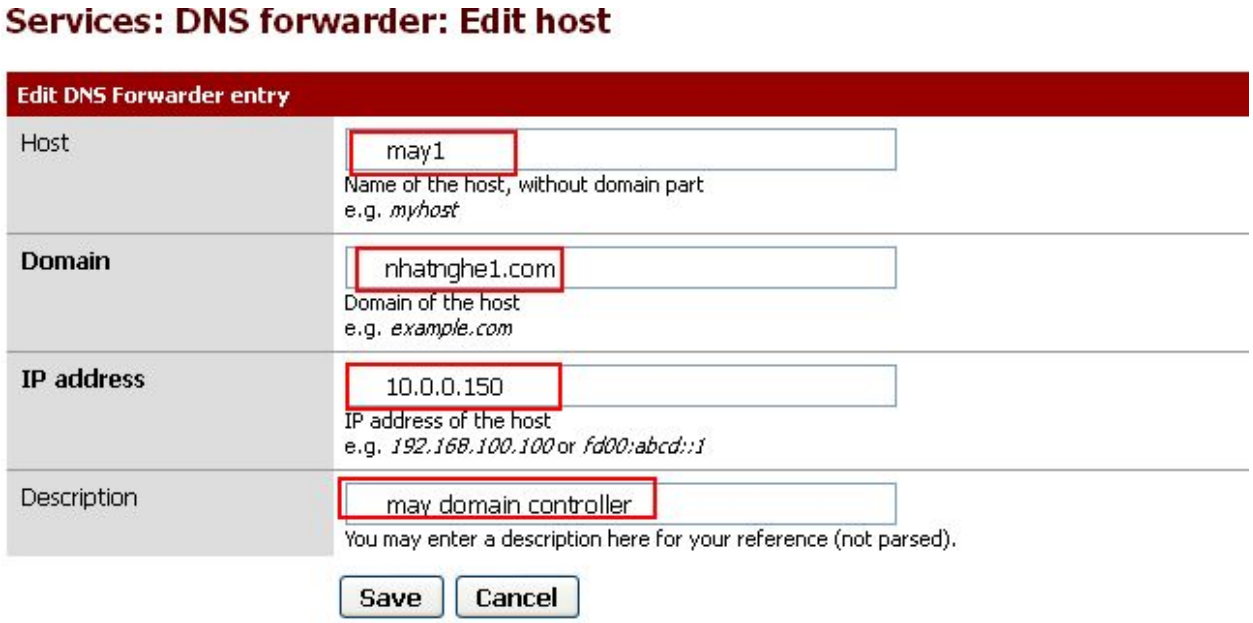
B2. Tạo DNS forwarder
Services, chọn DNS forwarder
Host Overrides, nhấn +



Nhập thông tin máy DC, domain:

Host	may1
Domain	nhatnghe1.com
IP address	10.0.0.150
Description	May domain controller

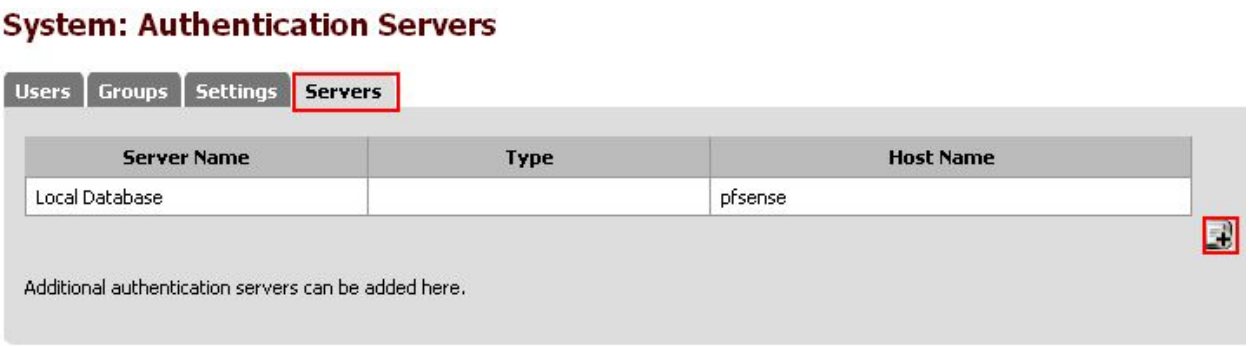
Chọn **Save**
Nhấn **Apply changes**



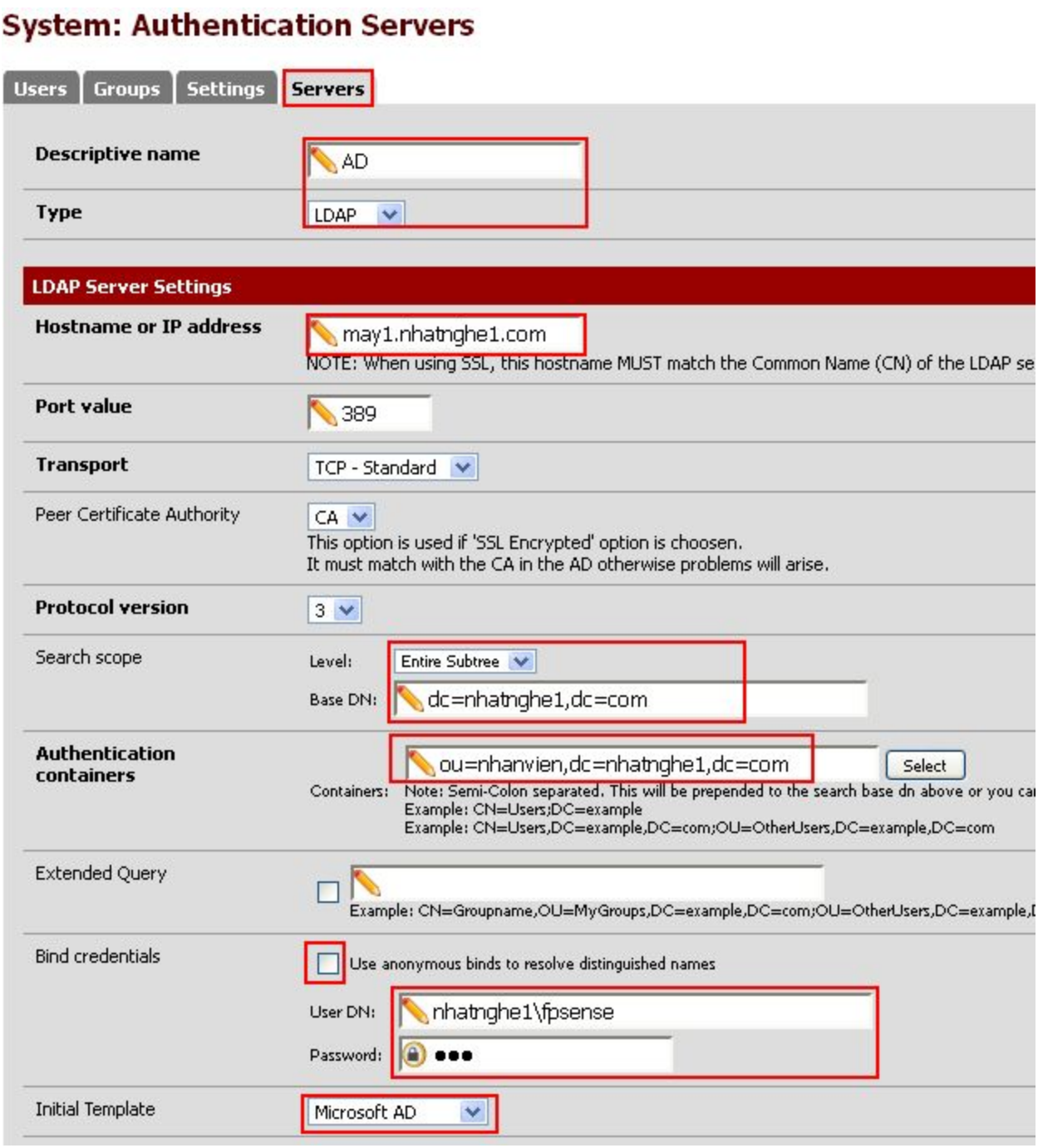
B3. Ping kiểm tra phân giải tên
Ping may1.nhatnghe1.com

```
Enter an option: 8

[2.1.5-RELEASE][root@pfsense.nhatnghe1.com]/root(1): ping may1.nhatnghe1.com
PING may1.nhatnghe1.com (10.0.0.150): 56 data bytes
64 bytes from 10.0.0.150: icmp_seq=0 ttl=128 time=3.091 ms
64 bytes from 10.0.0.150: icmp_seq=1 ttl=128 time=0.383 ms
64 bytes from 10.0.0.150: icmp_seq=2 ttl=128 time=0.383 ms
64 bytes from 10.0.0.150: icmp_seq=3 ttl=128 time=0.498 ms
64 bytes from 10.0.0.150: icmp_seq=4 ttl=128 time=0.383 ms
64 bytes from 10.0.0.150: icmp_seq=5 ttl=128 time=0.375 ms
```

B4. System, User Manager, chọn **Servers,** nhấn +



B5. Kết nối vối máy DC
Nhập các thông tin

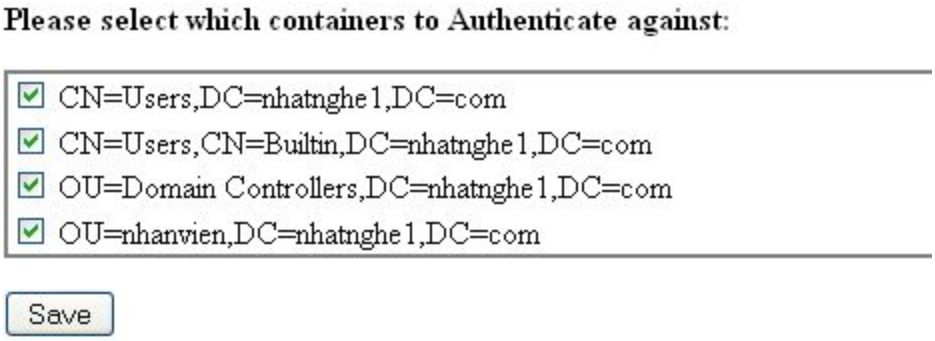


Descriptive name	DC
Type	Ldap
Hostname or IP address	may1.nhatnghe1.com (đã phân giải được tên)
Search scope	Level: Entire Subtree
	Base DN: dc=nhatnghe1,dc=com
Authentication containers	ou=nhanvien,dc=nhatnghe1,dc=com

Bind credentials bỏ check
User DN: nhatnghe1\fpsense (Tạo user fpsense ở cấp ngoài cùng của AD)
Password: 123

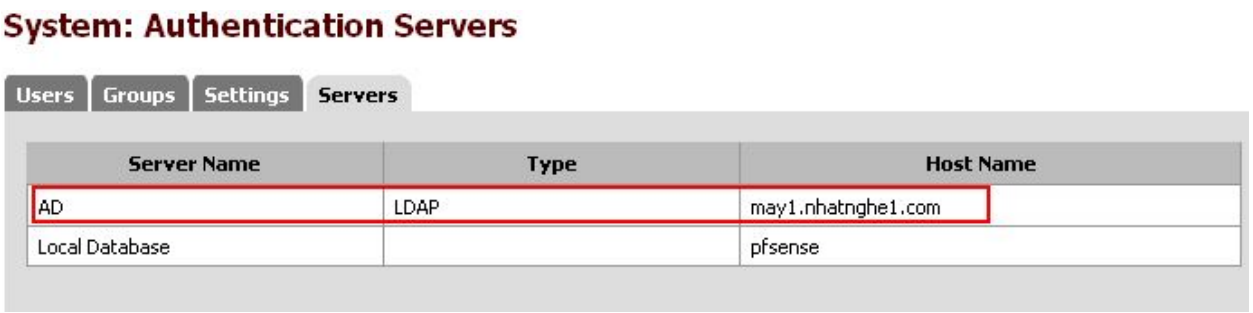
Initial Template: Microsoft AD

Nhấn select, chọn thêm các OU chứa các user cần chứng thực

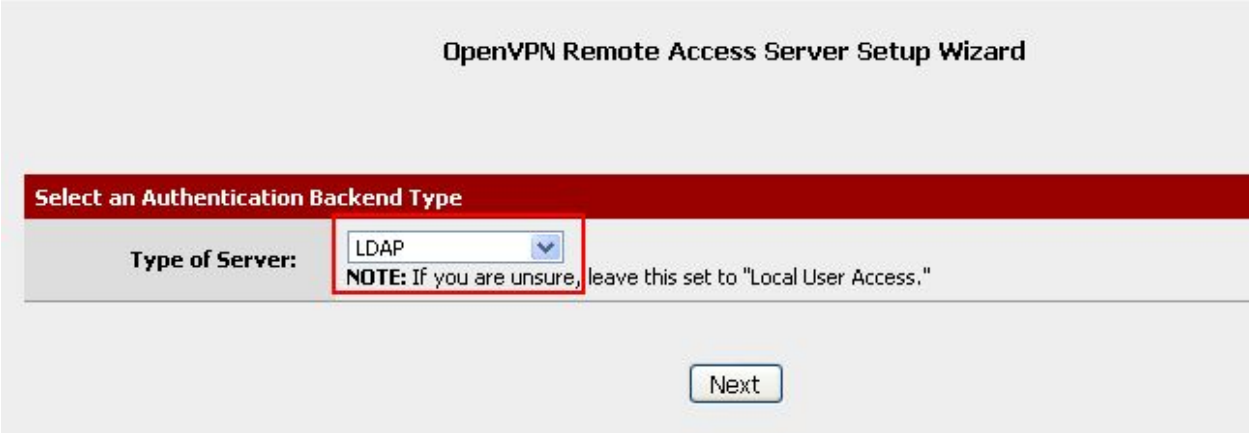


Chọn **Save**, **Save**

B6. Pfsense đã chứng thực được user từ DC



B7. Cấu hình openvpn
VPN, Openvpn, **wizard,** chọn **ldap, next**

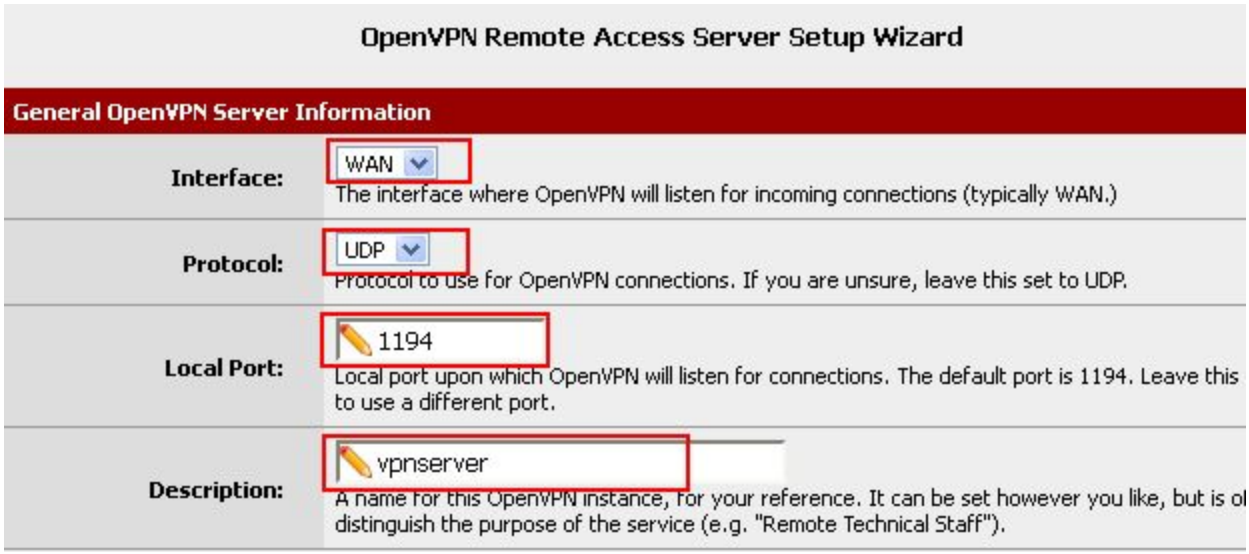


B8. chọn Ldap server, next

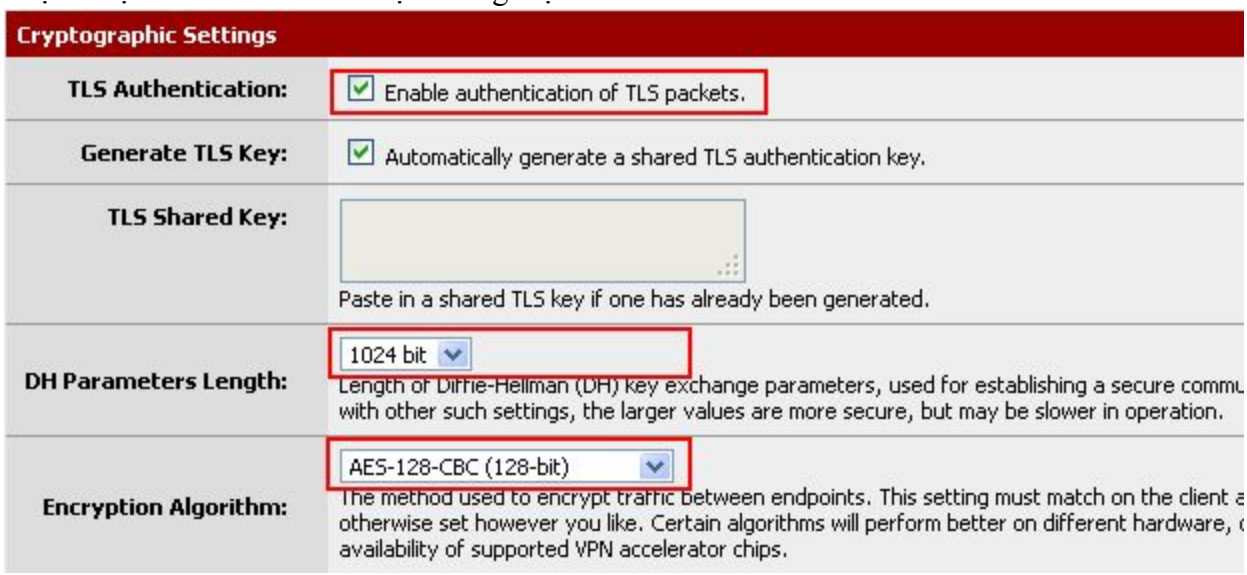
B9. Chọn hoặc tạo certificate cho vpnserver, next

B10. Chọn interface, giao thức, port cho kết nối VPN

(Chú ý: nếu đã tạo openvpn rồi thì phải đổi port 1194 thành port 1195)



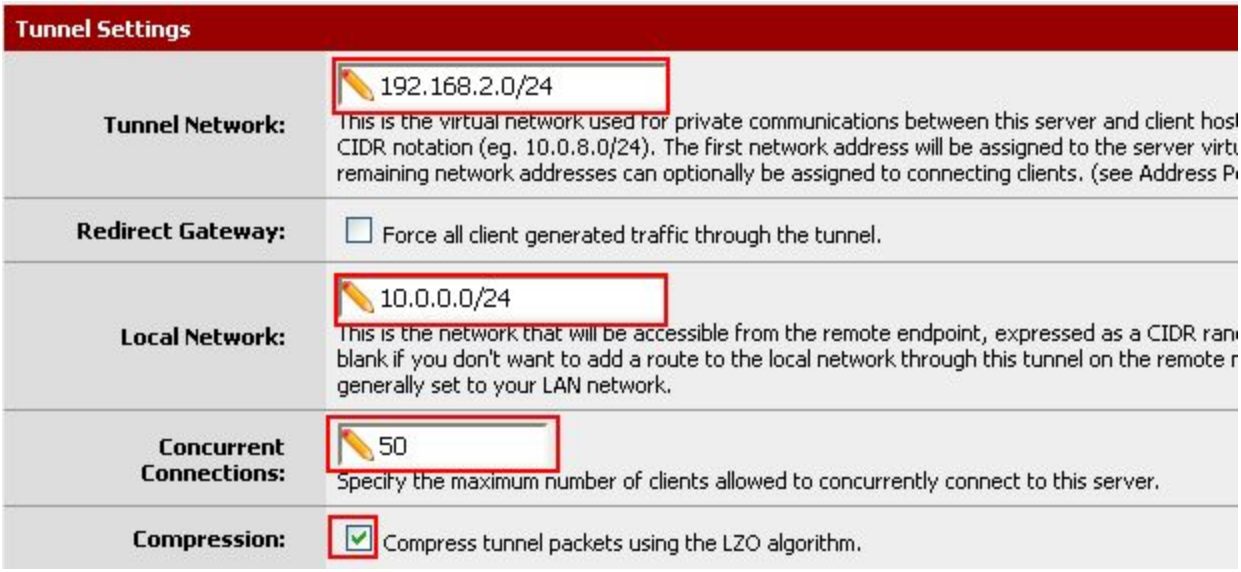
Chọn thuật toán mã hóa cho việc chứng thực và mã hóa data



Cấu hình tunnel:

Tunnel Network:	192.168.2.0/24	(vpn)
Local Network:	10.0.0.0/24	(internal network)
Concurrent Connections:	50	
Compression:	Check	

Nhấn **Next**



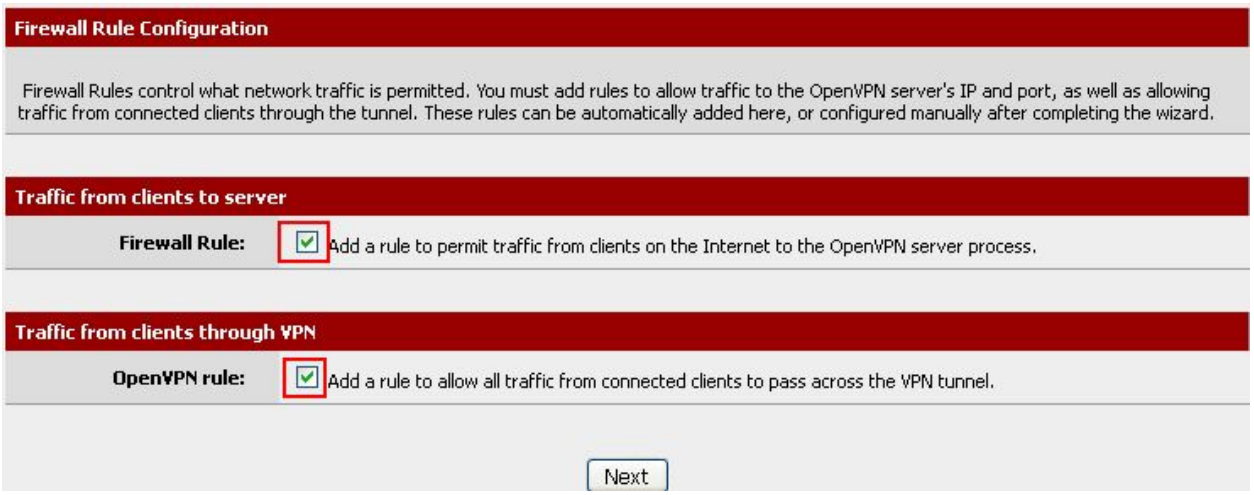
Chọn **Save**

B11**.** Tạo rule cho phép liên lạc giữa mạng LAN và vpn client

Firewall Rule: Check

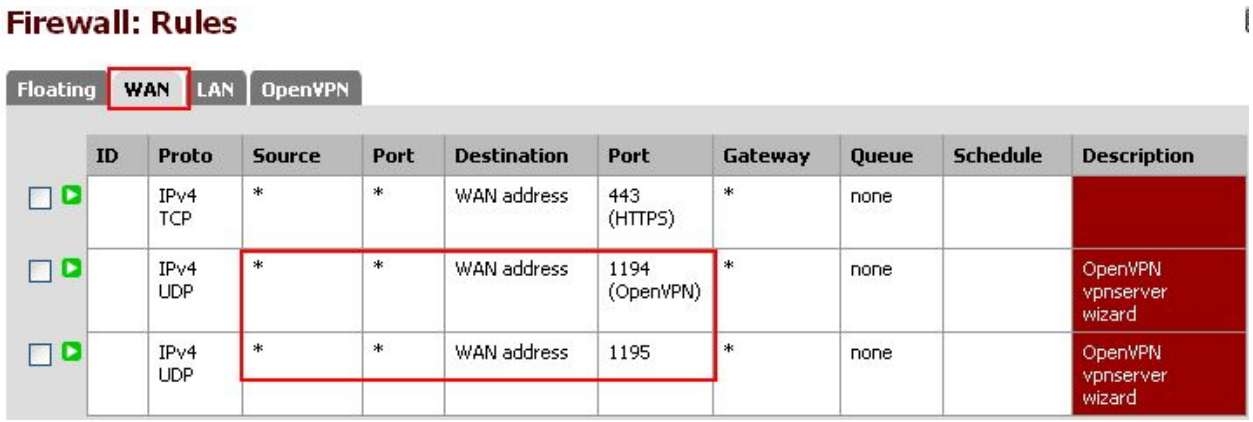
OpenVPN rule: Check

Nhấn **Next**

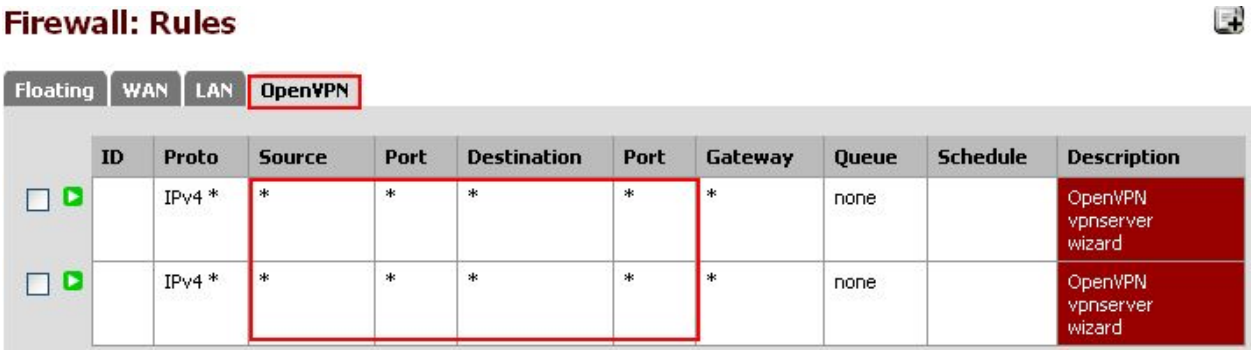


B12. Kết thúc

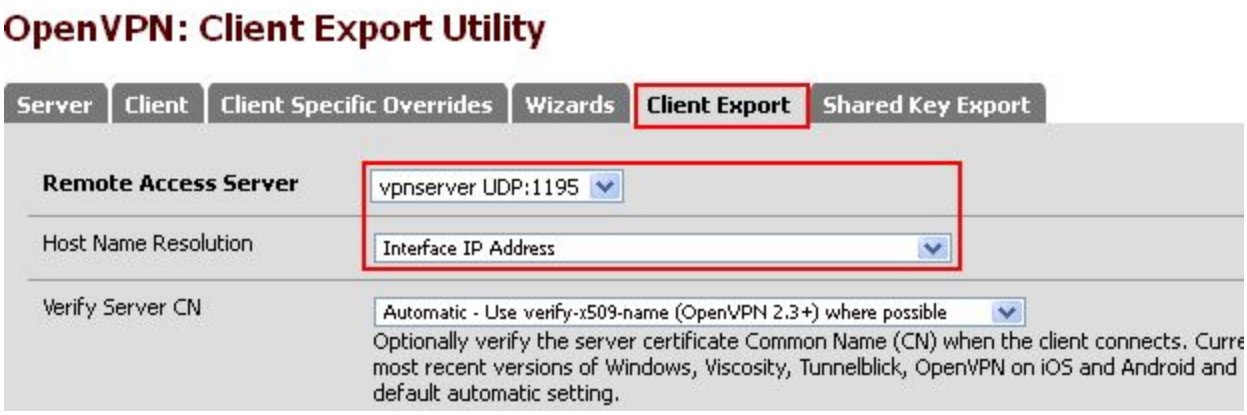
Quan sát các rule:
Firewall, chọn rule, chọn **WAN**



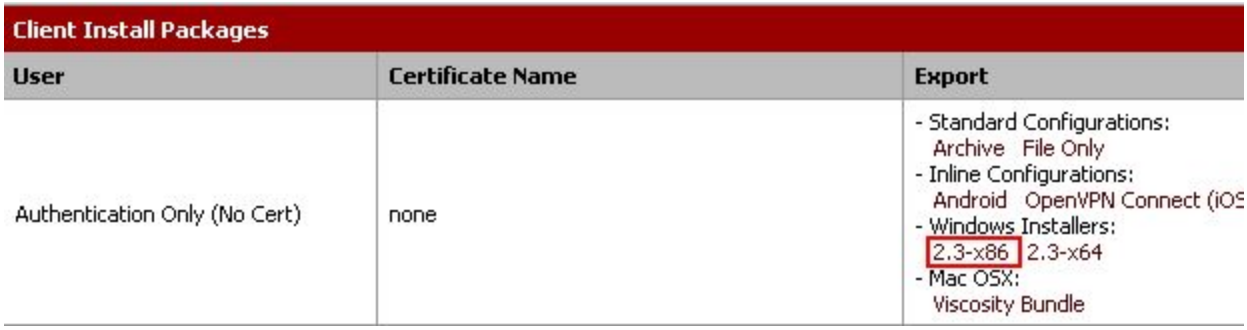
Firewall, chọn rule, chọn **OpenVPN**



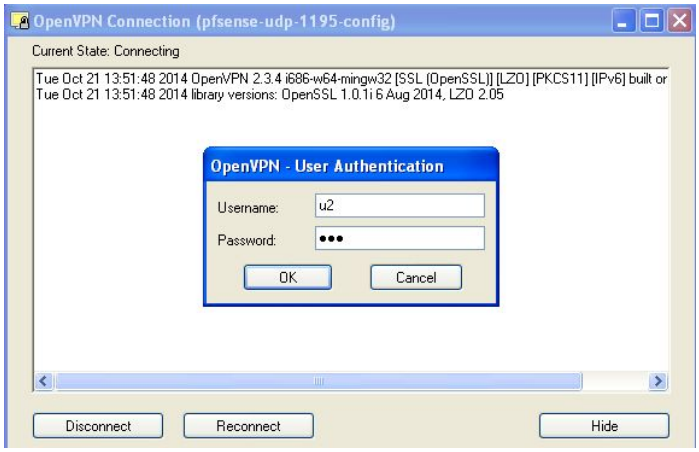
B13. Chọn client Export
Remote Access Server: Chọn **vpnserver UDP:1195**



Chọn **2.3-x68**, để download file cài đặt



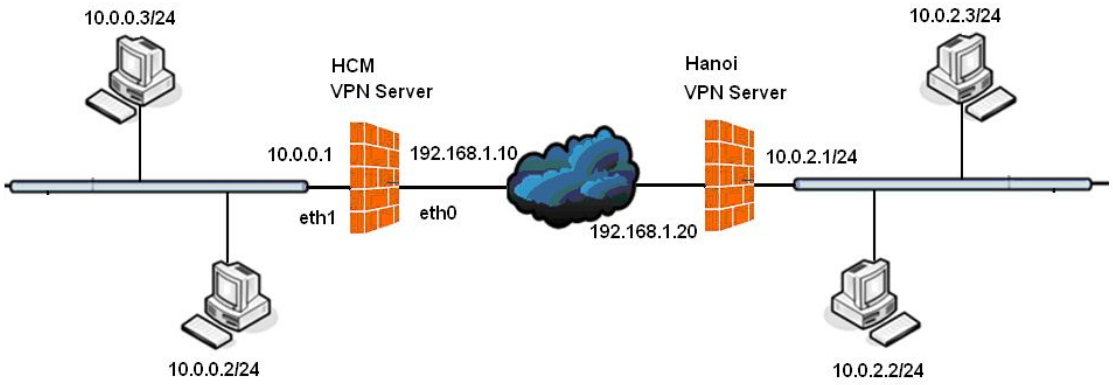
B14. Cài VPN client
Tại máy windows, chay file pfsense-udp-1195-install.exe
Tiến hành kết nới với user u2/123 từ AD



Kết nối thành công


OpenVPN GUI
Connected to: pfsense-udp-1195-config
Connected since: 10/21/2014 1:52 PM
Assigned IP: 192.168.2.6
INSTALL-win32.t...
1:53 PM

3. Site to site with with Shared key



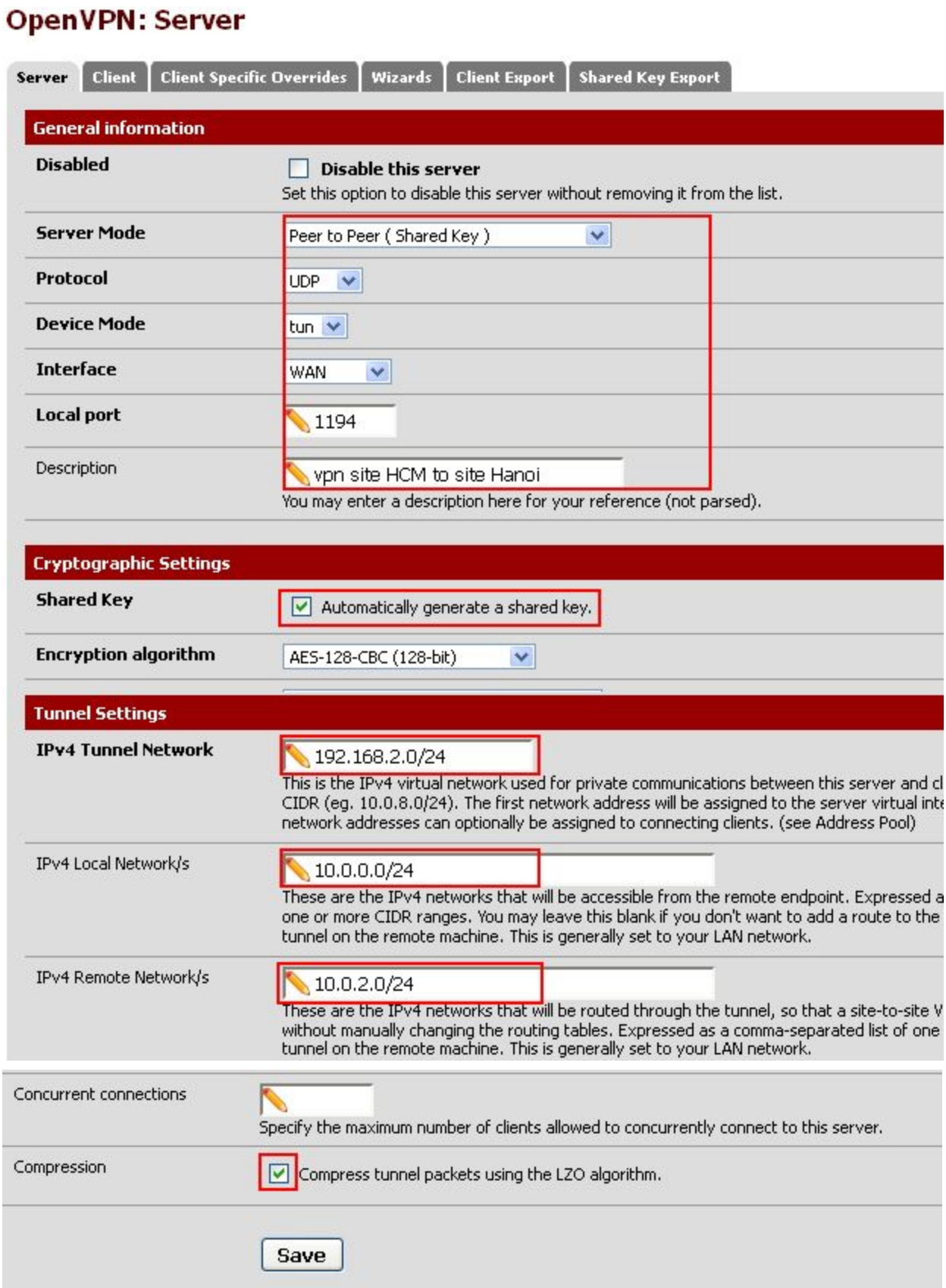
B1. tại site HCM

VPN**,** OpenVPN, server, nhấn +

Khai báo các tham số:

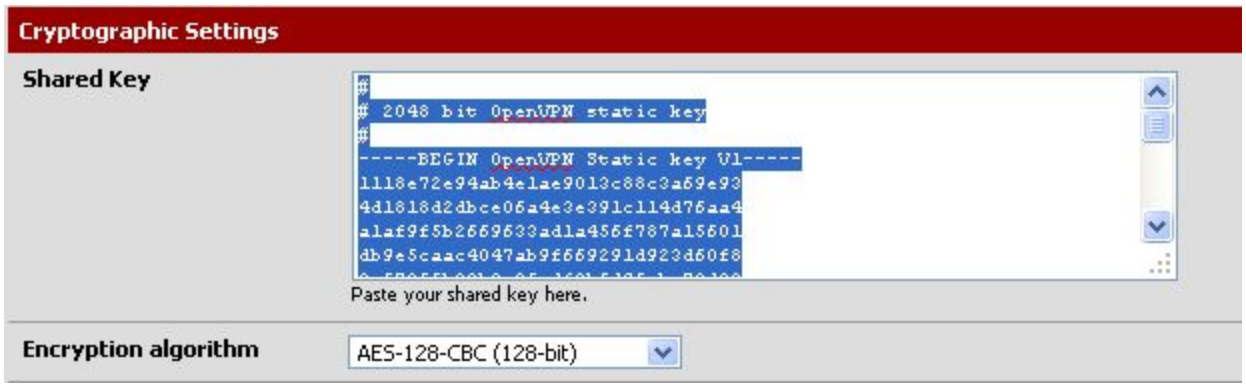
Server Mode	Peer to peer (Shared key)	
Protocol	UDP	
Device Mode	tun	
Local port	1194	
Description	vpn site HCM to site Hanoi	
Shared Key	check *Automatically generate a shared key.*	
IPv4 Tunnel Network	192.168.2.0/24	ip cho kết nối vpn
IPv4 Local Network/s	10.0.0.0/24	
IPv4 Remote Network/s	10.0.2.0/24	
Compression	check	

Chọn **Save**


OpenVPN: Server
Server
Client
Client Specific Overrides
Wizards
Client Export
Shared Key Export
General information
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Server Mode
Peer to Peer (Shared Key)
Protocol
UDP
Device Mode
tun
Interface
WAN
Local port
1194
Description
vpn site HCM to site Hanoi
You may enter a description here for your reference (not parsed).
Cryptographic Settings
Shared Key
Automatically generate a shared key.
Encryption algorithm
AES-128-CBC (128-bit)
Tunnel Settings
IPv4 Tunnel Network
192.168.2.0/24
This is the IPv4 virtual network used for private communications between this server and cl
CIDR (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual inte
network addresses can optionally be assigned to connecting clients. (see Address Pool)
IPv4 Local Network/s
10.0.0.0/24
These are the IPv4 networks that will be accessible from the remote endpoint. Expressed a
one or more CIDR ranges. You may leave this blank if you don't want to add a route to the
tunnel on the remote machine. This is generally set to your LAN network.
IPv4 Remote Network/s
10.0.2.0/24
These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site V
without manually changing the routing tables. Expressed as a comma-separated list of one
tunnel on the remote machine. This is generally set to your LAN network.
Concurrent connections
Specify the maximum number of clients allowed to concurrently connect to this server.
Compression
Compress tunnel packets using the LZO algorithm.
Save

B2. Chép key
Chọn edit

Shared Key: chọn và copy key này

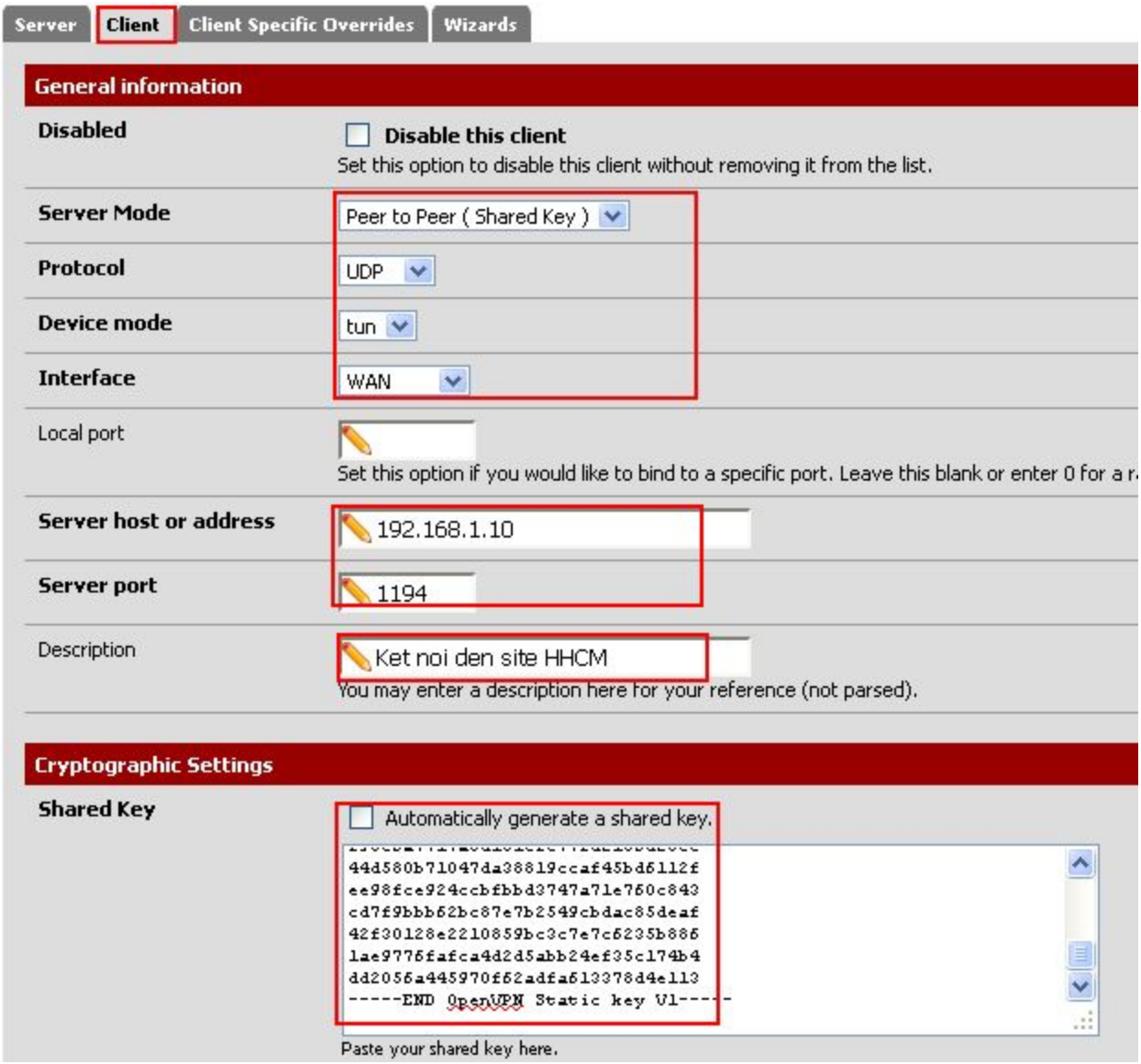


B3. Site Hanoi tạo kết nối VPN đến site HCM
Chọn thẻ Client, nhấn +

Khai báo các tham số:

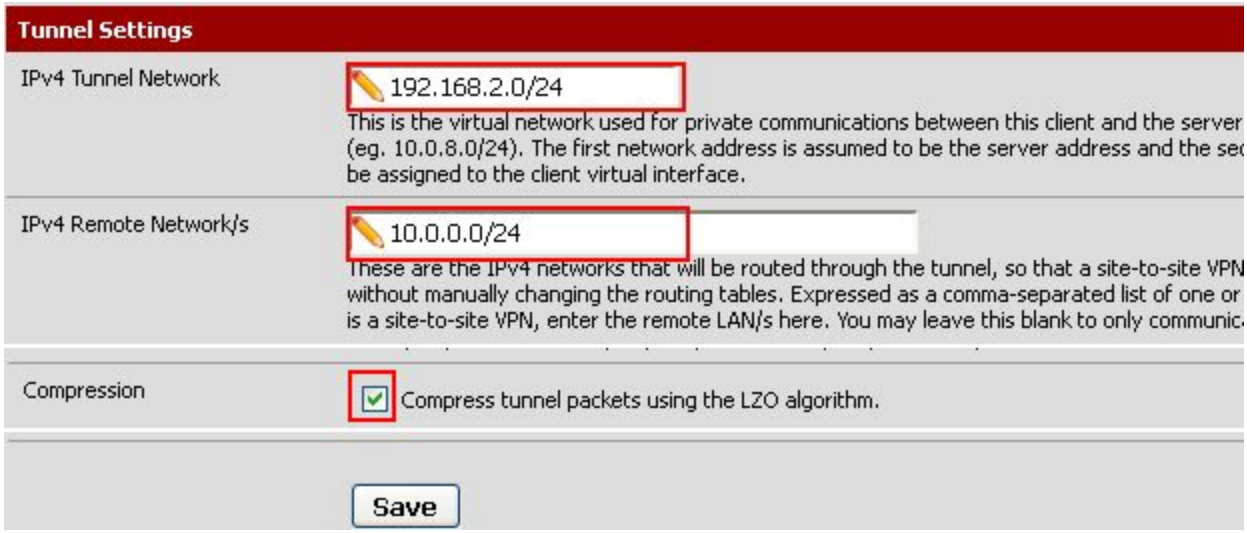
Server Mode	Peer to peer (Shared key)
Protocol	UDP
Device mode	tun
Server host or address	192.168.1.10

Server port	1194
Description	Ket noi den site HHCM
Shared Key	bỏ check *Automatically generate a shared key.* Dán nội dung key tạo ở site HCM

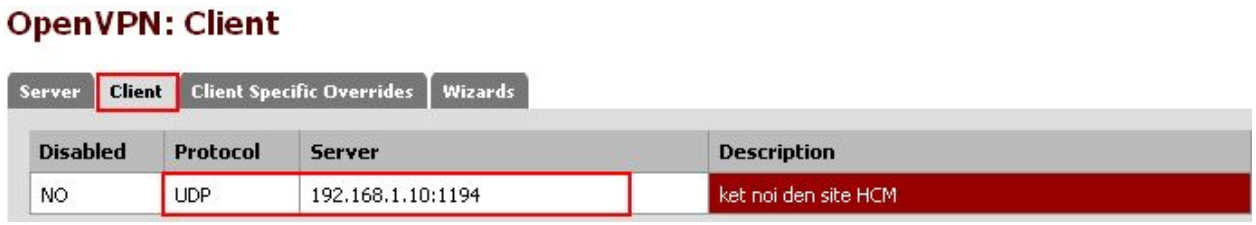


IPv4 Tunnel Network	192.168.2.0/24	ip cho kết nối vpn
IPv4 Remote Network/s	10.0.0.0/24	
Compression	check	

Chọn **Save**

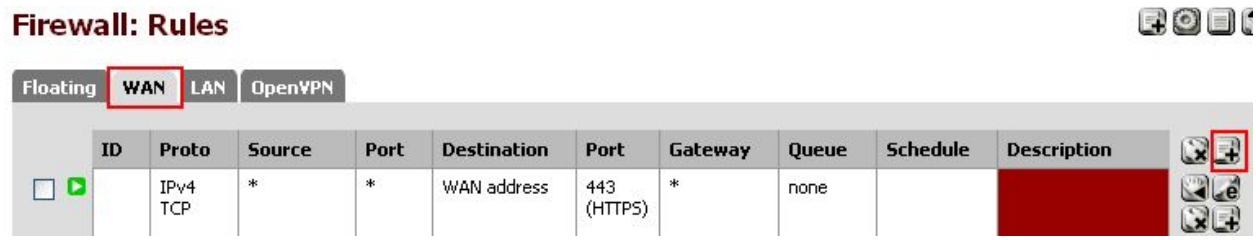


Kết nối VPN được tạo



B4. Site HCM - Tạo rule

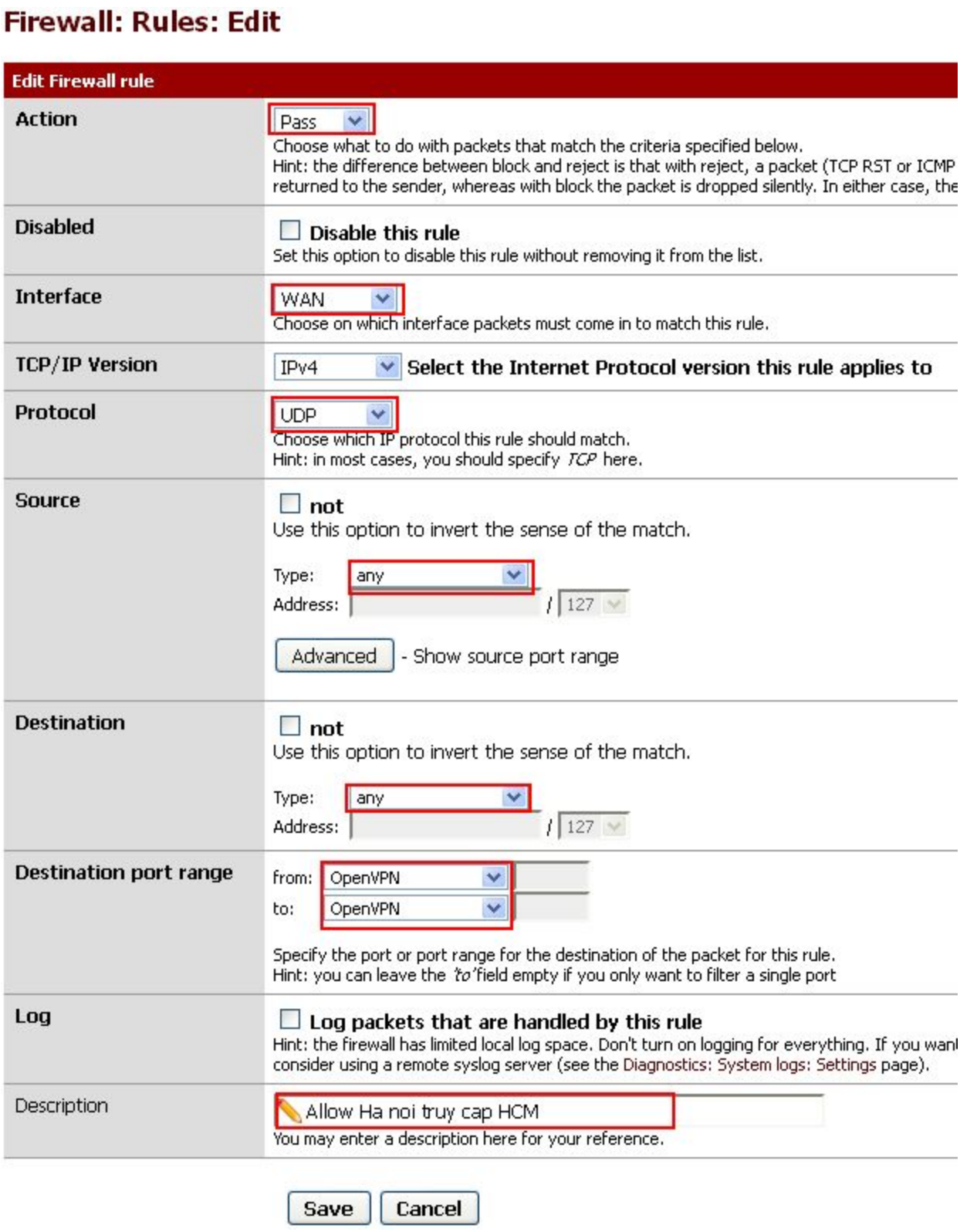
Firewall, Rules, chọn WAN, nhấn +



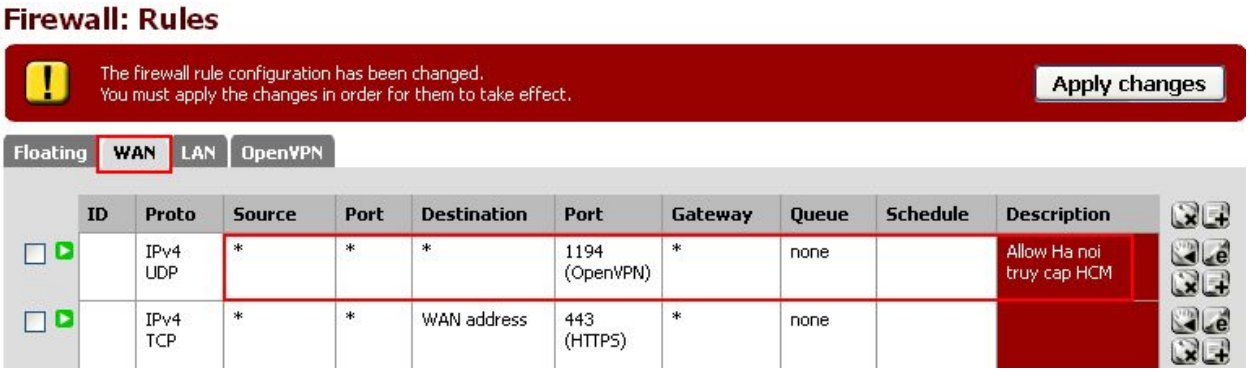
Khai báo các tham số:

Action	Pass
Interface	WAN
Protocol	**UDP**
Source	any
Destination	any
Destination port range	**OpenVPN**
Description	Allow Ha noi truy cap HCM

Chọn **Save**

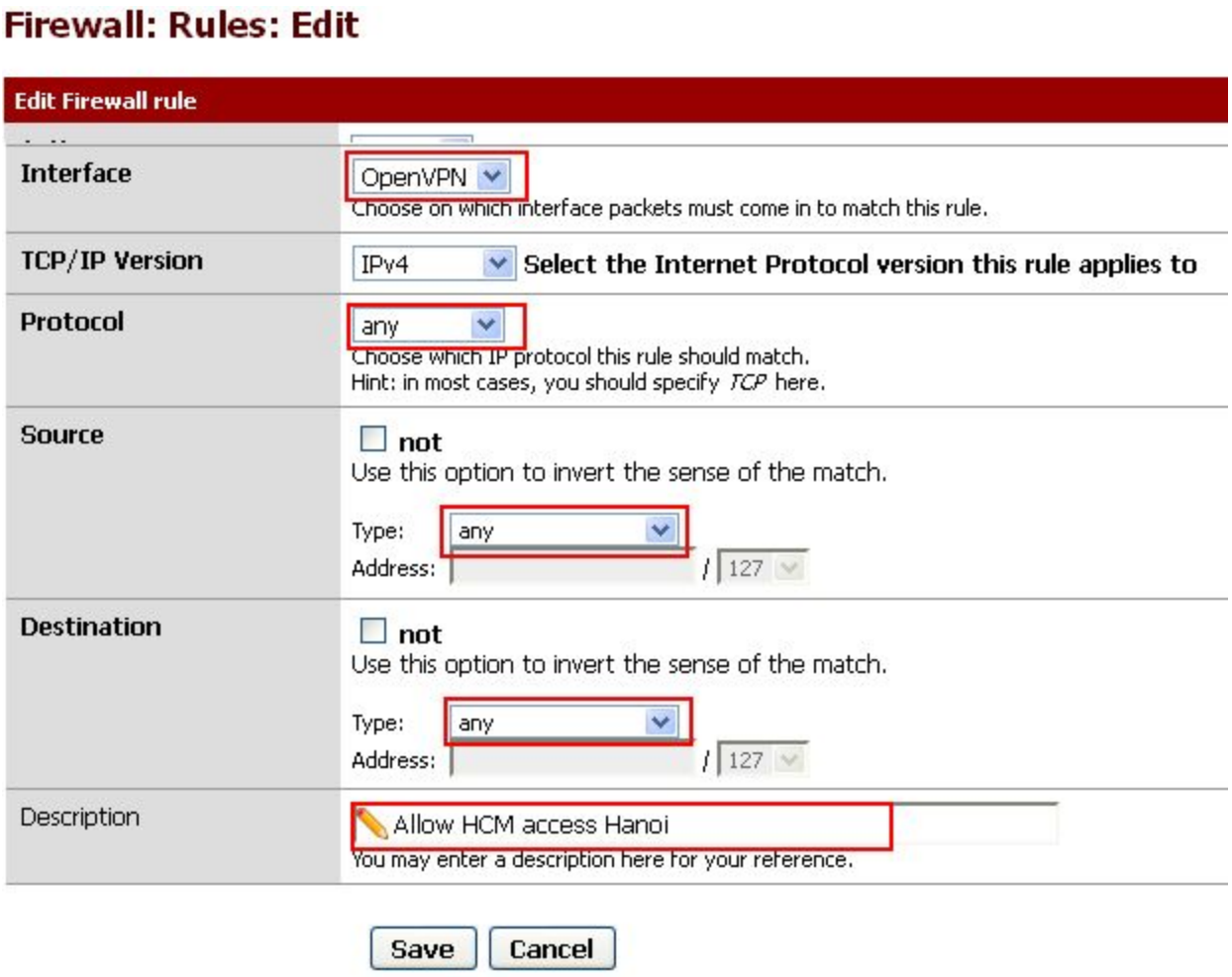


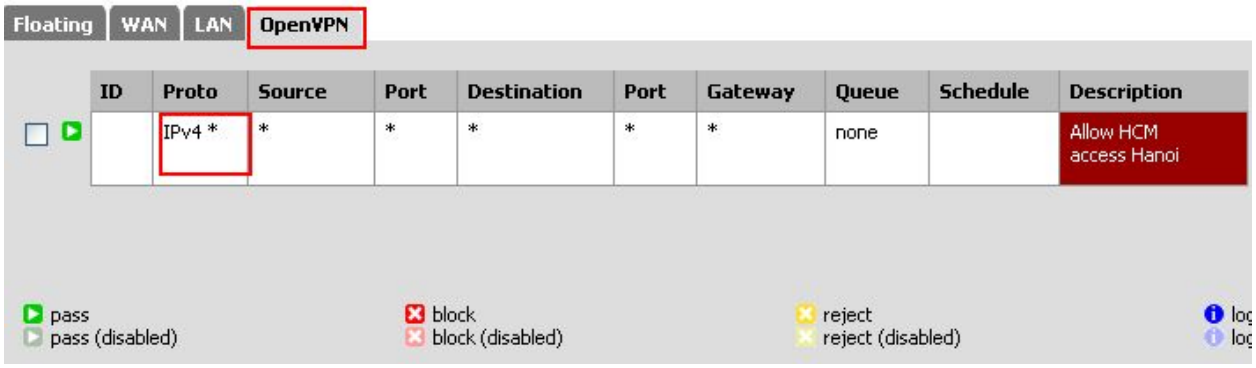
Nhấn **Apply changes**



B5. Tương tự tạo rule trên tab OpenVPN:

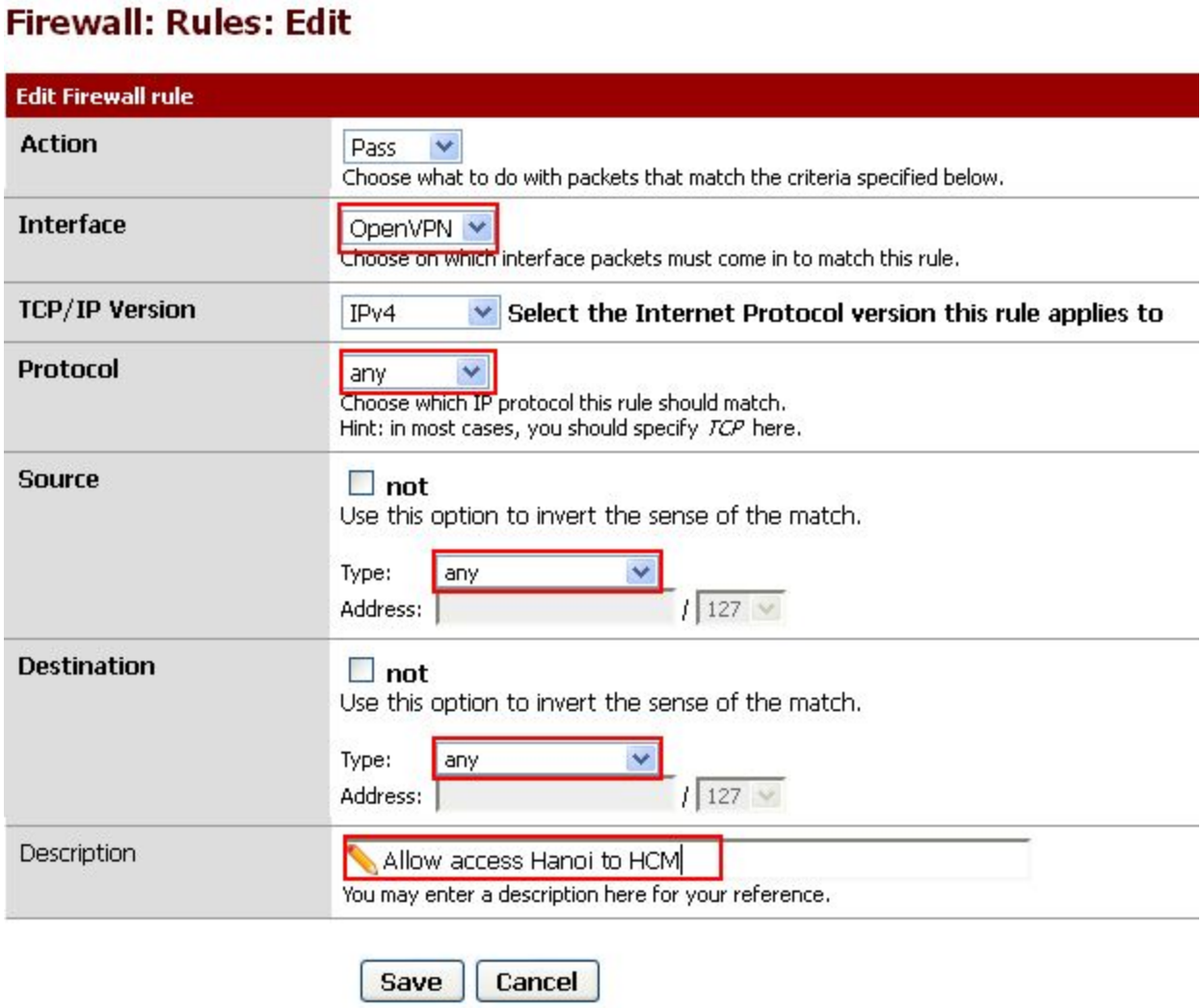
Interface OpenVPN
Protocol any
Source any
Destination any
Description Allow HCM access Hanoi



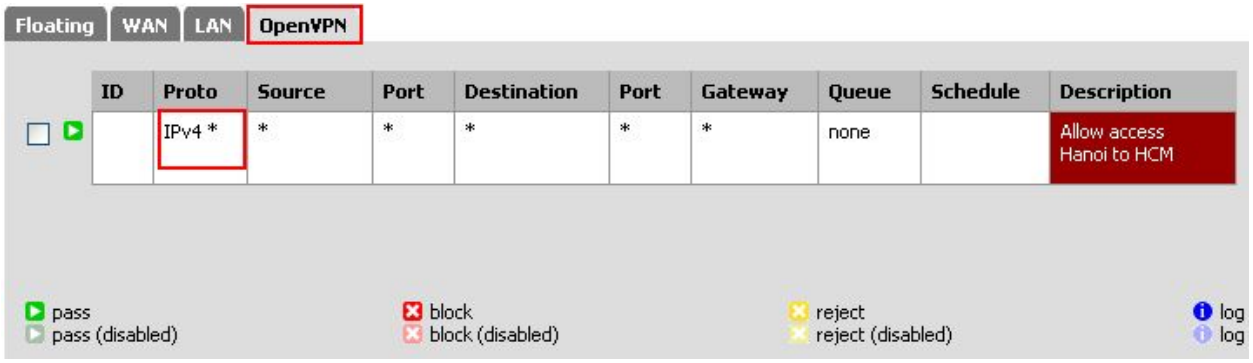


B7. Site Hanoi tạo rule trên tab OpenVPN:

Interface	OpenVPN
Protocol	any
Source	any
Destination	any
Description	Allow access Hanoi to HCM



Rule đã được tạo



B8. Kiểm tra

Tại site HCM: Status, OpenVPN

Status: OpenVPN

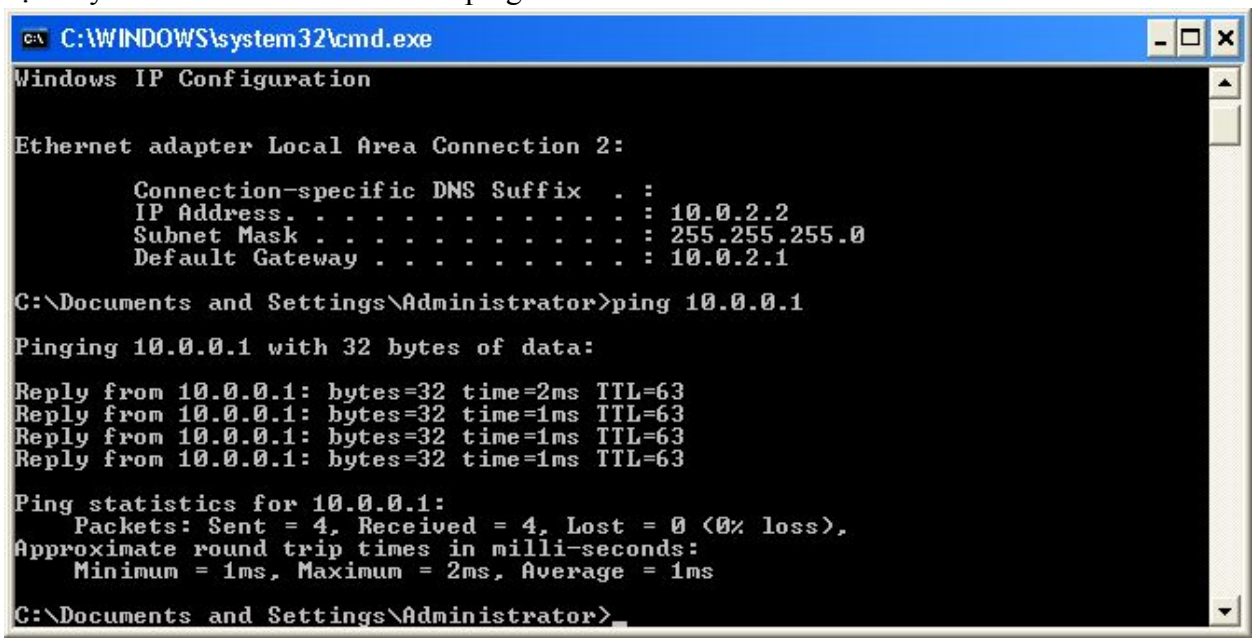
Peer to Peer Server Instance Statistics							
Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
vpn site HCM to site Hanoi UDP:1194	up	Thu Oct 23 9:00:06 2014	192.168.2.1	192.168.1.20	160316	179656	

Tại site Hanoi: Status, OpenVPN

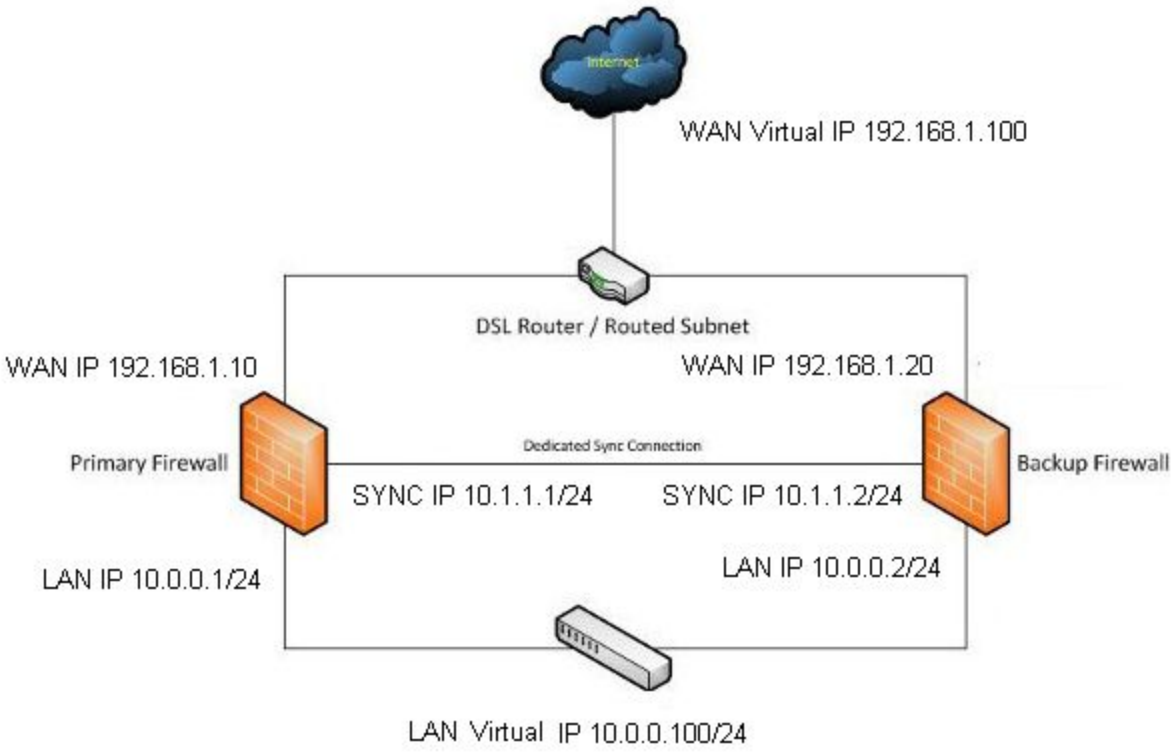
Status: OpenVPN

Client Instance Statistics							
Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
Ket noi den site HHCM UDP	up	Thu Oct 23 9:26:37 2014	192.168.2.2	192.168.1.10	2816	2332	

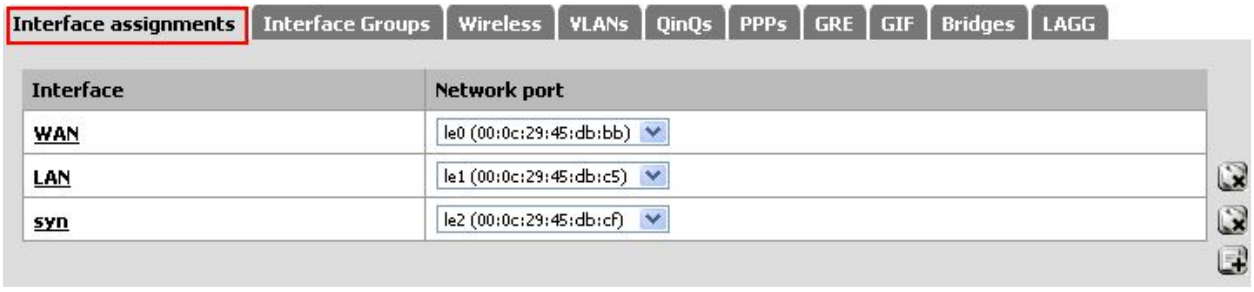
Tại máy PC 10.0.2.2 bên site Hanoi ping 10.0.0.1 bên site HCM



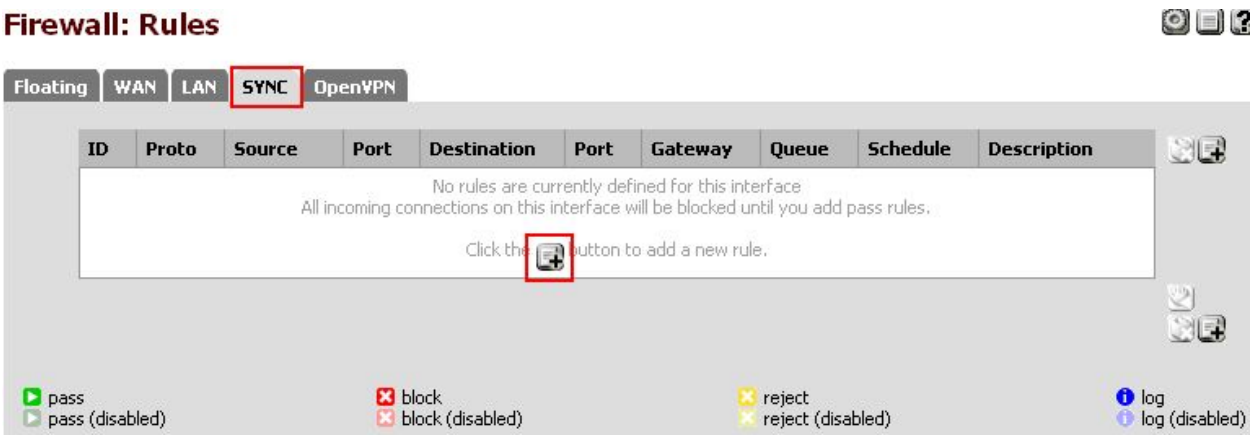
Pfsense Cluster Using CARP



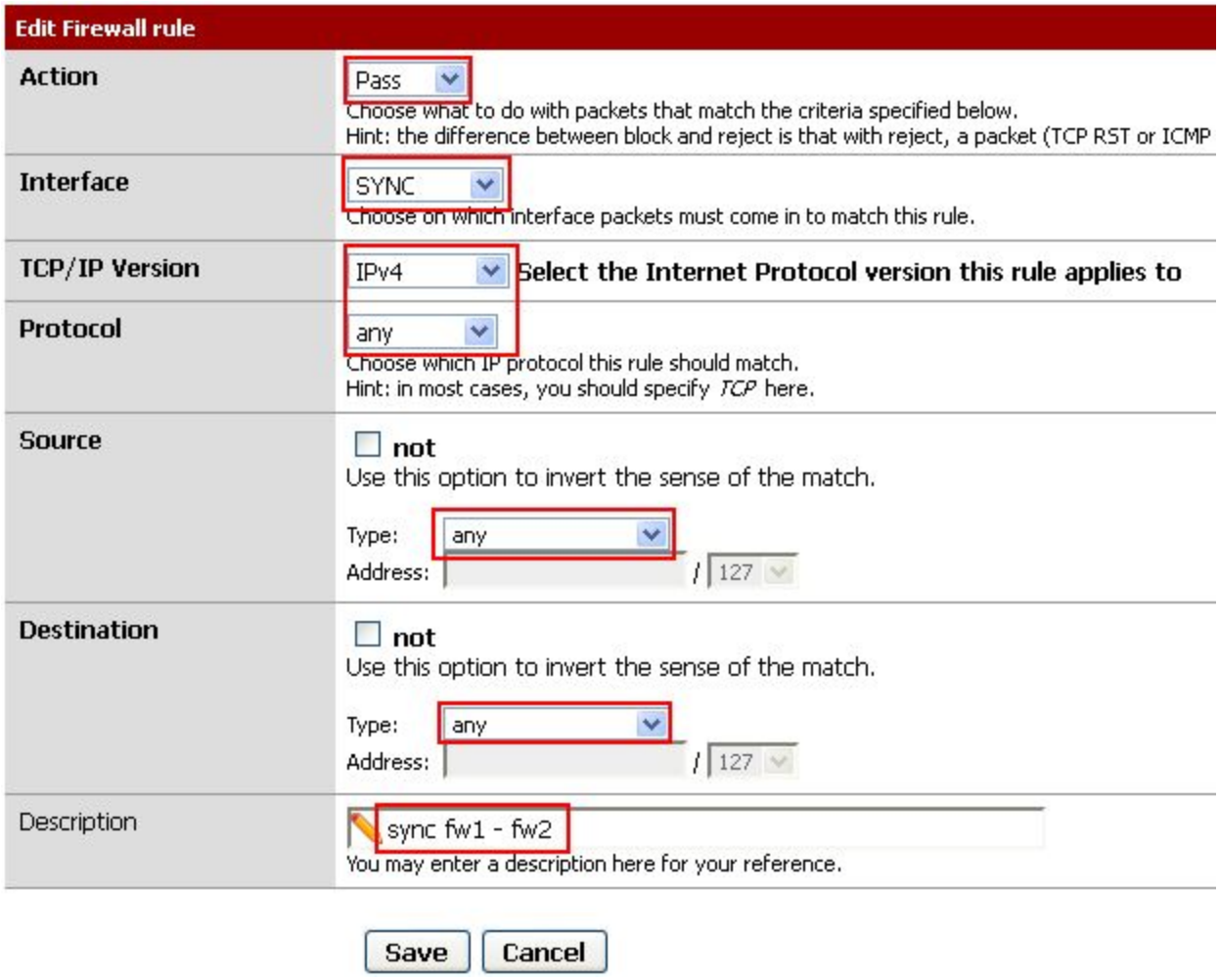
Chuẩn bị: Đặt IP theo sơ đồ
Chú ý: 2 fw phải dùng cùng giao thức http hoặc https
B1. Đặt tên, IP cho LAN card trên 2 firewall
Interfaces, Assign, Chọn edit, đặt IP cho cac LAN card



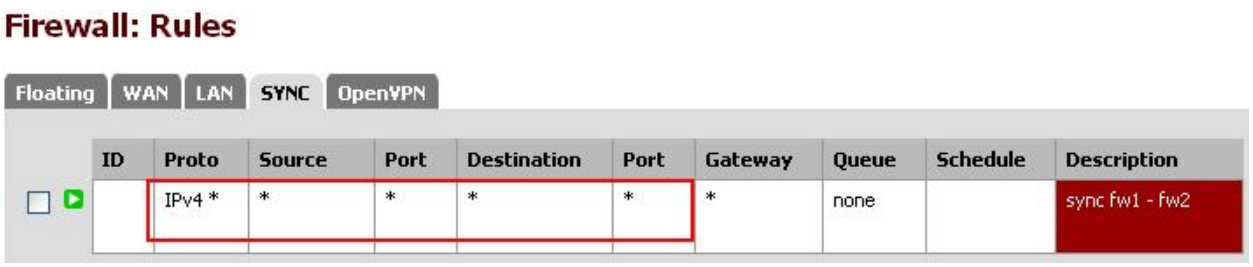
B2. Tạo rule trên 2 firewall
Firewall, Rules, nhấn +



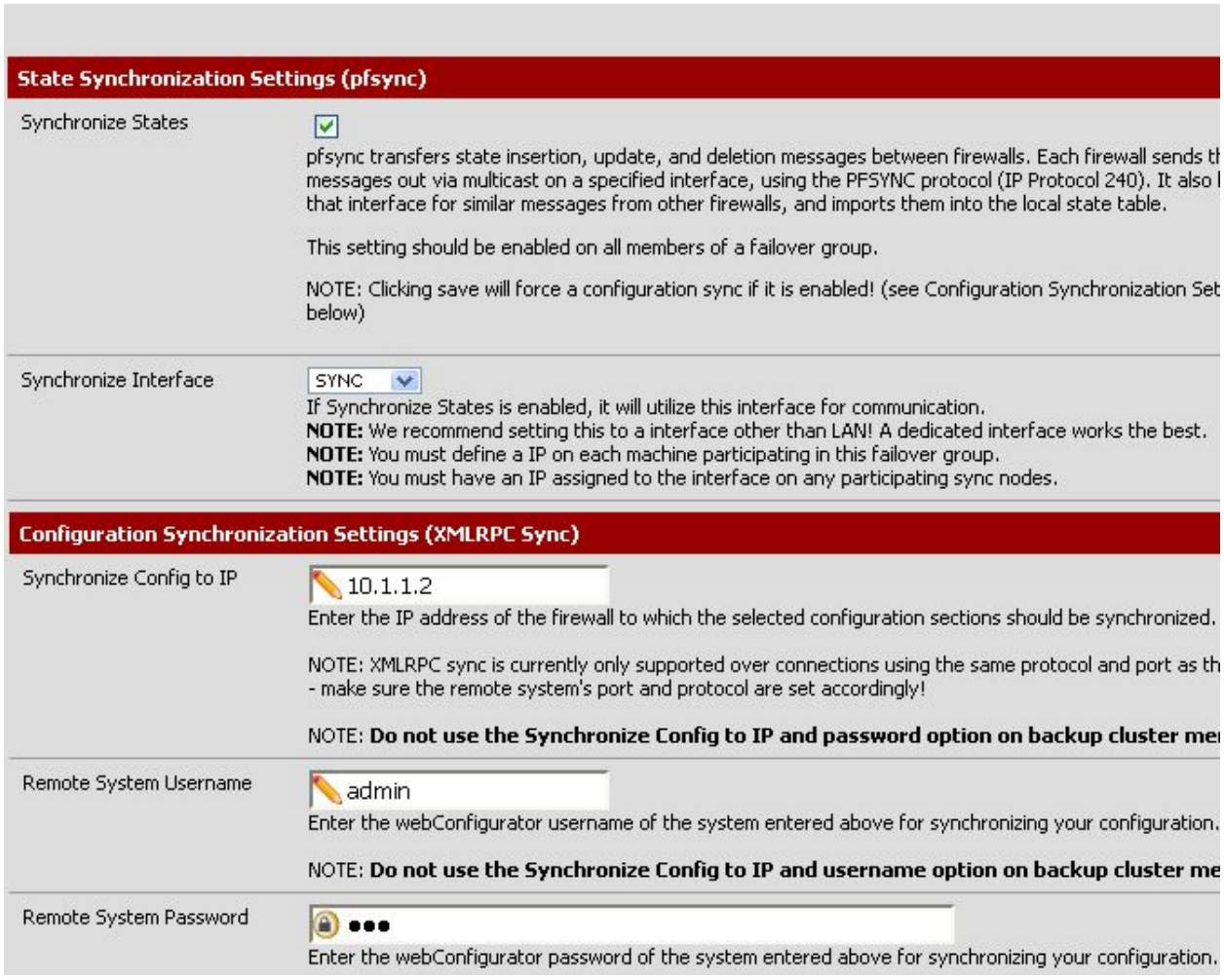
Interface: syns
Protocol: any
Source: any
Destination: any
Chọn **Save**



Nhấn **Apply changes**



B3. Cấu hình CARP setting cho Master Firewall
Firewall, Virtual Ips, chọn CARP setting



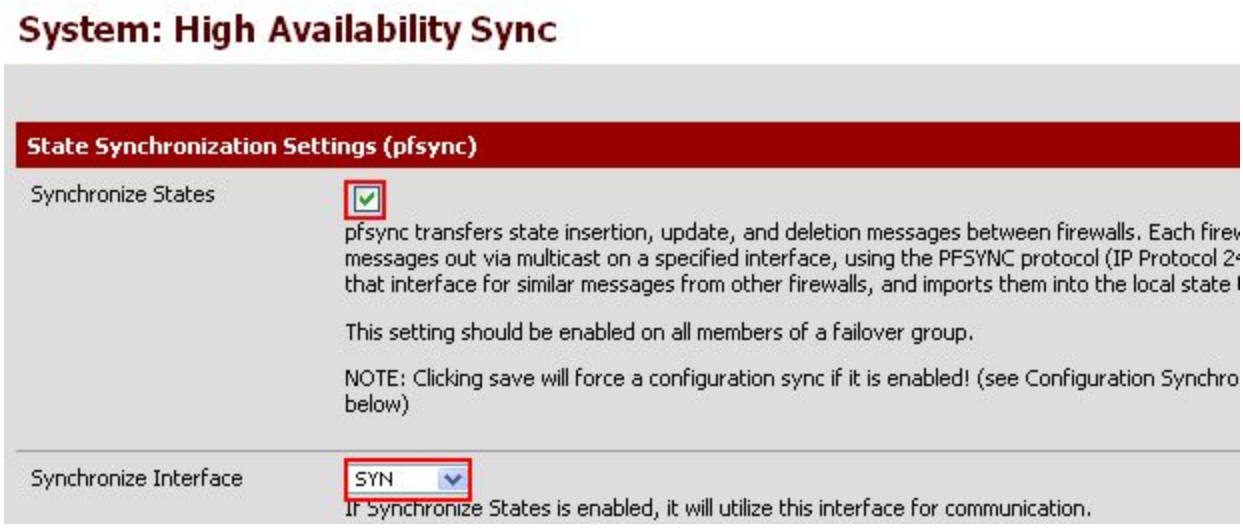
Thiết đặc các tham số cho Master Firewall:

Synchronize States	check
Synchronize Interface	SYNC
Synchronize Config to IP	10.1.1.2

Remote System Username admin
Remote System Password: 123
Synchronize rules check
Synchronize Virtual Ips check

Chọn **Save**

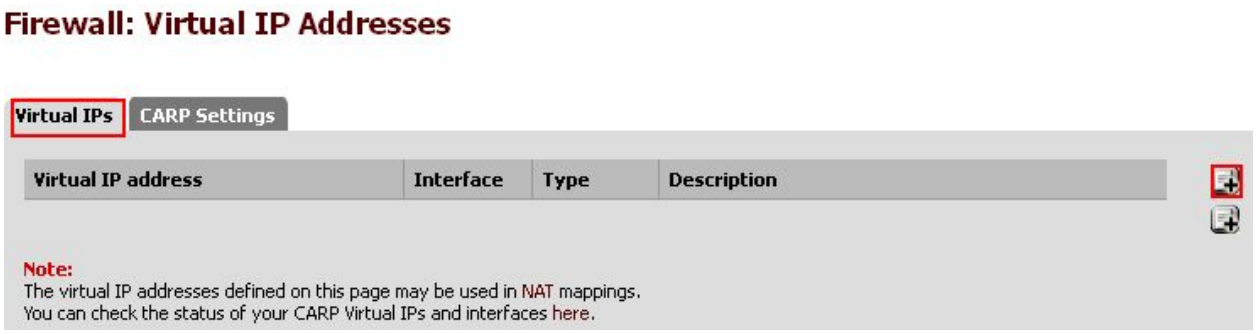
B4. Cấu hình CARP setting cho Backup Firewall

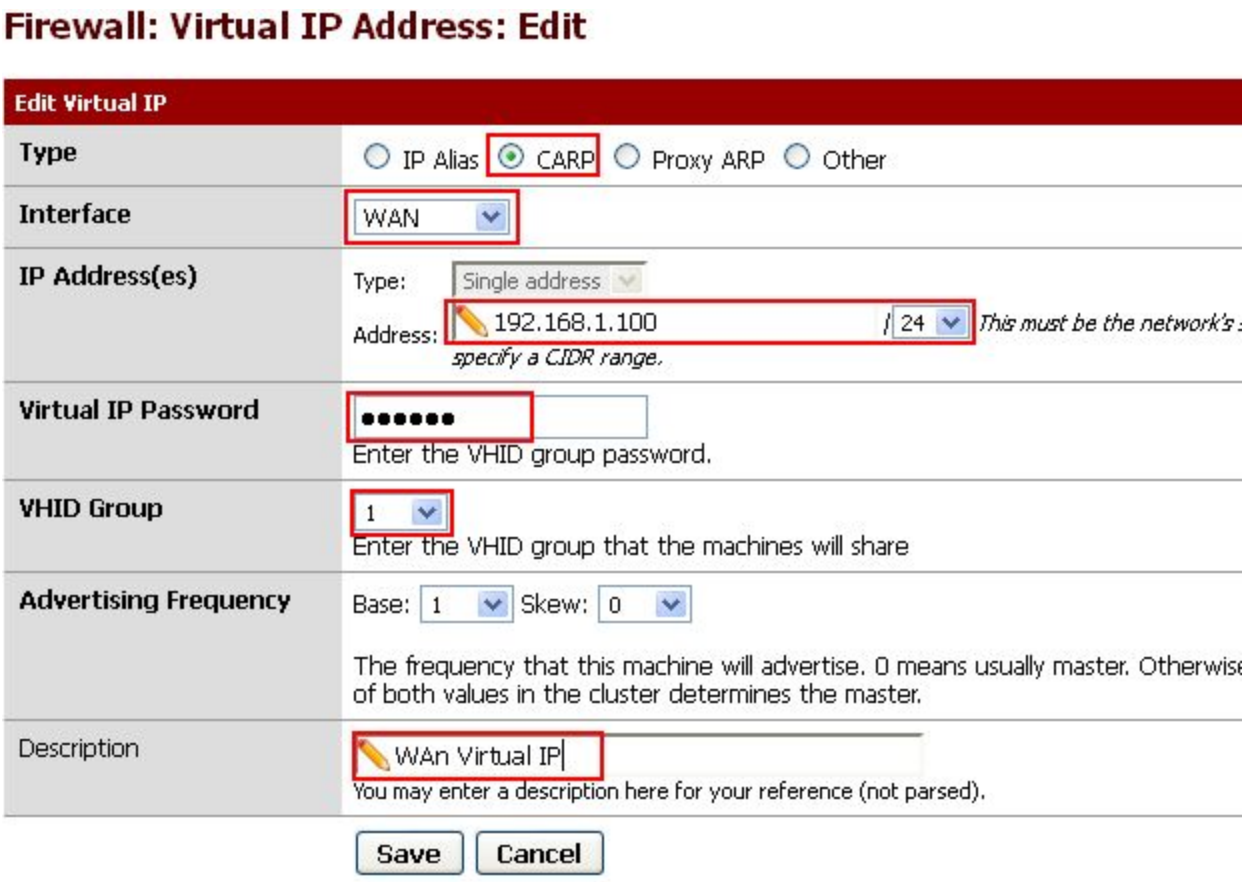


Chỉ thiết đặc 2 tham số cho Master Firewall:

Synchronize States check
Synchronize Interface SYNC

B5. Tạo WAN Virtual IP Addresses
Firewall, Virtual Ips, chọn Virtual Ips, nhấn +





Thiết đặc các tham số cho Virtual IP Addresses

Type:	Chọn CARP
Interface	WAN
IP Address(es)	192.168.1.100/24
Virtual IP Password	123456
VHID Group	1
Description	WAn Virtual IP

Chọn **Save**

B6. Tạo LAN Virtual IP Addresses

Tương tự như trên

Thiết đặc các tham số cho LAN Virtual IP Addresses

Type:	Chọn CARP
Interface	LAN
IP Address(es)	10.0.0.100/24
Virtual IP Password	123456
VHID Group	3
Description	LAN Virtual IP

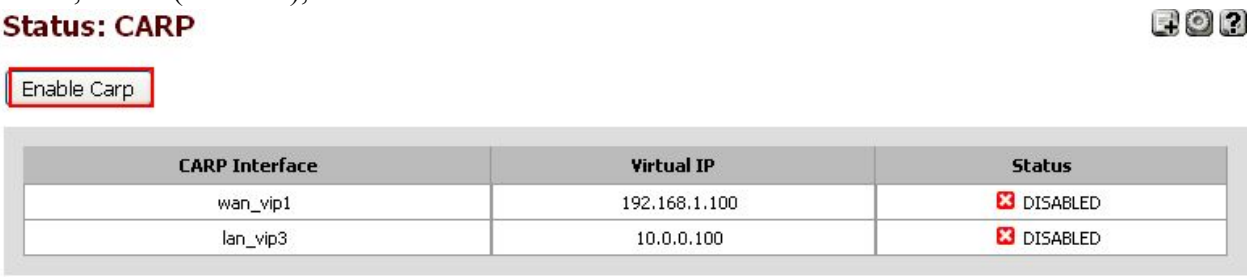
Chọn **Save**

2 Virtual IP được tạo

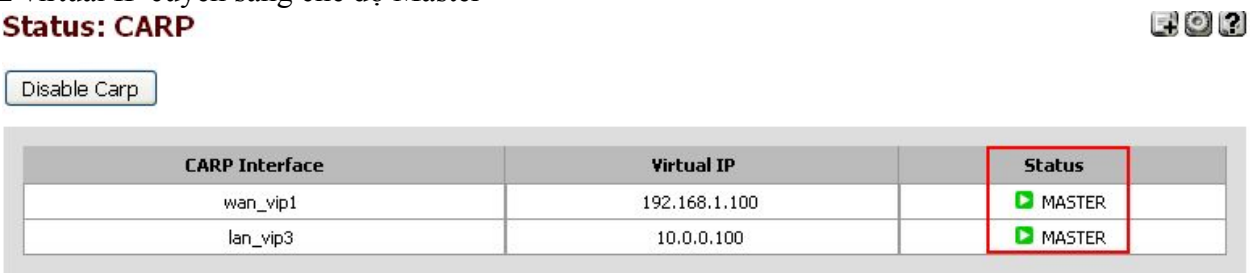
Nhấp Apply changes

B7. Enable CARP

Status, CARP(Failover), nhấn **Enable CARP**

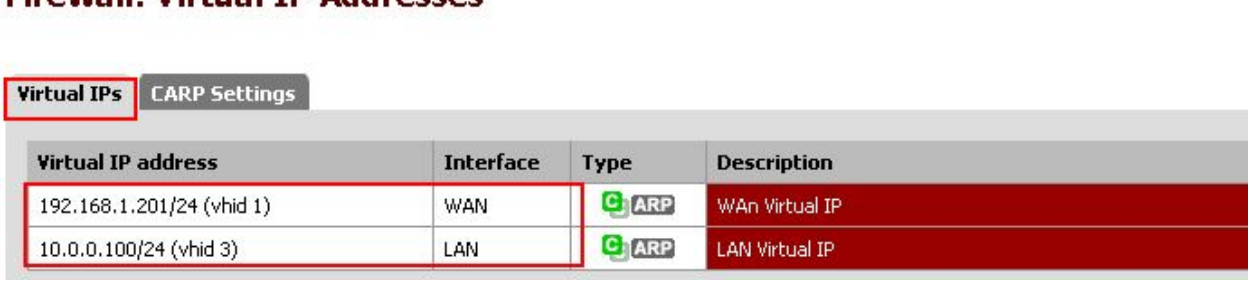


2 virtual IP cuyển sang chế độ Master



B8. Tại FW2 quan sát 2 Virtual IP đã được đồng bộ

Firewall, Virtual Ips, chọn Virtual Ips



Status, CARP(Failover), 2 Virtual IP ở chế độ Backup

Status: CARP

Disable Carp

CARP Interface	Virtual IP	Status
wan_vip1	192.168.1.201	BACKUP
lan_vip3	10.0.0.100	BACKUP

Note:
You can configure high availability sync settings here.

B9. Kiểm tra sự đồng bộ

Tại FW1 tạo rule cho phép truy cập SSH từ interface WAN

Firewall: Rules

Floating | WAN | LAN | SYNC

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 TCP	*	*	*	22 (SSH)	*	none		
	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		Allow Ha noi truy cap HCM
	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none		

Kiểm tra SYSTEM LOG

Status: System logs: General

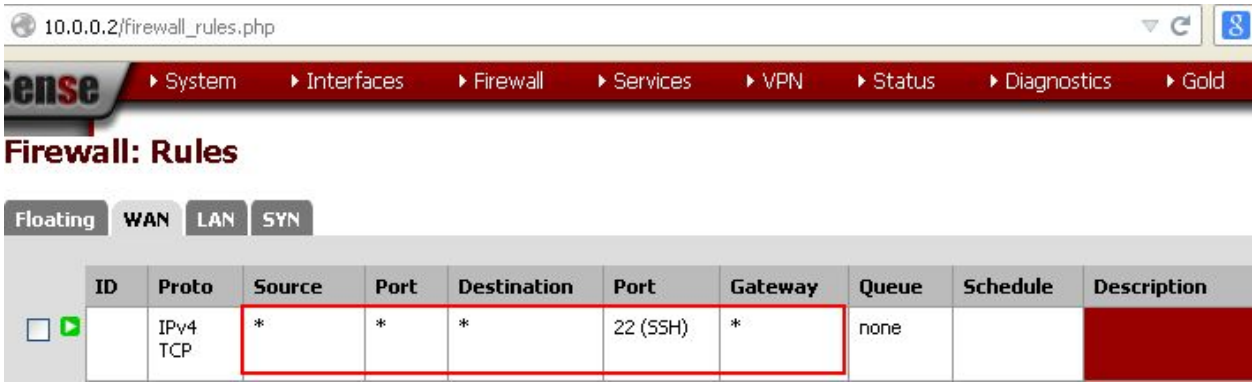
System | Firewall | DHCP | Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | NTP | Settings
General | Gateways | Routing | Resolver | Wireless

Last 50 system log entries

Oct 27 10:59:53	php: rc.filter_synchronize: XMLRPC sync successfully completed with http://10.1.1.2:80:80.
Oct 27 10:59:56	kernel: Bump sched buckets to 256 (was 0)
Oct 27 10:59:56	kernel: Bump sched buckets to 256 (was 0)
Oct 27 11:00:03	php: rc.filter_synchronize: Filter sync successfully completed with http://10.1.1.2:80:80.

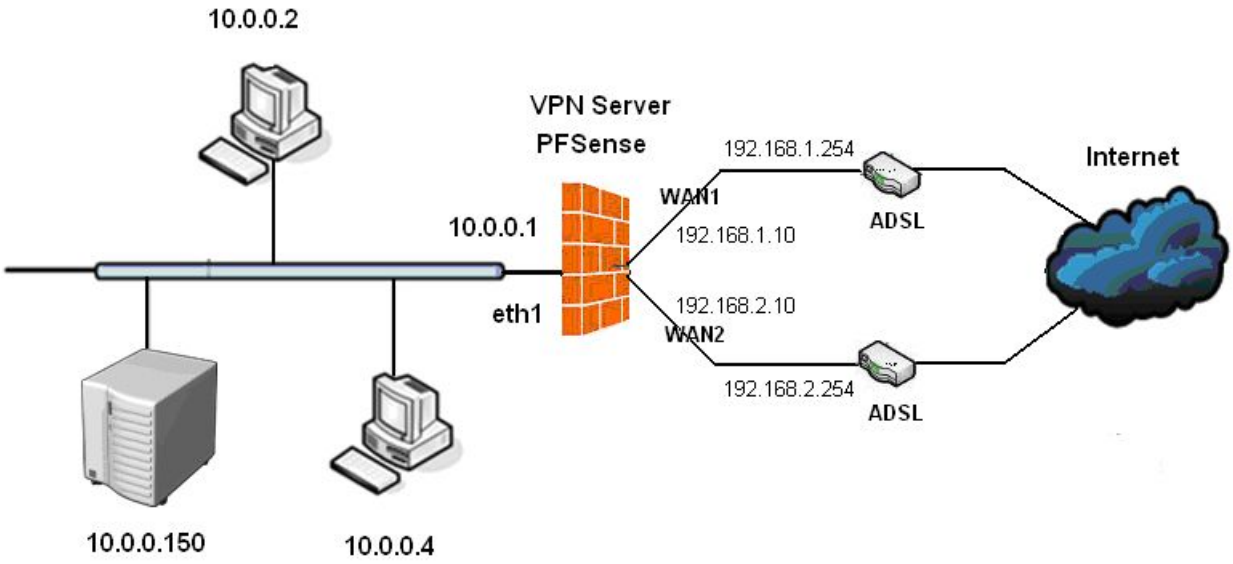
Clear log | Filter

Tại FW2 quan sát thấy rule đã được đồng bộ

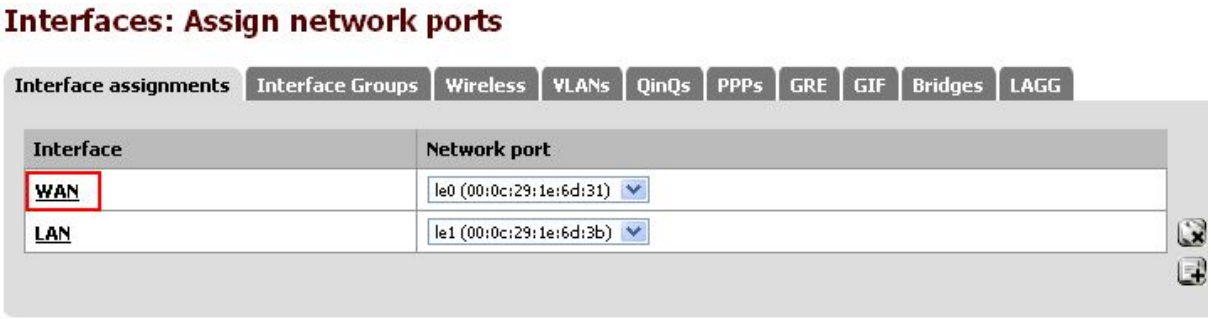


B10. Giả sử FW1 chết, các máy client bên trong LAN vẫn truy cập được Internet

Multi WAN



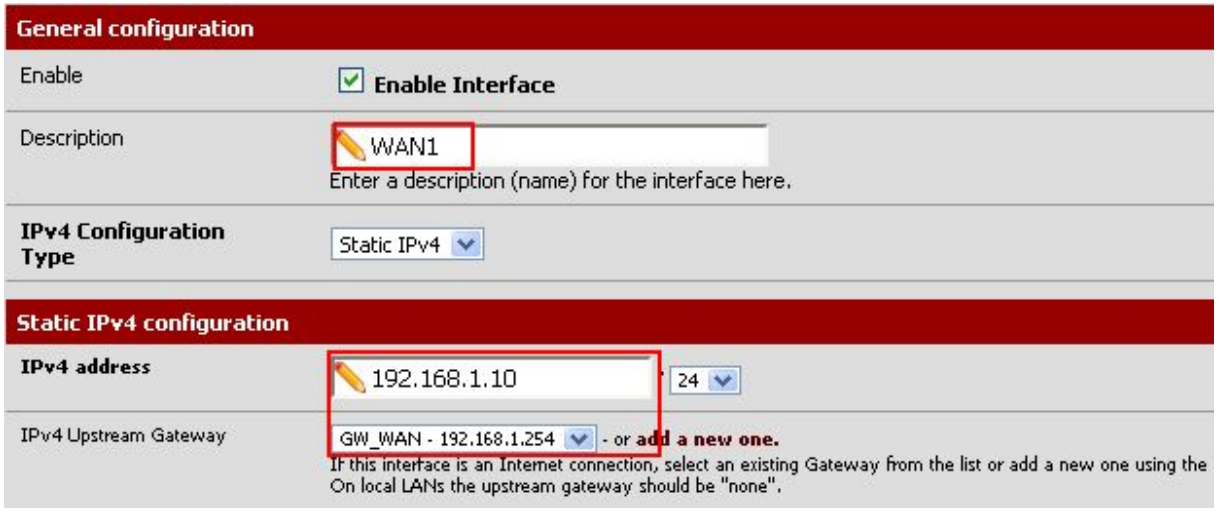
B1. Cấu hình WAN1 interface
Interfaces, chọn Assign



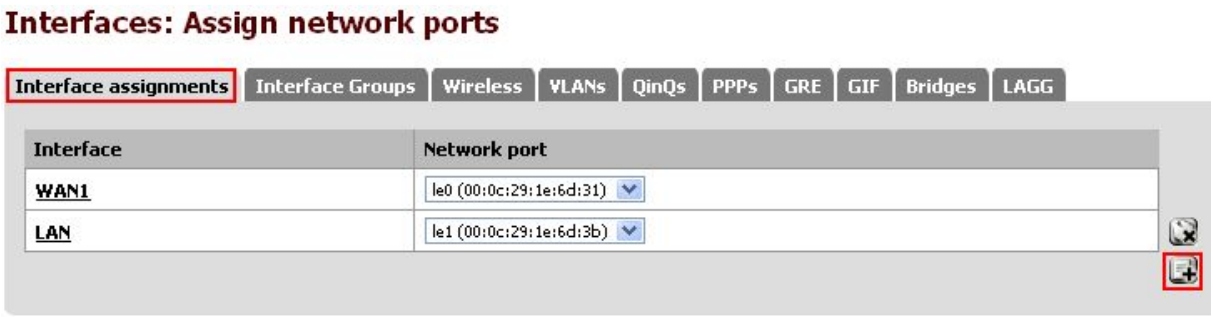
Chọn **Wan**

Enable	Check
IPv4 Configuration Type	Static
IPv4 address	192.168.1.10
IPv4 Upstream Gateway	192.168.1.254

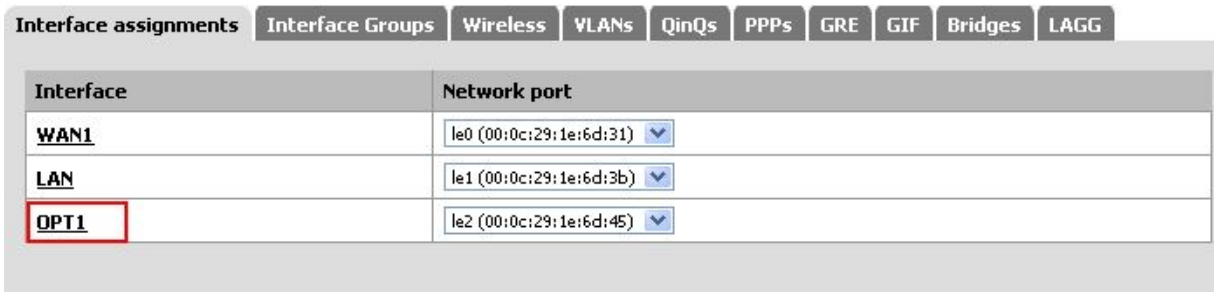
Chọn **Save**



B2. Cấu hình WAN2 interface
Chọn +

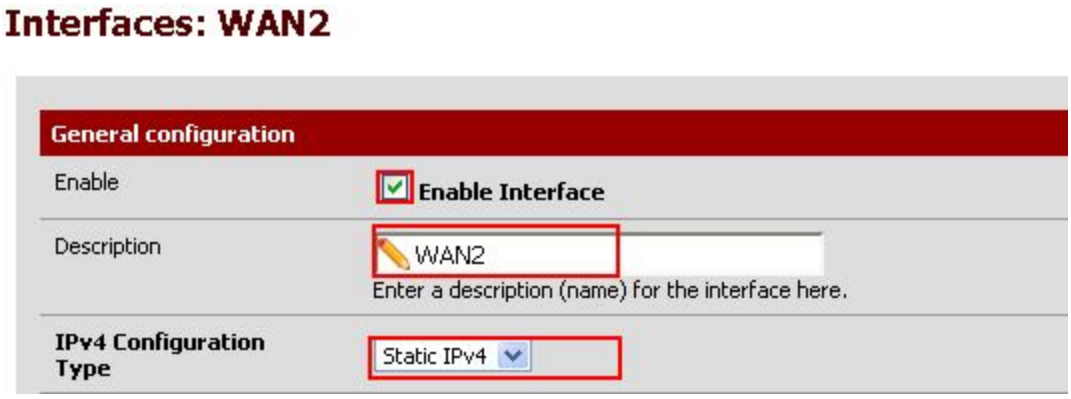


Lan card thứ 3 được thêm vào, chọn OPT1



Nhập thông tin choo WAN2

Description	WAN2
Enable	Check
IPv4 Configuration Type	Static

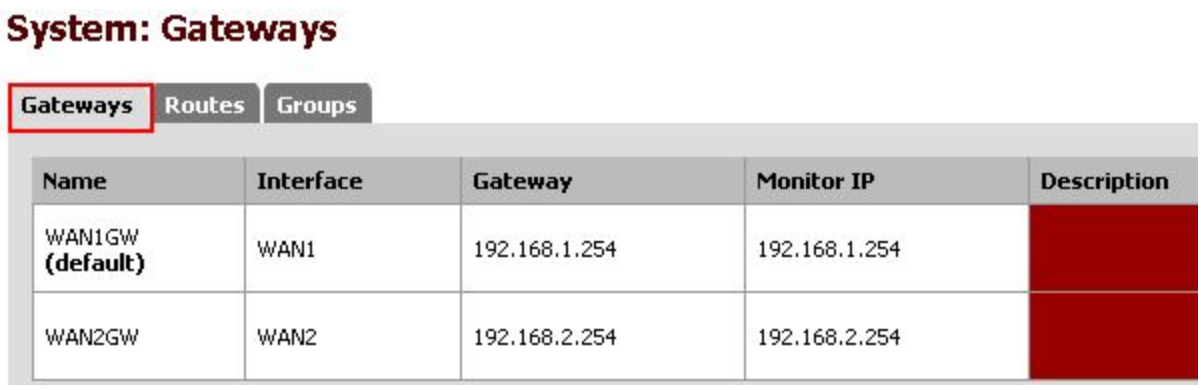


IPv4 address 192.168.2.10
IPv4 Upstream Gateway Nhấn add new one
Nhập 192.168.2.254

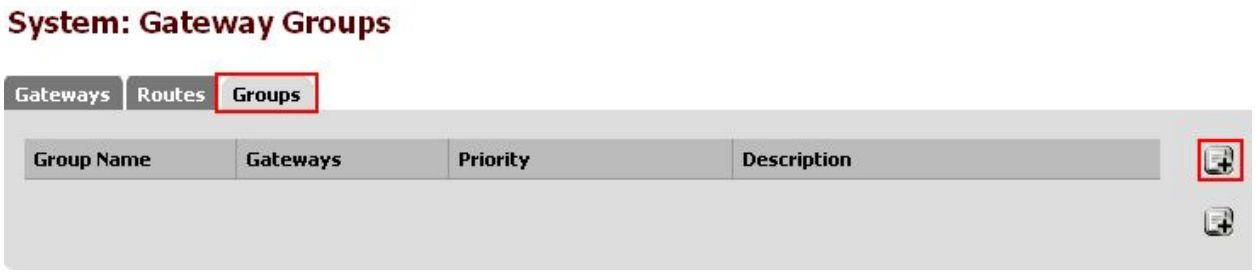
Chọn **Save**

Chọn **Save**

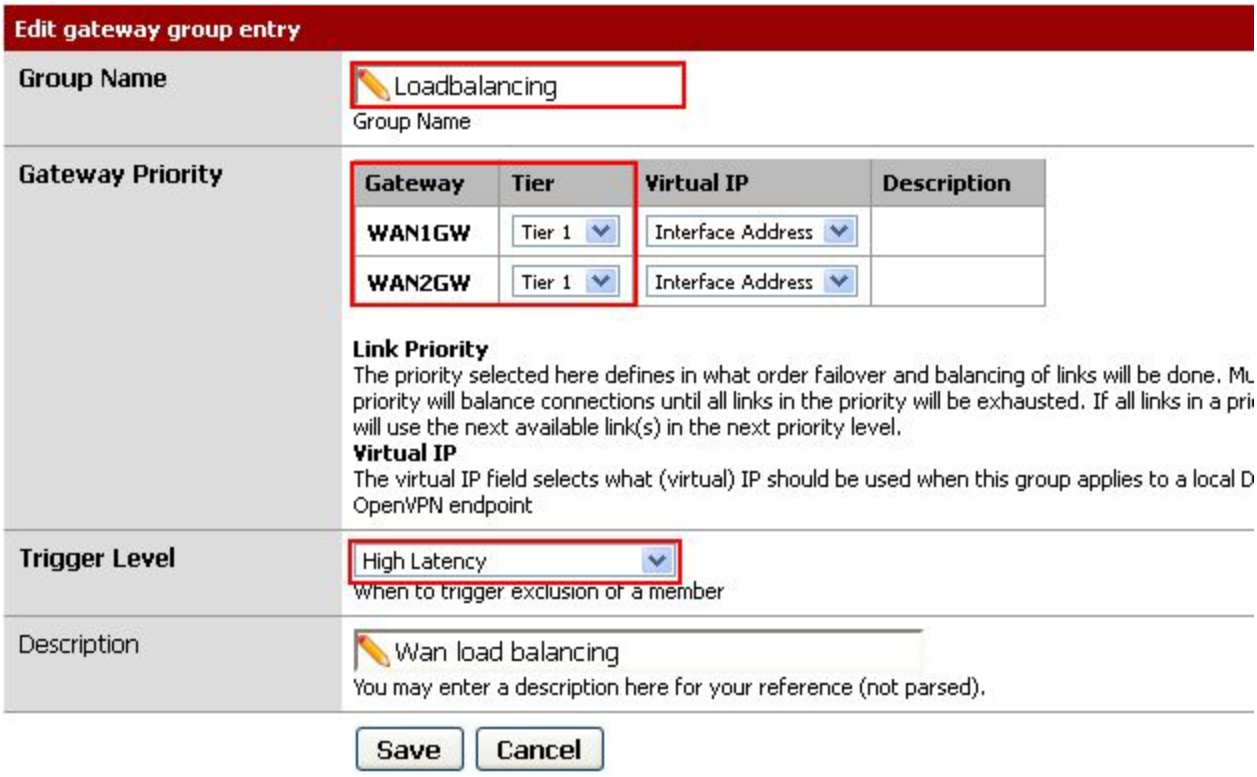
B3. Quan sát các GW đã tạo
System, routing



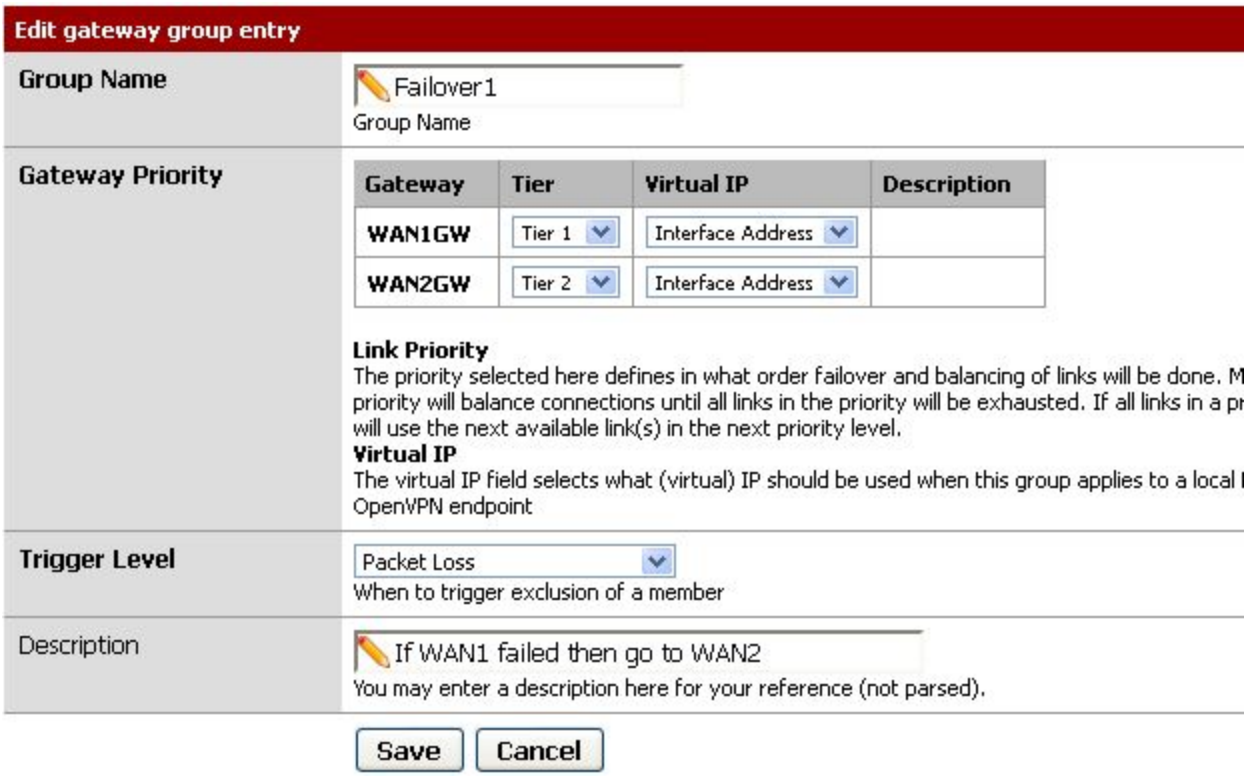
B4. Tạo Group
System, routing, chọn +



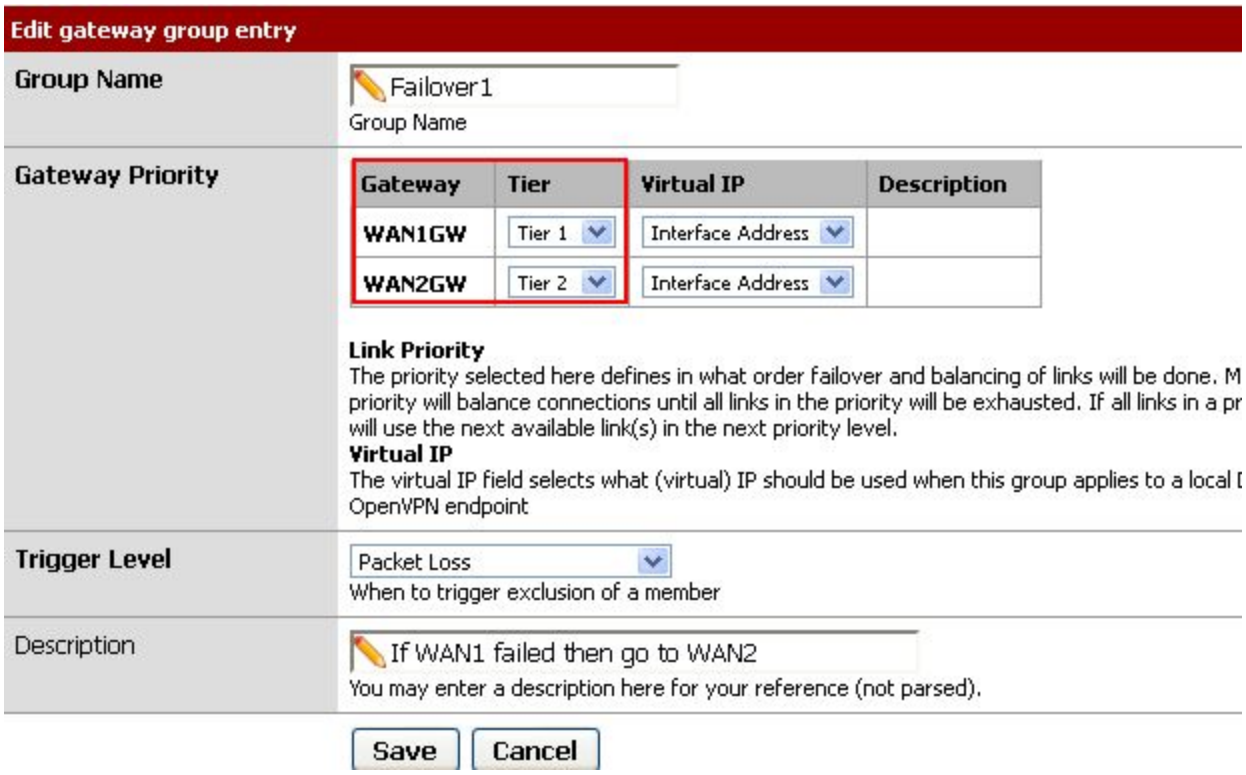
Group Name	Loadbalancing
Gateway Priority	chọn Tier 1 cho 2 cổng WAN
Trigger Level	Chọn Packet Loss or High Latency
Chọn	**Save**



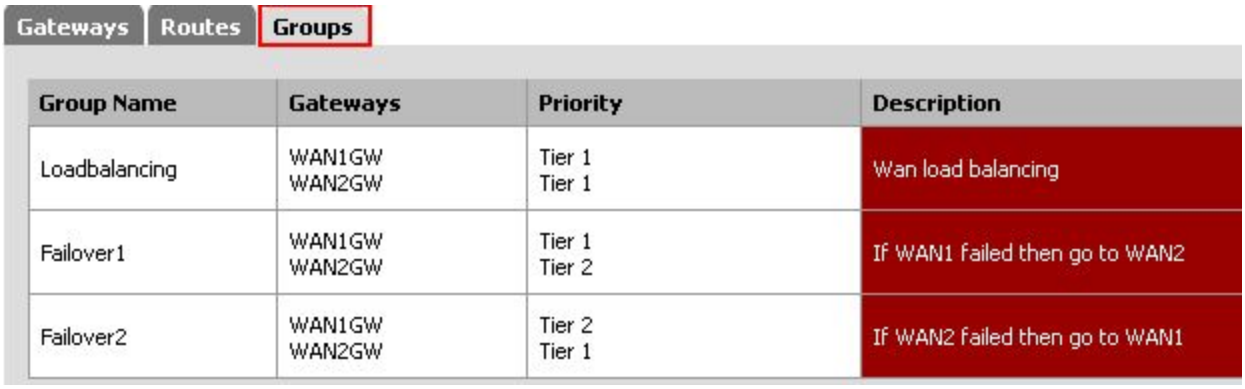
Tạo tiếp group Failover1



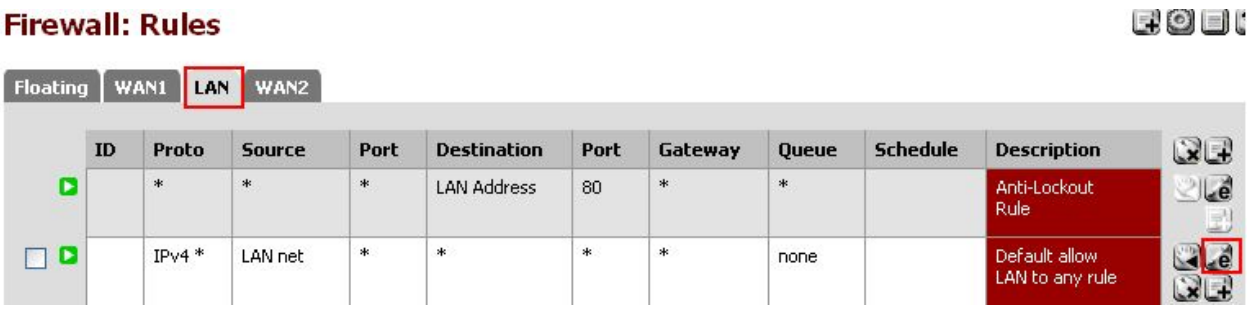
Tạo tiếp group Failover1



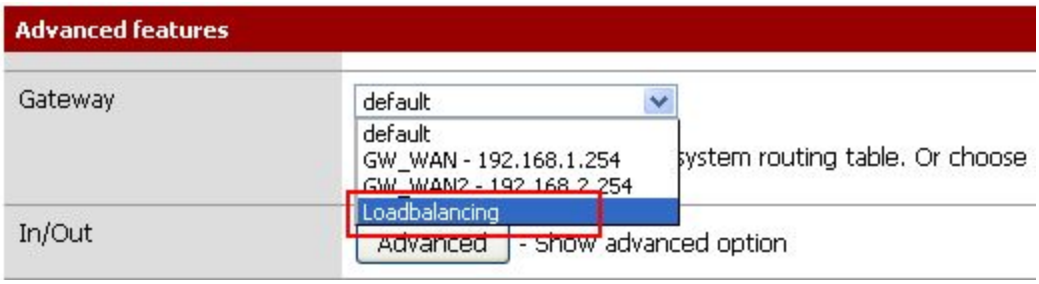
Kết quả 3 group được tạo ra



B6. Tạo rule từ LAN đến Gateway Groups
Firewall, Rules, Lan, chọn edit **LAN net**

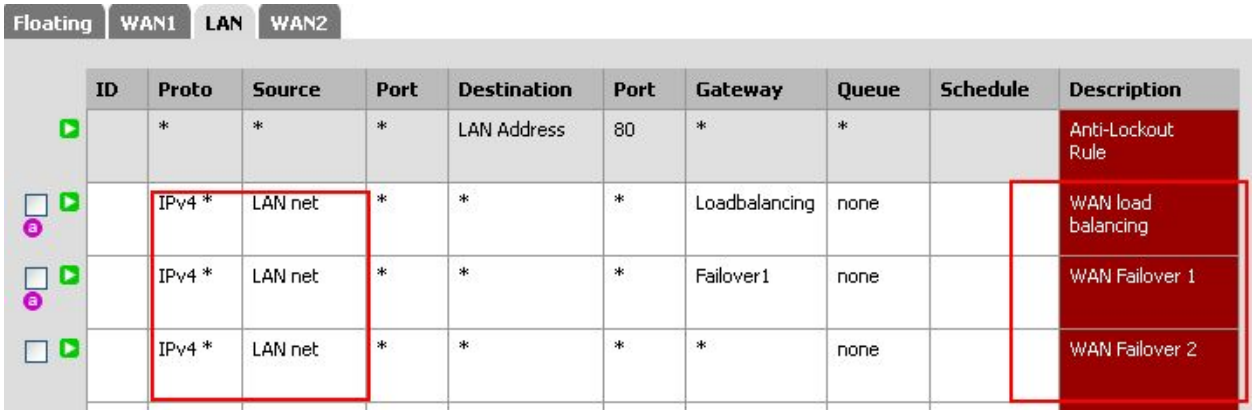


Protocol any
Gateway chọn Loadbalancing
Chọn **Save**

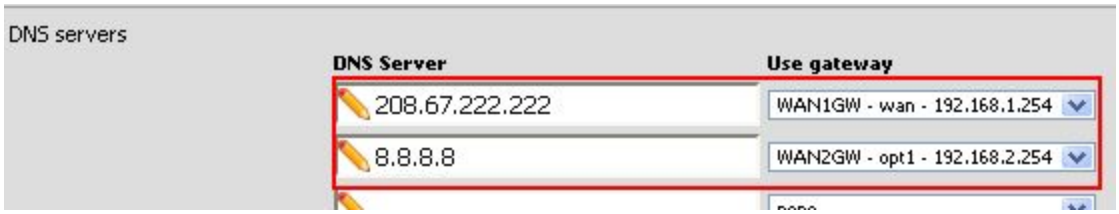


Tạo tiếp 2 rule giống như trên nhưng lần lượt chỉ đến Gateway là Failover1 và Failover2

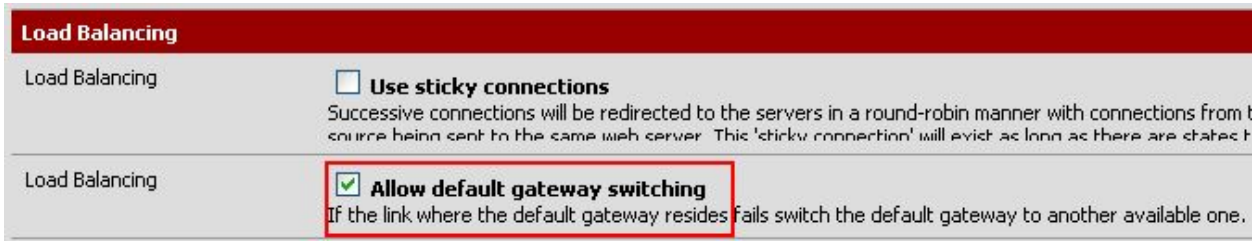
Kết quả 3 rule được tạo:



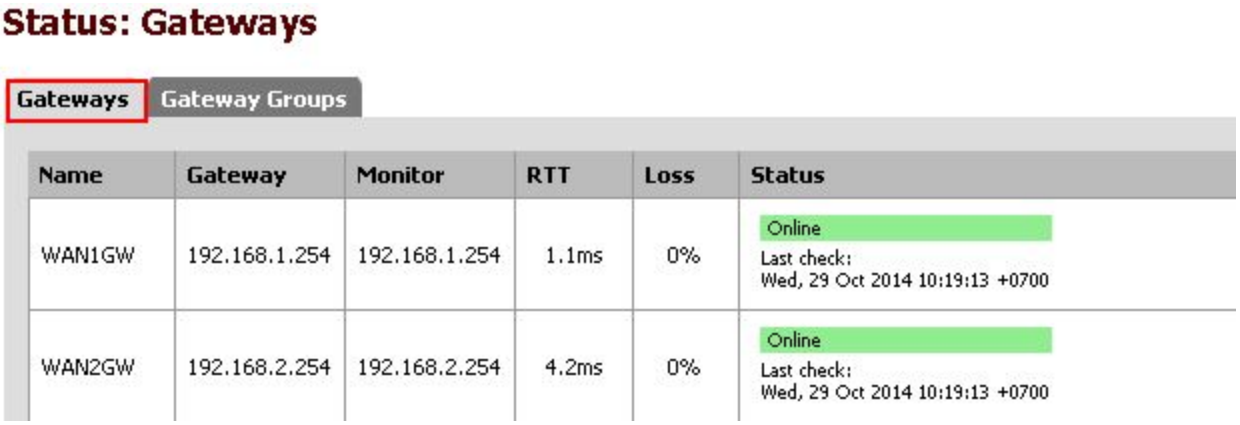
B7. Gán DNS cho mỗi Gateway
System, General Setup



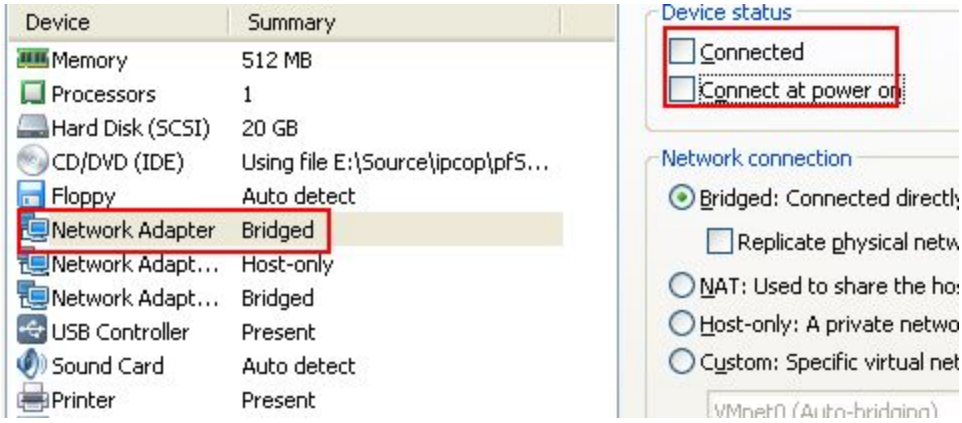
Chọn **Save**
B8. Tự chuyển Gateway khi có 1 gateway hư
System, Advanced, chọn thẻ **Miscellaneous**
Allow default gateway switching: Check



B9. Kiểm tra
Status, chọn **Gateway**
Cả 2 Gateway cùng ở trạng thái online
Các máy client truy cập web



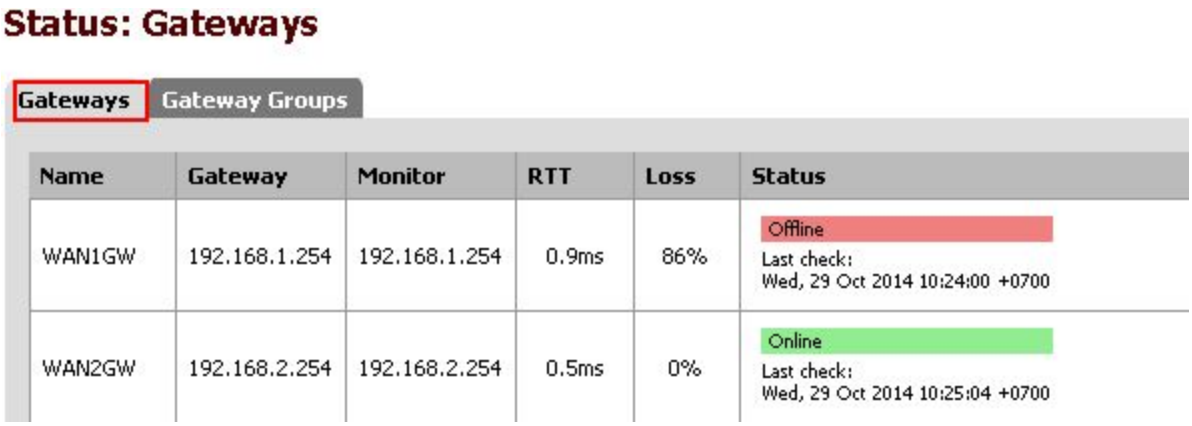
B10. Giả sử mất kết nối GW1
VMWare, setting: bỏ chọn Connected, Connect at power on
Chọn **OK**



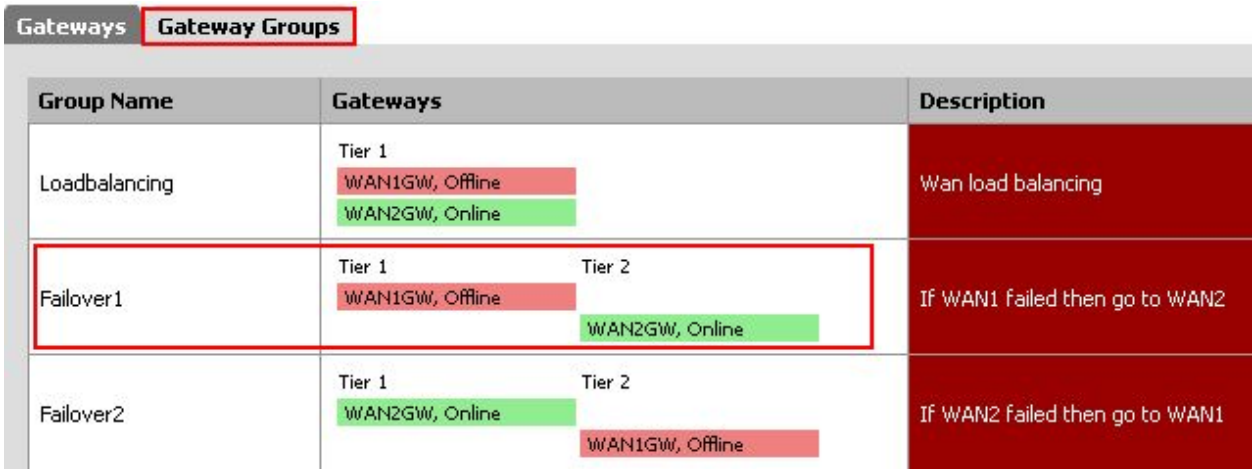
Các máy client truy cập web bình thường

B11. Trạng thái gateway

Status, Gateway**,** chọn **Gateway**

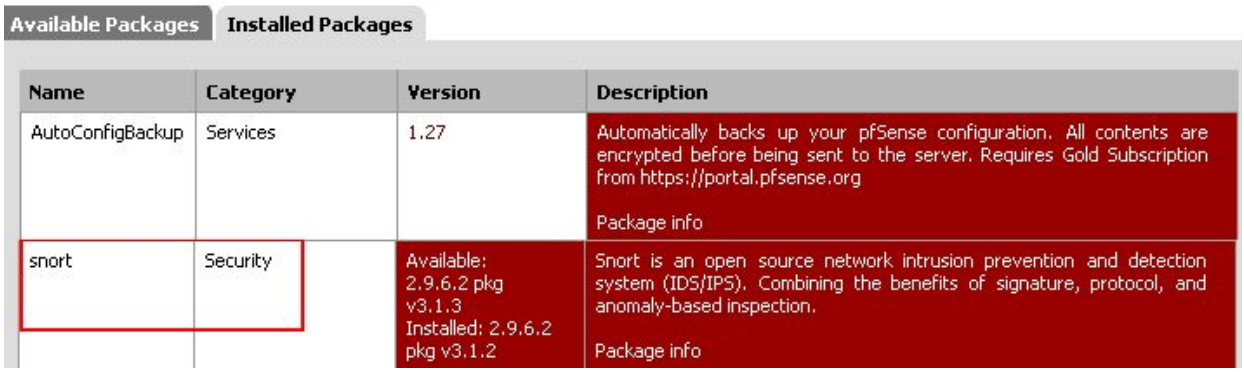


Chọn Gateway Groups

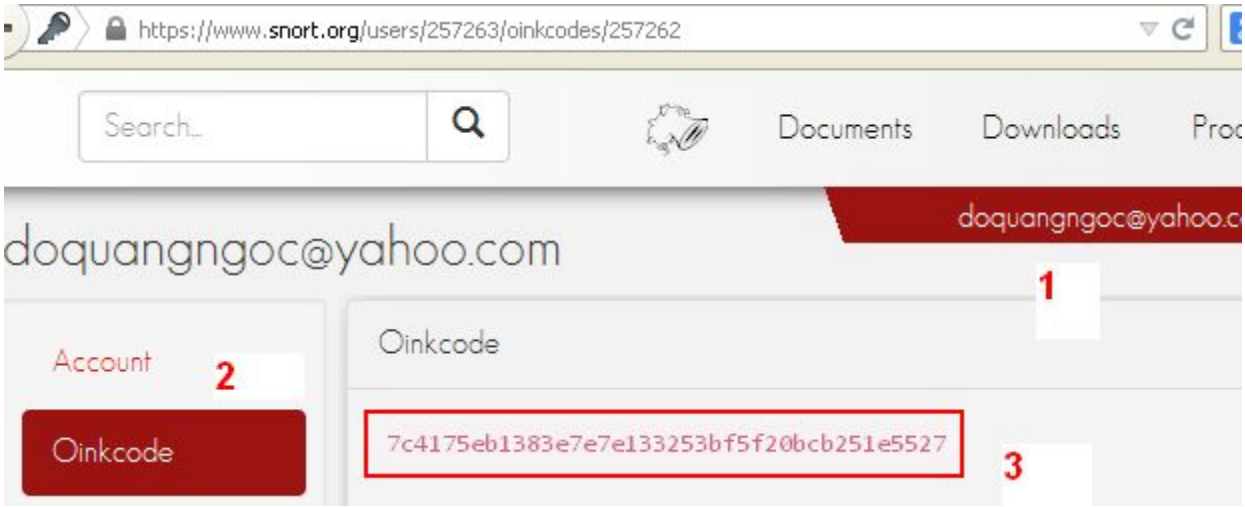


IDS – IPS

Xây dựng hệ thống phát hiện và ngăn chặn xâm nhập mạng
B1. Cài gói Snort
System, Package Manager



B2. Lấy mã Oinkcode từ trang snort.org
Truy cập trang snort.org
Click địa chỉ email, chọn Oinkcode, copy đoạn mã : 7c4175eb1383e7e7e133253bf5f20bcb251e5527



B3. Kết nối đến Snort
Service, Snort, chọn thẻ **Global Settings**

Install **Snort VRT** rules Check
Code: Dán đoạm mã cấp bởi Snort
Vd: 7c4175eb1383e7e7e133253bf5f20bcb251e5527

Install **Snort Community** rules Check

Install **Emerging Threats** rules Check
Chọn **Save**

B4. cập nhật tập rule từ Snort
Chọn tab Updates, nhấn Check đẩ bắt đầu cập nhật

Quá trình cập nhật tập rule được tiến hành

B5. Cấu hình Snort bảo vệ interface WAN
Service, Snort, chọn thẻ **Snort Interface, nhấn +**

Khái báo các thiết đặt

Enable	Check
Interface	Chọn WAN
Send Alerts to System Logs	Check
Block Offenders	Check

Chọn **Save**

B6. Gán tập rule cho interface WAN
Trên interface WAN, chọn Edit

Chọn WAN Categories
Use IPS Policy Check
Chọn Select All
Chọn **Save**

B7. Khởi động Snort trên interface WAN
Snort Interface, nhấn icon X

8. Kiểm tra hoạt động của Snort
Dùng Zenmap qét IP WAN 192.168.1.10 của Firewall

9. Snort đã phát hiện ip 192.168.1.250 quét hệ thống và đã Blocked IP này

Tại ip 192.168.1.250 không thể ping đến FW (tạo thêm rule trên WAN cho phép ping)

Nhấn X để đưa IP nà ra khỏi danh sách block nếu muốn

Monitor - Services

1. BandwidthD
B1. cài BandwidthD.
System, Packages

B2. Cấu hình BandwidthD
Service, Bandwidthd,

Enable bandwidthd	Check
Interface	Chọn LAN
Draw Graphs	Check

Chọn **Save**

B3. Xem thống kê bandwidth

Chọn **Access bandwidthD**

Nhắp chọn **Daily**, xem thông kế theo ngày

Nhắp chọn **Weekly**, xem thông kế theo ngày

2. Dashboard
Xem thông tin tóm tắt toàn bộ hệ thống
Status: Dashboard
Quan sát các thông số: CPU, Memory, Disk, interface

Thêm các đối tượng vào Dashboard:
nhấn +, chọn đối tượng cần thêm
Chọn **Save Settings**

3. RRD Summary
Status, RRD Summary xem thống kê bandwidth theo tháng

RRD Database: Chọn kết nối cần theo dõi
Start Day: Chọn ngày bắt đầu thống kê

4. ntopng

Diagnostics, chọn ntopng Settings
Khai báo password cho ntopng
Interface: chọn LAN, WAN
Chọn **Change**

Login với user: admin, password: admin	

+Talkers: Xem các host cùng với các kết nối đang tích cực	
+ Hosts: biểu diễn các host đang truy cập cùng với tỉ lệ phần trăm	

+ Applications: biểu diễn tỉ lệ phần trăm các ứng dụng đang sử dụng	

Xem thông tin chi tiết về host
Host, Host List, chọn 10.0.0.150

Chọn Flows

5. cron
Lập lịch
Service, chọn Cron

Lập lịch xóa cache của Proxy service vào ngày 1 của mỗi tháng:
Nhập thông tin như hình
Chọn **Save**

6. DHCP
b1. Cấu hình DHCP server
Services, DHCP server, Chọn LAN

Range: nhập 10.0.0.10 - 10.0.0.245
DNS servers 8.8.8.8
Gateway 10.0.0.10
Chọn **Save**

B2. client xin IP
Tại máy Clent nhập lệnh ipconfig /renew để xin mới IP
Ipconfig /all hiển thị IP đã cấp phát

B3. Kiểm tra ip đã cấp
Status, chọn DHCP leases

B4. Gán IP theo MAC Address

DHCP Static Mappings for this interface: nhấn +

Nhập các thông tin cho host cần nhận IP

MAC address	Nhập 00:0c:29:8a:f1:8e	(MAC address của host xin IP)
IP address	10.0.0.246	
Hostname	client1	
DNS servers	8.8.8.8	

Gateway 10.0.0.10
Chọn **Save**

b5. Client xin lại IP

6. Backup/Restore
B1. sao lưu toàn bộ hệ thống
Diagnostics, Backup/restore

Backup area	Chọn ALL
Chọn	Download configuration

Kết quả file xml (vd: config-pfsense.nhatnghe1.com-20141031121055.xml) được lưu ra đĩa C

B2. Phục hồi toàn bộ hệ thống
Hệ thống bị mất file cấu hình hoặc hư hỏng nặng có thể phải cài lại
Đảm bảo hệ thống đặt ip thích hợp, kết nối được với Internet

Trước khi restore, tiến hành xóa user, rule….
Diagnostics, Backup/restore
Restore area: Chọn đối tượng cần restore
Browser chọn file backup xml
Nhấn **Restore configuration** để restaore

Fw sẽ boot lại và tiến hành cài lại tất cả các gói cần thiết

7. Quản lý service
Status, Services
Tại đây có thể start, stop, restart lại các service

8. System log
Status, System logs
Ghi lại tất cả các sự kiện xảy ra trong hệ thống