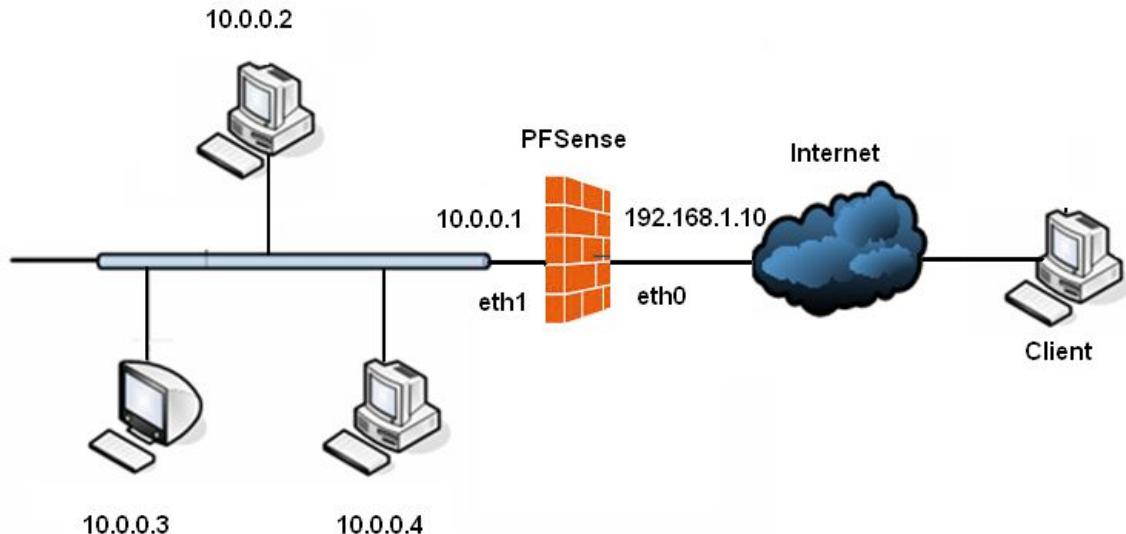


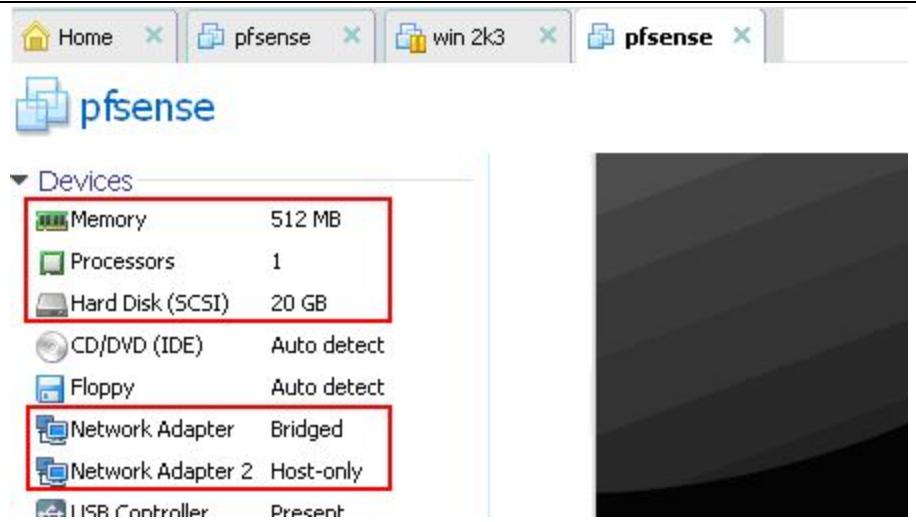
Cài đặt PfSense

Mô hình mạng

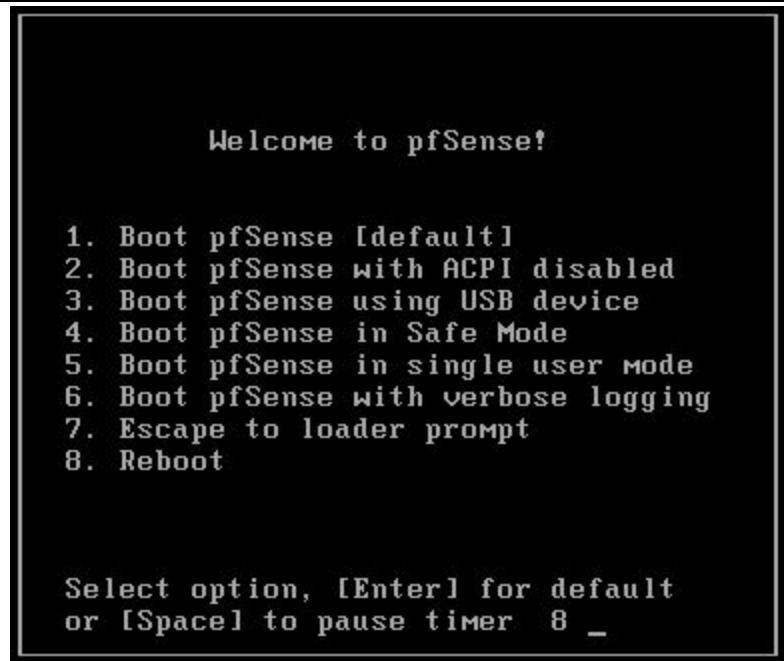


1. Cài máy PfSense

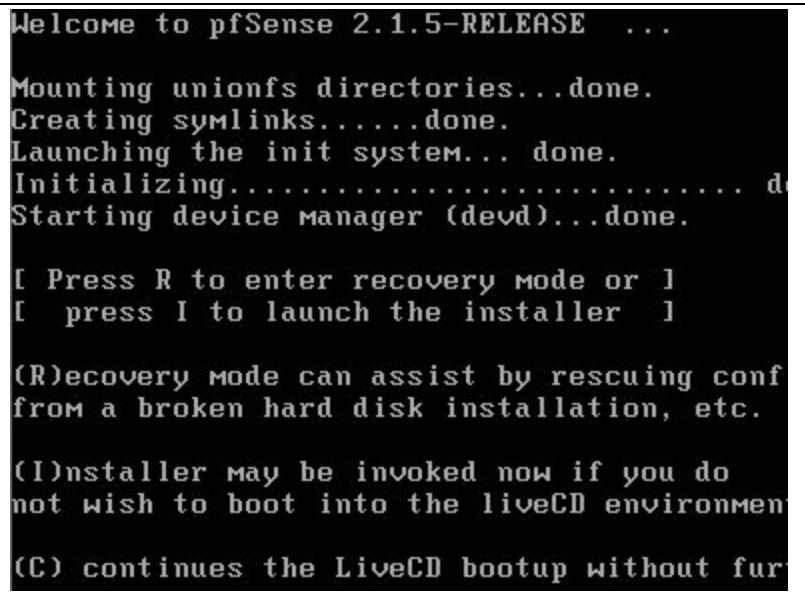
B1. Trên VMWare, Tạo máy ảo có cấu hình như sau



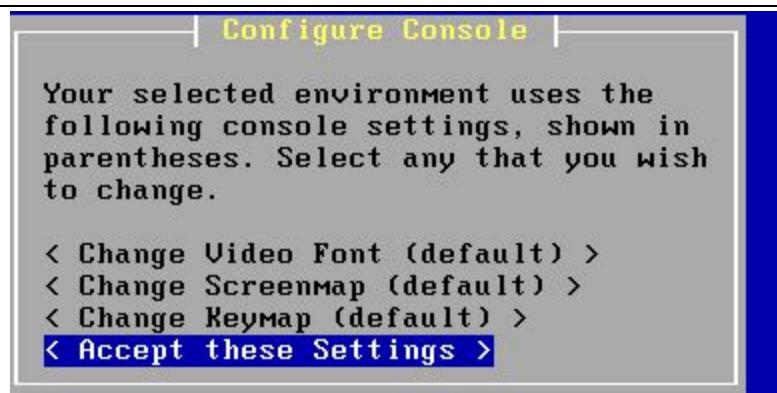
B2. Nhấn Enter



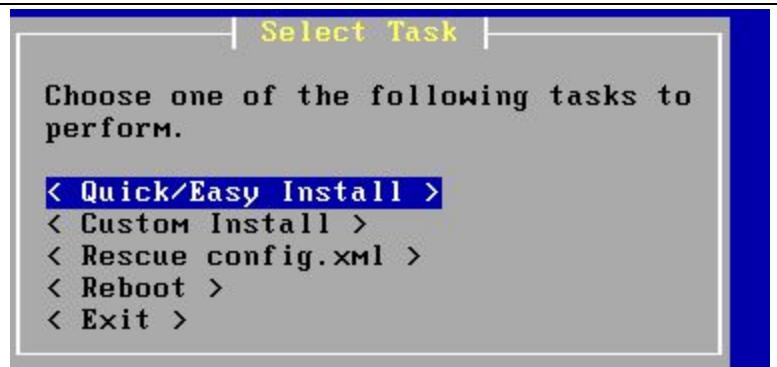
B3. Nhấn I để cài đặt (press I to launch the installer)



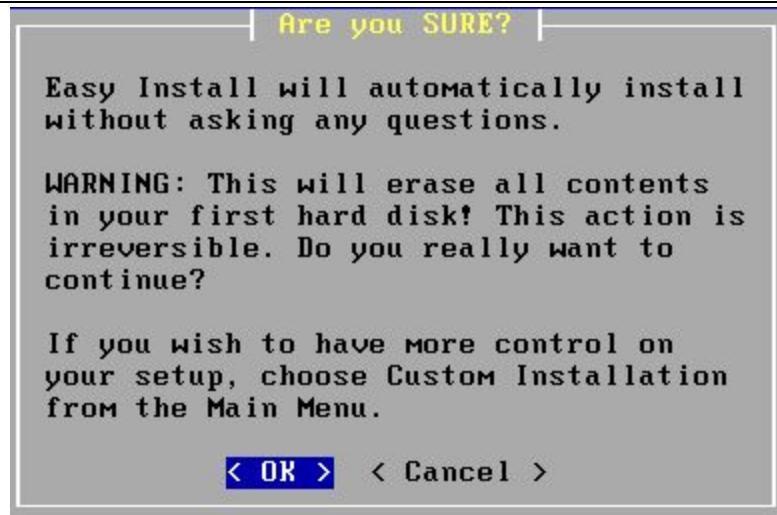
B4. Chọn Accept these settings , chấp nhận các tham.



B5. Chọn Quick/Easy Install



B6. Nhấn OK để bắt đầu cài đặt



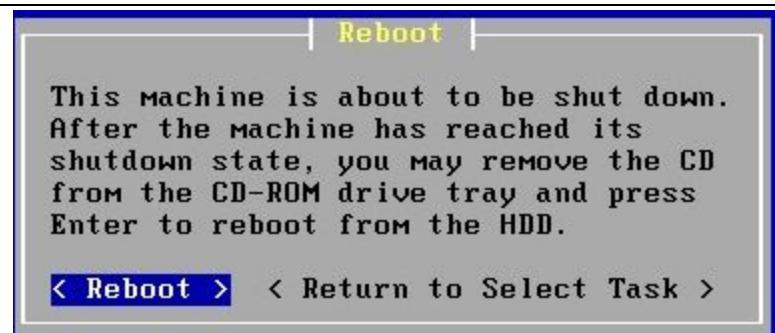
Quá trình cài đặt bắt đầu



B7. Chọn Standard Kernel



B8. Chọn Reboot để khởi động máy



B9. Chọn N, không cấu hình VLAN

```
Default interfaces not found -- Running interface assignment option
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0  00:0c:29:1e:6d:31  (up) AMD PCnet-PCI
le1  00:0c:29:1e:6d:3b  (up) AMD PCnet-PCI

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces
say no here and use the webConfigurator to configure VLANs later,
No you want to set up VLANs now [y/n]? ■
```

B10. Nhập tên Lan card:

kết nối WAN, nhập le0,
kết nối LAN, nhập le1. Nhấn Enter, chọn Y

```
If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.
```

```
Enter the WAN interface name or 'a' for auto-detection: le0
```

```
Enter the LAN interface name or 'a' for auto-detection
```

```
NOTE: this enables full Firewalling/NAT mode.
```

```
(or nothing if finished): le1
```

```
Enter the Optional 1 interface name or 'a' for auto-detection
```

```
(or nothing if finished): enter
```

```
The interfaces will be assigned as follows:
```

```
WAN -> le0
LAN -> le1
```

```
Do you want to proceed [y\!n]?■
```

B11. 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/DHCP4: 192.168.1.67/24
LAN (lan)      -> le1      -> v4: 192.168.1.1/24
```

- | | |
|-----------------------------------|----------------------------------|
| 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: ■
```

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

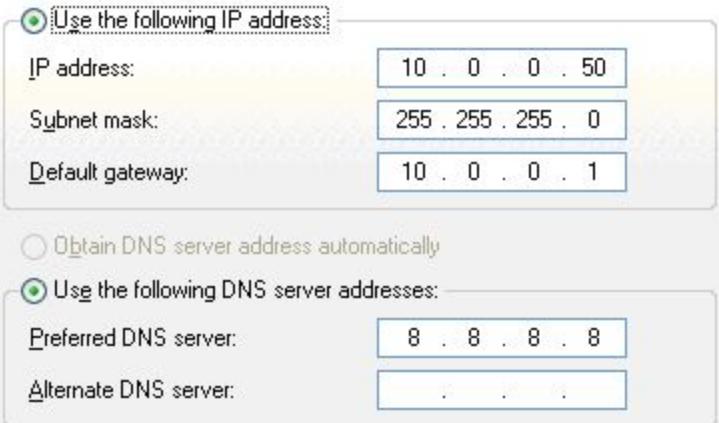
Do you want to enable the DHCP server on LAN? [y\?n] n
Disabling DHCPD...Done!
Disabling DHCPD...Done!

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	

General Information

Hostname:	<input type="text" value="pfSense"/> pfSense EXAMPLE: myserver
Domain:	<input type="text" value="nhatnghe1.com"/> nhatnghe1.com EXAMPLE: mydomain.com
Primary DNS Server:	<input type="text" value="8.8.8.8"/>
Secondary DNS Server:	<input type="text"/>
Override DNS:	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

B5. Nhập Timezone, Nhấn Next

Please enter the time, date and time zone.

Time Server Information

Time server hostname:	<input type="text" value="0.pfsense.pool.ntp.org"/> 0.pfsense.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone:	<input type="text" value="Asia/Ho_Chi_Minh"/> <input type="button" value="▼"/>

Next

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

On this screen we will configure the Wide Area Network information.

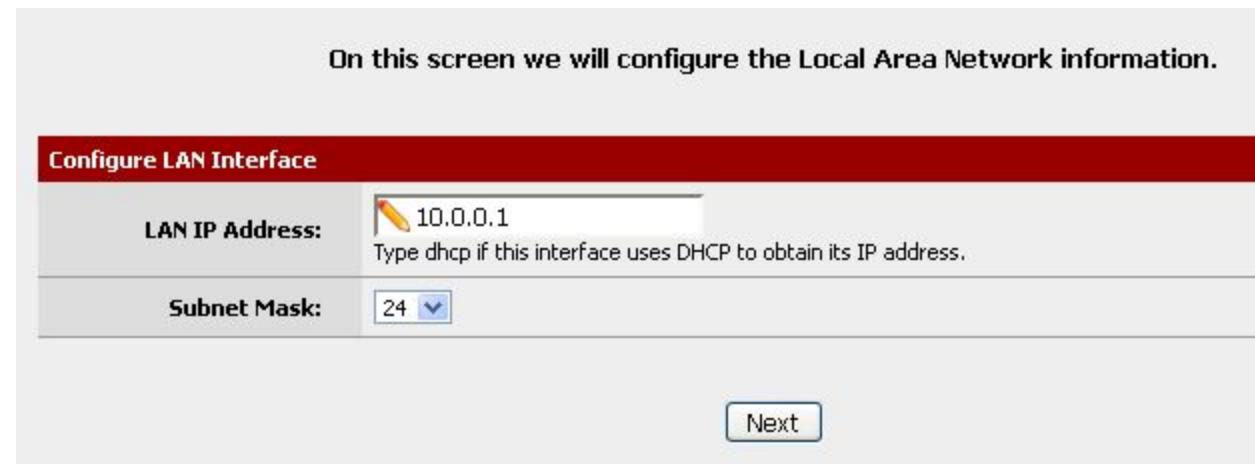
Configure WAN Interface

SelectedType:	<input type="text" value="Static"/> <input type="button" value="▼"/>
----------------------	--

General configuration

MAC Address:	This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required for reconnections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
---------------------	---

B7. Khai báo thông tin cho LAN interface, nhấn Next để 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

Tin nhanh VnExpress - Đọc b... × +

vnexpress.net

Thất bại - bài học của mọi doanh nhân 22

Chúng ta thường tránh những tình huống có thể khiến bản thân gục ngã, nhưng nếu không thất bại, bạn không thể học hỏi. Và nếu không học hỏi, bạn sẽ không ...

- Đừng lãng phí tuổi 20 ở các công ty lớn / Bài học vượt qua thất bại của triệu phú 26 tuổi

Thổ Nhĩ Kỳ cho phép Mỹ sử dụng căn cứ quân sự để chống IS

Ankara vừa chấp thuận để Washington sử dụng các căn cứ không quân ở Thổ Nhĩ Kỳ trong chiến dịch không kích chống Nhà nước Hồi giáo tự xưng, bao gồm cả ...

- Lính Anh trở lại Iraq huấn luyện lực lượng chống IS / Máy bay Mỹ thả vũ khí xuống cho quân đội Iraq

Proxy server

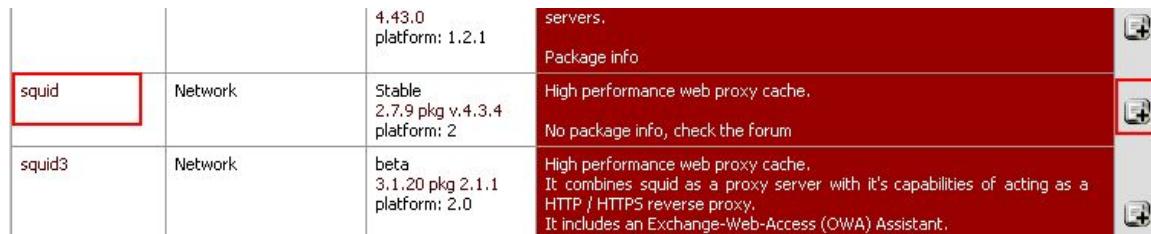
Quản lý, giám sát truy cập internet

1. Chuẩn bị

Cài các gói cần thiết

1.1 cài gói squid

System, Packages, chọn squid, nhấn dấu +



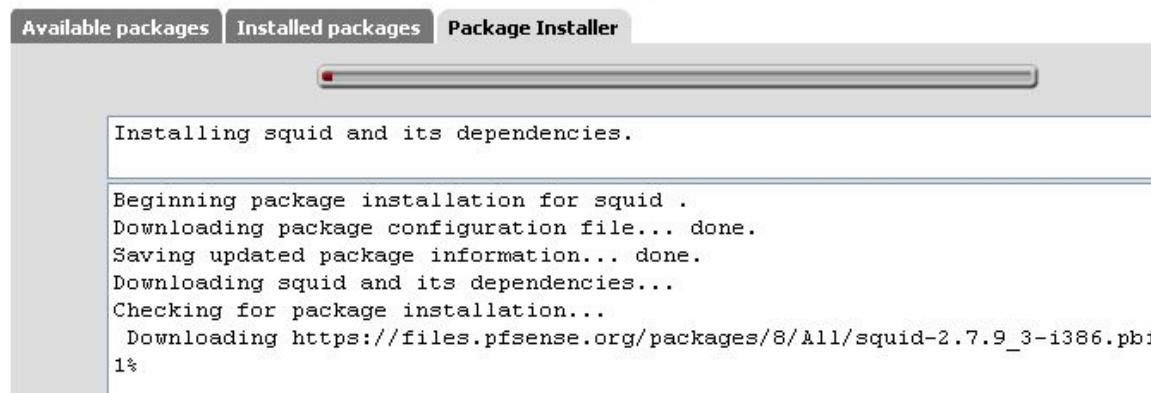
Chọn Confirm

System: Package Manager: Install Package



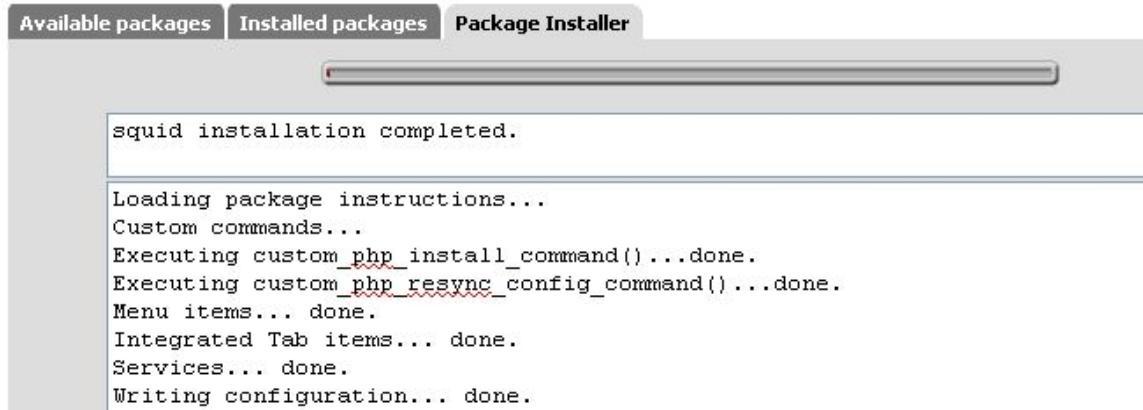
Quá trình cài bắt đầu

System: Package Manager: Install Package



Quá trình cài kết thúc

System: Package Manager: Install Package



1.2 cài gói squidGuard

System, Packages, chọn squidGuard, nhấn dấu +

			andvirus integration via Fcap Package info
squidGuard	Network Management	Beta 1.4_4 pkg v.1.9.6 platform: 1.1	High performance web proxy URL filter. Requires proxy Squid 2.x package. No package info, check the forum
squidGuard-devel	Network Management	Beta 1.5_1.1 beta platform: 2.1	High performance web proxy URL filter. Requires proxy Squid 2.x package. No package info, check the forum

1.3 cài gói Lightsquid

System, Packages, chọn Lightsquid, nhấn dấu +

		platform: 2.1	Package info
Lightsquid	Network Report	RC1 1.8.2 pkg v.2.33 platform: 2.0	High performance web proxy report (LightSquid). Proxy realtime stat (SQStat). Requires squid HTTP proxy. No package info, check the forum
LCDproc	Utility	BETA lcdproc-0.5.5 pkg.v.1.0.1 platform: 1.2.1	LCD display driver No package info, check the forum

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

Proxy server: General settings

General **Upstream Proxy** **Cache Mgmt** **Access Control** **Traffic Mgmt** **Auth Settings** **Local Users**

Proxy interface	<input type="button" value="LAN"/> <input type="button" value="WAN"/> <input type="button" value="loopback"/>	The interface(s) the proxy server will bind to.
Allow users on interface	<input checked="" type="checkbox"/>	If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.
Transparent proxy	<input checked="" type="checkbox"/>	If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

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

Enable logging	<input checked="" type="checkbox"/>	This will enable the access log. Don't switch this on if you don't have much disk space left.
Log store directory	<input type="text" value="/var/squid/logs"/>	The directory where the log will be stored (note: do not end with a / mark)
Log rotate	<input type="button" value=""/>	Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Proxy port	<input type="text" value="3128"/>	This is the port the proxy server will listen on.

Chọn Save

You can put your own custom options here, separated by semi-colons (;). They'll be added to the configuration. They need to be squid.conf native options, otherwise squid will NOT work.

Save

Tại máy client có thẻ 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

Proxy server: Cache management

A screenshot of the Squid configuration interface, specifically the 'Cache Mgmt' tab. The interface has several configuration sections:

- Hard disk cache size:** Set to 1000 MB. Description: This is the amount of disk space (in megabytes) to use for cached objects.
- Hard disk cache system:** Set to 'ufs'. Description: This specifies the kind of storage system to use. Options include 'ufs' (old well-known format), 'aufs' (uses POSIX-threads to avoid blocking the main Squid process on disk-I/O), 'diskd' (uses a separate process to avoid blocking the main Squid process on disk-I/O), and 'null' (does not use any storage, ideal for Embedded/NanoBSD).
- Hard disk cache location:** Set to '/var/squid/cache'. Description: This is the directory where the cache will be stored. Note: do not end with a '/'. If you change this, it may take a while.
- Memory cache size:** Set to 128 MB. Description: This is the amount of physical RAM (in megabytes) to be used for negative cache and in-transit objects. It should not exceed more than 50% of the installed RAM. The minimum value is 1MB.

Chọn save

3. Giới hạn truy cập

Service, chọn Proxy server, Access control

Banned host addresses: Nhập danh sách địa chỉ IP cấm truy cập

Blacklist : Danh sách web site cấm truy cập

Chọn Save

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Allowed subnets

Unrestricted IPs

Blacklist

Tại máy 10.0.0.50 truy cập web sẽ báo lỗi



ERROR

The requested URL could not be retrieved

While trying to retrieve the URL: <http://vnexpress.net/>

Tại máy 10.0.0.51 truy cập ngoisao.net sẽ báo lỗi



ERROR

The requested URL could not be retrieved

While trying to retrieve the URL: <http://ngoisao.net/>

The following error was encountered:

- Access Denied.

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

Proxy server: General settings

The screenshot shows the 'General' tab selected in a navigation bar with tabs: General, Upstream Proxy, Cache Mgmt, Access Control, Traffic Mgmt, Auth Settings, and Local Users. The 'General' tab is highlighted with a red border. Below the tabs, there are two main sections: 'Proxy interface' and 'Allow users on interface'. In the 'Proxy interface' section, there is a list of network interfaces: LAN (selected), WAN, and loopback. A note below says: 'The interface(s) the proxy server will bind to.' In the 'Allow users on interface' section, there is a checked checkbox labeled 'Allow users on interface'. A note below says: 'If this field is checked, the users connected to the interface selected in the 'Proxy interface' will be able to access the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets.' In the 'Transparent proxy' section, there is an unchecked checkbox labeled 'Transparent proxy'. A note below says: 'If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy. This requires additional configuration necessary.' The entire configuration page has a light gray background.

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

Proxy server: Local users: Edit

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Username Enter the username here.

Password Enter the password here.

Description You may enter a description here for your reference (not parsed).

Save **Cancel**

B2. Service, chọn Proxy server, Auth Settings

Authentication method: chọn Local

Chọn Save

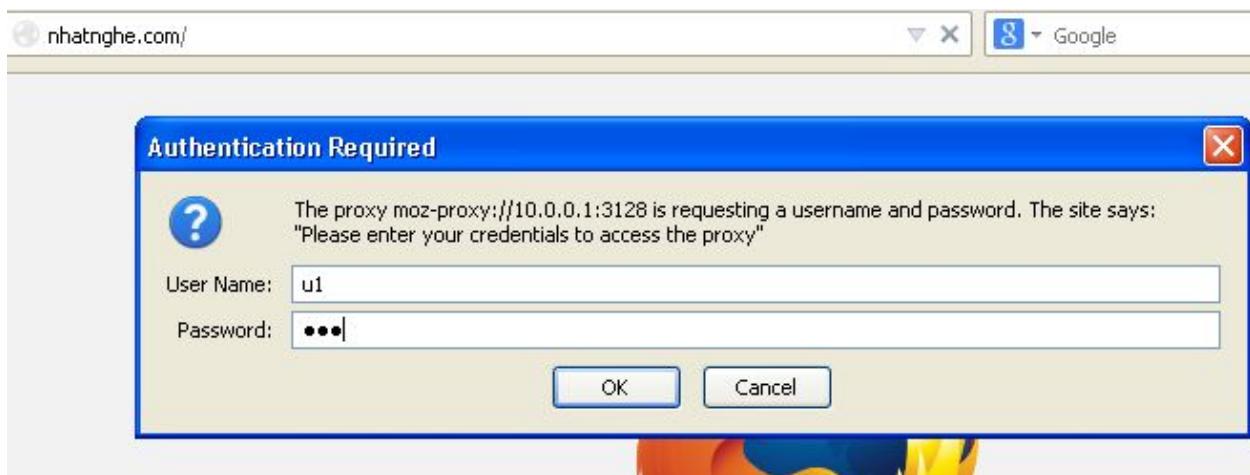
Proxy server: Authentication

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Authentication method Select an authentication method. This will allow users to be authenticated by local or external methods.

LDAP version Enter LDAP protocol version (2 or 3).

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

The screenshot shows the ADUC interface. On the left, the navigation pane displays the tree structure: 'Active Directory Users and Computers' -> 'nhatnghe1.com' -> 'nhanvien'. The 'nhanvien' container is selected. On the right, a table titled 'nhanvien 5 objects' lists the five users:

Name	Type	Description
hung	User	
ngoc	User	
u2	User	
u3	User	
u1	User	

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

Nhập các thông tin:

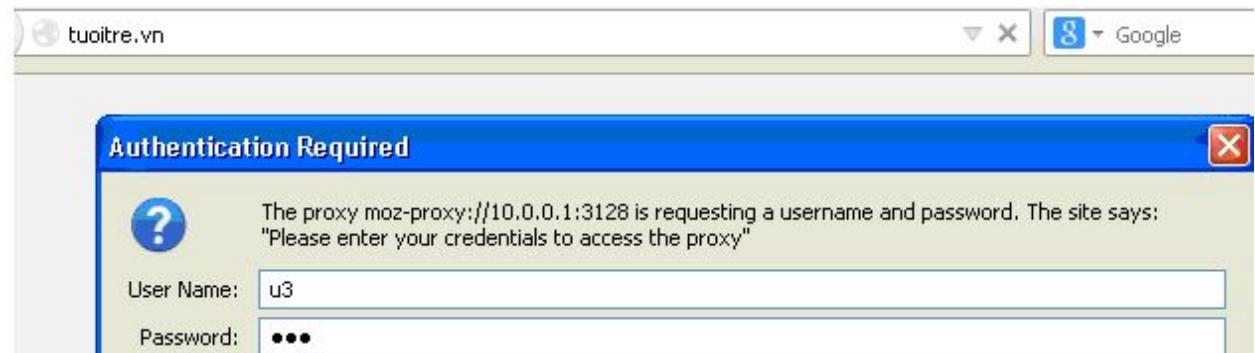
Authentication method: LAP
 LDAP version: 3
 Authentication server: 10.0.0.150
 Authentication server port: 389
 LDAP server user DN: cn=u1,ou=nhanvien,dc=nhatnghe1,dc=com
 LDAP password: 123
 LDAP base domain: dc=nhatnghe1,dc=com
 LDAP username DN attribute: uid
 LDAP search filter: sAMAccountName=%s

Chọn **Save**

Proxy server: Authentication

General	Upstream Proxy	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
Authentication method						
<input type="button" value="LDAP"/> <input type="button" value=""/>						
Select an authentication method. This will allow users to be authenticated by local or external servers.						
LDAP version						
<input type="button" value="3"/> <input type="button" value=""/>						
Enter LDAP protocol version (2 or 3).						
Authentication server						
<input type="button" value="10.0.0.150"/> <input type="button" value=""/>						
Enter here the IP or hostname of the server that will perform the authentication.						
Authentication server port						
<input type="button" value="389"/> <input type="button" value=""/>						
Enter here the port to use to connect to the authentication server. Leave this field blank to use the method's default port.						
NT domain						
<input type="button" value=""/> <input type="button" value=""/>						
Enter here the NT domain.						
LDAP server user DN						
<input type="button" value="cn=u1,ou=nhanvien,dc=rhatnghe1,dc=com"/> <input type="button" value=""/>						
Enter here the user DN to use to connect to the LDAP server.						
LDAP password						
<input type="button" value=""/> <input type="button" value="..."/> <input type="button" value=""/>						
Enter here the password to use to connect to the LDAP server.						
LDAP base domain						
<input type="button" value="dc=rhatnghe1,dc=com"/> <input type="button" value=""/>						
For LDAP authentication, enter here the base domain in the LDAP server.						
LDAP username DN attribute						
<input type="button" value="uid"/> <input type="button" value=""/>						
Enter LDAP username DN attribute.						
LDAP search filter						
<input type="button" value="sAMAccountName=%s"/> <input type="button" value=""/>						
Enter LDAP search filter.						

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



Truy cập thành công

TUỔI TRẺ CUỐI TUẦN | TUỔI TRẺ CƯỜI | TRUYỀN HÌNH TUỔI TRẺ | TUOTRENEWS

Thứ 3, Ngày 14.10.2014

tuoitre online

TRƯỜNG CAO ĐẲNG KINH TẾ - KỸ THUẬT VINATECH TP.HCM
(TRƯỜNG CÔNG LẬP)
HỆ TUYỂN NGUYỄN VĂN BỒ SUNG
CAO ĐẲNG CHÍNH QUY 2014
Thời gian từ ngày 01/10 đến 30/10/2014
DT: (08) 38 970 160 - (08) 3720 6426 | xem chi tiết >>>

Chi tiêu 700

0918.033.

Thuyền trưởng tàu Sunrise 689: "Tim tôi to đến đâu mà dám!"

Nội

5. Thông kê truy cập

5.1 Cấu hình chung

Status, Proxy reports, settings

Language: chọn English

Refresh scheduler: chọn 10min

Nhấn: Refresh

Chọn Save

Services: Proxy Reports (LightSquid, SQStat) -> Settings

Settings		Lightsquid Report	Proxy State
Language	<input type="button" value="English"/> <input type="button" value="Select report language"/>		
Bar color	<input type="button" value="Orange"/> <input type="button" value="Select bar color"/>		
Report scheme	<input type="button" value="Base"/> <input type="button" value="Select report scheme"/>		
IP resolve method (future)	<input type="button" value="IP"/> <input type="button" value="Select IP to Name resolve method (take effect only on new data):"/>		
Refresh scheduler	<input type="button" value="10min()"/> <input type="button" value="Select data refresh period. System will execute task every XX time as from 00:00 hours. For example: if selected 2h - system will start task at 0-2-4-..-24h. Note: (!),(*) - use only for powerful system; (+) - recommended."/>		
	<input type="button" value="Refresh now"/> <input type="button" value="Refresh full"/>		
	Press button for start background refresh (this take some time). Note after installation: On the first - enable log in squid package with "/var/squid/logs" path. On the second - press Refresh button for create lightsquid reports, else you will have error diagnostic page.		

5.2 Xem báo cáo truy cập

Status, Proxy reports, Lightsquid Report

Chọn tháng, ngày, Group cần xem báo cáo

Squid user access report											
Work Period: Oct 2014											
Calendar											
2014											
01	02	03	04	05	06	07	08	09	10	11	12

Date	Group	Users	Oversize	Bytes	Average	Hit %
13 Oct 2014	grp	1	0	7.0 M	7.0 M	0.00%
Total/Average:		1	0	7.0 M	7.0 M	0.00%

Thống kê theo User hoặc Top sites, Big files

Squid user access report						
Date: 13 Oct 2014 (update :: 18:36 :: 13 Oct 2014)						
Top Sites Report Big Files Report						
#	Time	User	Real Name	Connect	Bytes	%
00.	no in group					
1	⌚ 10.0.0.50			?	276 27.0 M	74.5%
2	⌚ 10.0.0.100			?	454 9.2 M	25.4%
					36.2 M	100.0%

Thống kê theo User

Squid user access report						
User: 10.0.0.50 (?)						
Group: ?						
Date: 13 Oct 2014						
						7.0 M
Total	#	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**

Proxy filter SquidGuard: General settings

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync
<input checked="" type="checkbox"/> Enable Check this option to enable squidGuard For saving configuration YOU need click button 'Save' on bottom of page After changing configuration squidGuard you must apply all changes <input type="button" value="Apply"/>	SquidGuard service state: STOPPED							

Chọn Common ACL, nhấp click here

Default access [all]: chọn allow
chọn: Save

Proxy filter SquidGuard: Common Access Control List (ACL)

Các máy client truy cập web bình thường

6.1 Blacklist

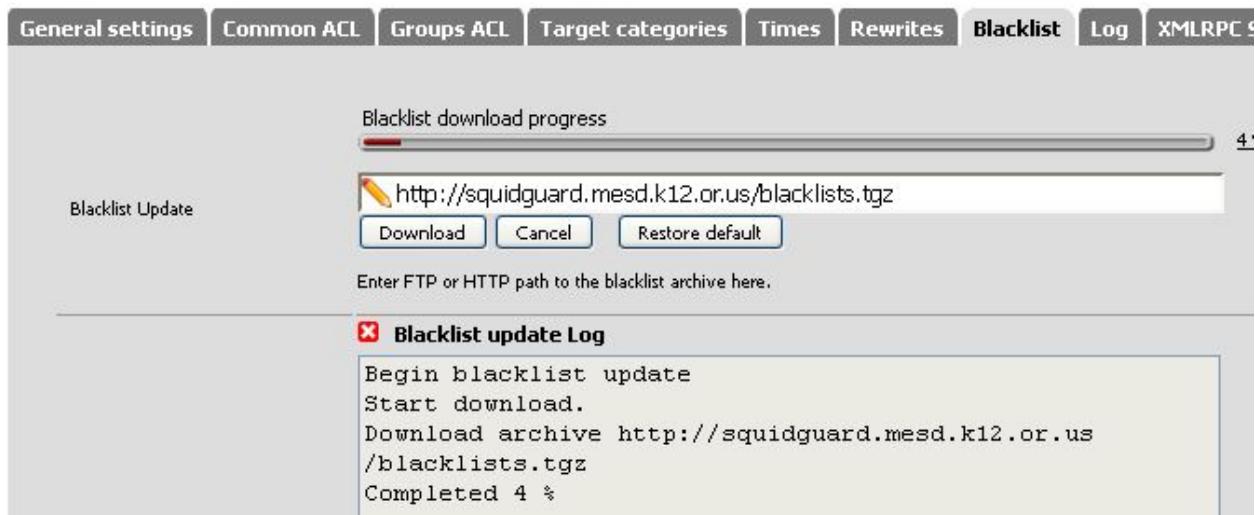
Service, Proxy filter, General Setting

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**

Proxy filter SquidGuard: Blacklist page



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

General settings **Common ACL** Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

Target Rules !blk_BL_shopping all

Target Rules List (click here)

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

Danh sach web bi cam truy cap [webdenry]	access ...
web trong gio [webtronggio]	access ...
[blk_BL_adv]	access ...
[blk_BL_shopping]	access deny
[blk_BL_socialnet]	access ...
[blk_BL_webphone]	access ...
[blk_BL_webradio]	access ...
[blk_BL_webtv]	access ...
Default access [all]	access allow

Redirect mode **int error page (enter error message)**
Select redirect mode here.
Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.
Options:ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.

Redirect info Trang web nay thuoc danh muc bi cam
Enter external redirection URL, error message or size (bytes) here.

Chọn Save, Apply

Tại máy client truy cập trang shopping.com

Request denied by pfSense proxy: 403 Forbidden

Reason: Trang web này thuộc danh mục bị cấm

Client address: 10.0.0.150

Client group: default

Target group: blk_BL_shopping

URL: http://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

Proxy filter SquidGuard: Target categories: Edit

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync
<p>Name <input type="text" value="webdeny"/>  Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-zA-Z0-9]. The first one must be a letter.</p> <p>Order <input type="text" value="....."/> Select the new position for this target category. Target categories are listed in this order on ALCs and are matched from the sequence.</p> <p>Domain List <input type="text" value="ngoisao.net 24h.com.vn"/></p>								

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

Redirect mode	<input type="checkbox"/> int error page (enter error message) <input checked="" type="checkbox"/>
Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.	
Redirect	Ban khong duoc truy cap trang nay
Enter the external redirection URL, error message or size (bytes) here.	
Description	Danh sach web bi cam truy cap You may enter any description here for your reference.
Log	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Chọn Common ACL

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

Proxy filter SquidGuard: Common Access Control List (ACL)

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync				
<p>Target Rules</p> <p>!webdeny all</p> <p>Target Rules List (click here) ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.</p> <table border="1"> <tr> <td colspan="2">Target Categories</td> </tr> <tr> <td>Danh sach web bi cam truy cap [webdeny] Default access [all]</td> <td>access <input type="button" value="deny"/> <input checked="" type="button" value="allow"/></td> </tr> </table>									Target Categories		Danh sach web bi cam truy cap [webdeny] Default access [all]	access <input type="button" value="deny"/> <input checked="" type="button" value="allow"/>
Target Categories												
Danh sach web bi cam truy cap [webdeny] Default access [all]	access <input type="button" value="deny"/> <input checked="" type="button" value="allow"/>											

Chọn General settings, Apply

Proxy filter SquidGuard: General settings

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync
<p>Enable <input checked="" type="checkbox"/> Check this option to enable squidGuard For saving configuration YOU need click button 'Save' on bottom of page After changing configuration squidGuard you must apply all changes</p> <p>Apply</p> <p>SquidGuard service state: STARTED</p>								

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

Chú ý: xóa cache trình duyệt nếu cần

Request denied by pfSense proxy: 403 Forbidden

Reason: Ban khong duoc truy cap trang nay

Client address: 10.0.0.50
Client group: default
Target group: webdeny
URL: http://ngoisao.net/

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 điểm 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

General settings		Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log
Name	<input type="text" value="webtronggio"/>							
Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-zA-Z_0-9]. The first one must be a letter.								
Order	<input type="text" value="....."/>							
Select the new position for this target category. Target categories are listed in this order on ALCs and are in sequence.								
Domain List	<input type="text" value="vnexpress.net nhatnghe.com"/>							

B2. Service, Proxy filter, General Setting, Times

Name: giolamviec

Values: weekly 08:00-12:00
weekly 13:00-17:00

Description: Gio lam viec
Chon Save

Values	Time type	Days	Date or Date range	Time range
	Weekly	all		08:00-12:00
	Weekly	all		13:00-17:00

Description: Gio lam viec

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

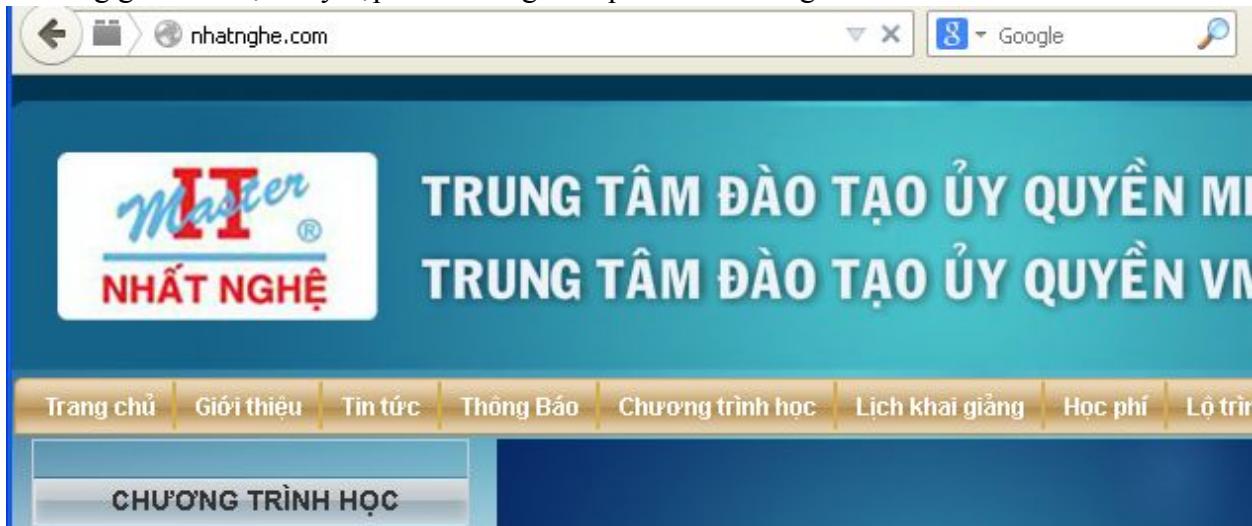
Client (source)
10.0.0.10-10.0.0.100

Time	giolamviec	Select the time in which 'Target Rules' will operate or leave 'none' for rules without time restriction. If this option is set then in off-time the second ruleset will operate.						
Target Rules	!webdeny webtronggio !all [!webdeny webtronggio all]							
Target Rules List (click here) <p>ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Target Categories</th> <th style="text-align: center;">Target Categories for off-time</th> </tr> </thead> <tbody> <tr> <td>Danh sach web bi cam truy cap [webdeny] web trong gio [webtronggio] Default access [all]</td> <td style="text-align: center;"> access deny access allow access deny </td> <td style="text-align: center;"> Danh sach web bi cam truy cap [webdeny] web trong gio [webtronggio] Default access [all] </td> <td style="text-align: center;"> access deny access allow access allow </td> </tr> </tbody> </table>			Target Categories	Target Categories for off-time	Danh sach web bi cam truy cap [webdeny] web trong gio [webtronggio] Default access [all]	access deny access allow access deny	Danh sach web bi cam truy cap [webdeny] web trong gio [webtronggio] Default access [all]	access deny access allow access allow
Target Categories	Target Categories for off-time							
Danh sach web bi cam truy cap [webdeny] web trong gio [webtronggio] Default access [all]	access deny access allow access deny	Danh sach web bi cam truy cap [webdeny] web trong gio [webtronggio] Default access [all]	access deny access allow access allow					
Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.							
Redirect mode	int error page (enter error message) <input type="button" value="▼"/> <p>Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.</p>							
Redirect	Trong gio lam viec khong duoc truy cap trang nay							
	Enter the external redirection URL, error message or size (bytes) here.							

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.

Request denied by pfSense proxy: 403 Forbidden

Reason: Trong gio khong duoc vao trang nay

Client address: 10.0.0.20

Client group: web_lamviec

Target group: none

URL: http://google.com/

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 điểm 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

General settings **Common ACL** **Groups ACL** **Target categories** **Times** **Rewrites** **Blacklist** **Log** **XMLRPC Sync**

Disabled	<input type="checkbox"/>	Check this to disable this ACL rule.																														
Name	<input type="text" value="web_kogioihan"/>																															
Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-zA-Z_0-9]. The first one must be a letter.																																
Client (source)	<input type="text" value="10.0.0.101-10.0.0.254"/>																															
Time	<input type="text" value="none (time not defined)"/>																															
Select the time in which 'target Rules' will operate or leave 'none' for rules without time restriction. If this option is set then in off-time the second ruleset will operate.																																
Target Rules	<input type="text" value="!webdeny webtronggio all [!webdeny webtronggio all]"/>																															
Target Rules List (click here) <p>ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.</p> <table border="1"> <thead> <tr> <th colspan="3">Target Categories</th> <th colspan="3">Target Categories for off-time</th> </tr> <tr> <th colspan="3"></th> <th colspan="3">If 'Time' not defined, this column will be ignored.</th> </tr> </thead> <tbody> <tr> <td>Danh sach web bi cam truy cap [webdeny]</td> <td>access</td> <td>deny</td> <td>Danh sach web bi cam truy cap [webdeny]</td> <td>access</td> <td>deny</td> </tr> <tr> <td>web trong gio [webtronggio]</td> <td>access</td> <td>allow</td> <td>web trong gio [webtronggio]</td> <td>access</td> <td>allow</td> </tr> <tr> <td>Default access [all]</td> <td>access</td> <td>allow</td> <td>Default access [all]</td> <td>access</td> <td>allow</td> </tr> </tbody> </table>			Target Categories			Target Categories for off-time						If 'Time' not defined, this column will be ignored.			Danh sach web bi cam truy cap [webdeny]	access	deny	Danh sach web bi cam truy cap [webdeny]	access	deny	web trong gio [webtronggio]	access	allow	web trong gio [webtronggio]	access	allow	Default access [all]	access	allow	Default access [all]	access	allow
Target Categories			Target Categories for off-time																													
			If 'Time' not defined, this column will be ignored.																													
Danh sach web bi cam truy cap [webdeny]	access	deny	Danh sach web bi cam truy cap [webdeny]	access	deny																											
web trong gio [webtronggio]	access	allow	web trong gio [webtronggio]	access	allow																											
Default access [all]	access	allow	Default access [all]	access	allow																											
Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/>		To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.																													
Redirect mode	<input type="text" value="none"/>		Select redirect mode here.																													

Chọn Save

Kết quả có 2 rule được tạo

General settings **Common ACL** **Groups ACL** **Target categories** **Times** **Rewrites** **Blacklist** **Log** **XMLRPC Sync**

Disabled	Name	Time	Description		
	web_kogioihan		web_khong_gioihan		
	web_lamviec	giolamviec	web trong gio lam viec		

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

JỎI TRẺ CUỐI TUẦN | TUỔI TRẺ CƯỜI | TRUYỀN HÌNH TUỔI TRẺ | TUOTRENEWS

Thứ 5, Ngày 16.10.2014

tuổi trẻ online

TRƯỜNG CAO ĐẲNG KINH TẾ - KỸ THUẬT VINATECH TP.HCM
(TRƯỜNG CÔNG LẬP)
XÉT TUYỂN NGUYỄN VƯƠNG BỔ SUNG
CAO ĐẲNG CHÍNH QUY 2014
Thời gian từ ngày 01/10 đến 30/10/2014
ĐT: (08) 38 970 160 - (08) 3720 6426 | xem chi tiết >>>
Chỉ tiêu
700

7. HAVP (HTTP Antivirus Proxy)

System, Packages, cài gói HAVP Antivirus

System: Package Manager

Available Packages		Installed Packages	
Name	Category	Version	Description
HAVP antivirus	Network Management	0.91_1 pkg v1.02	Antivirus: HAVP (HTTP Antivirus Proxy) is a proxy with a ClamAV anti-virus scanner. The main aims are continuous, non-blocking downloads and smooth scanning of dynamic and password protected HTTP traffic. Havp antivirus proxy has a parent and transparent proxy mode. It can be used with squid or standalone. And File Scanner for local files. No package info, check the forum
Lightsquid	Network Report	1.8.2 pkg v.2.33	High performance web proxy report (LightSquid). Proxy realtime stat (SQStat). Requires squid HTTP proxy.

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*

Proxy server: General settings

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local User

Proxy interface



The interface(s) the proxy server will bind to.

Allow users on interface If this field is checked, the users connected to the interface selected in the 'Proxy interface' will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed interfaces.

Transparent proxy If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy. This requires additional configuration necessary.

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 |

Antivirus: HTTP proxy (havp + clamav)

General page **HTTP proxy** Settings

Enable Check this for enable proxy.

Proxy mode Select interface mode:
standard - client(s) bind to the 'proxy port' on selected interface(s);
parent for squid - configure HAVP as parent for Squid proxy;
transparent - all HTTP requests on interface(s) will be directed to the HAVP proxy server; no configuration necessary (works as parent for squid with transparent Squid proxy);
internal - HAVP will listen on the loopback (127.0.0.1) on configured 'proxy port.' Use your own port number if you want to use it with squid.

Proxy interface(s)

Log Check this for enable log.

Syslog Check this for enable Syslog.

Save

Log check
Syslog check
Chọn Save

B3. Cấu hình cập nhật 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

General page **HTTP Proxy** **Settings** **Antivirus: Settings**

AV base update Press button for update AV database now.

Regional AV database update mirror Select regional database mirror.

Optional AV database update servers
Enter here space separated AV update servers, or leave empty.

Log Check this for enable log.

SysLog Check this for enable SysLog.

Save

B4. Kiểm tra các dịch vụ đã chạy

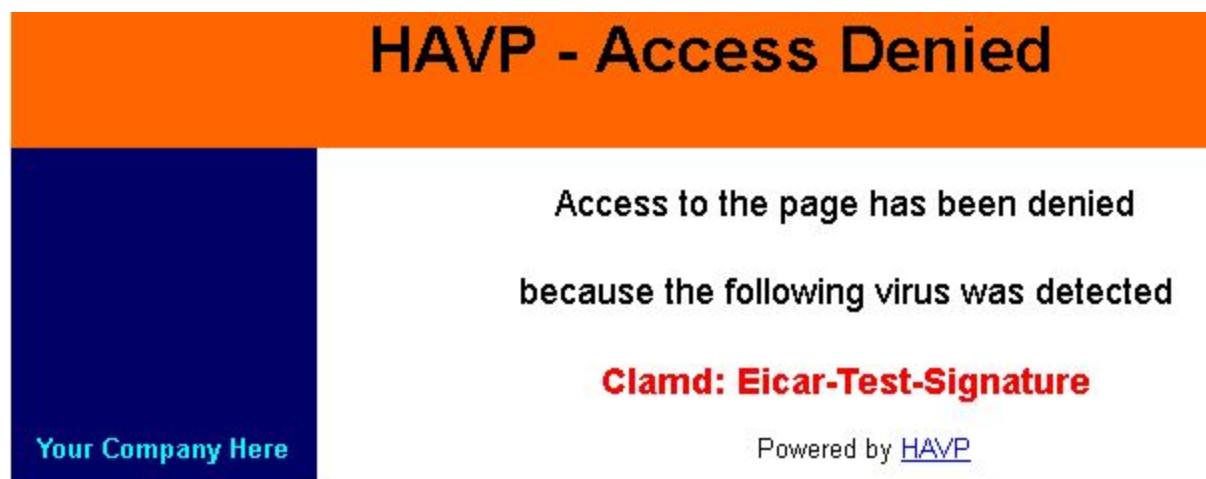
Antivirus: General page

General page	HTTP proxy	Settings				
Service	Status	Version				
HTTP Antivirus Proxy (Started)	Running					
Antivirus Server (Started)	Running	ClamAV 0.97.6/19520/Thu Oct 16 21:12:57 2014				
Antivirus Update	Update status					
Start Update	Not found.					
Antivirus Base Info	Database	Date	Size	Ver.	Signatures	Builder
	main.cvd	2013.09.17	61.72 M	55	2424225	neo
	daily.cvd	2014.10.16	28.96 M	19520	1209163	jesler
	bytecode.cvd	2014.06.24	0.07 M	242	46	dgoddard

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, aliases, IP, nhấp dấu +

Firewall: Aliases

IP Ports URLs All

Name

Values

Description



Note:

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

Alias Edit

Name

Gioi_han_bandwidth

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

Gioi han toc do down/up load

You may enter a description here for your reference (not parsed).

Type

Network(s)

Network(s)

Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry

Network	CIDR	Description
---------	------	-------------

10.0.0.100-10.0.0.200

128



Save

Cancel

Nhấn Apply Change

Firewall: Aliases

The alias list has been changed.
 You must apply the changes in order for them to take effect.

Apply changes

IP Ports URLs All

Name

Values

Description

Gioi_han_bandwidth

10.0.0.100/30, 10.0.0.104/29, 10.0.0.112/28, 10.0.0.128/26,
 10.0.0.192/29, 10.0.0.200/32

Gioi han toc do down/u

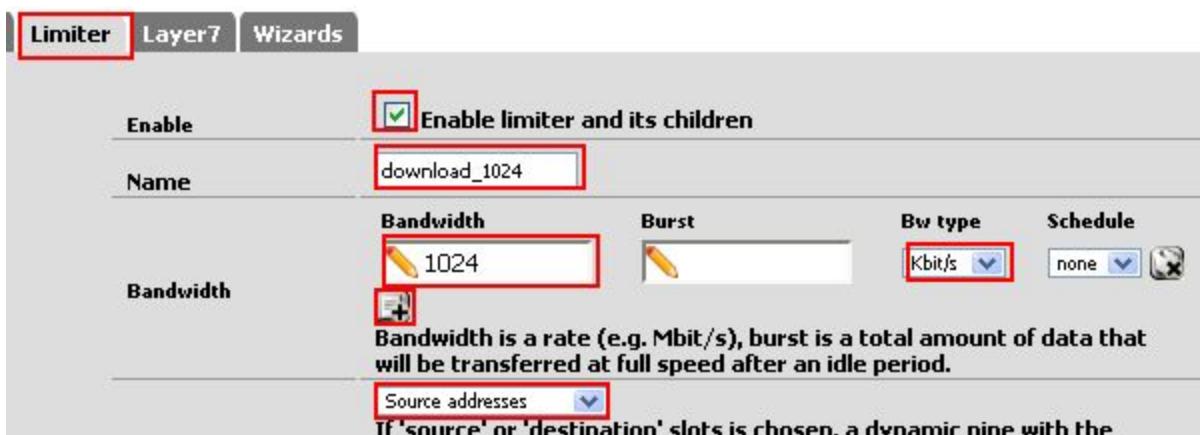
B2. Firewall, Traffic Shaper, Limiter

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 tốc 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	

Limiter Layer7 Wizards

Enable	<input checked="" type="checkbox"/> Enable limiter and its children
Name	upload_100
Bandwidth	<input type="text" value="100"/>  <p>Bandwidth is a rate (e.g. Mbit/s), burst is a total amount of data that will be transferred at full speed after an idle period.</p>
Burst	<input type="text"/>
Bw type	Kbit/s
Schedule	none
Source addresses  <p>If 'source' or 'destination' slots is chosen, a dynamic pipe with the</p>	

Nhấp Apply changes



By Interface By Queue Limiter Layer7 Wizards

 download_1024  upload_100	Enable	<input checked="" type="checkbox"/> Enable limiter and its children
	Name	upload_100

B3. Khai báo giờ làm việc
Firewall, Schedules, nhấp +

Schedule information																																											
Schedule Name	giolamviec NOTE: This schedule is in use so the name may not be modified!																																										
Description	gio lam viec You may enter a description here for your reference (not parsed).																																										
Month	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="October_14"/> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; margin-top: 5px;"> <p style="text-align: center;">October_2014</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #f0f0f0;">Mon</th> <th style="background-color: #f0f0f0;">Tue</th> <th style="background-color: #f0f0f0;">Wed</th> <th style="background-color: #f0f0f0;">Thu</th> <th style="background-color: #f0f0f0;">Fri</th> <th style="background-color: #f0f0f0;">Sat</th> <th style="background-color: #f0f0f0;">Sun</th> </tr> </thead> <tbody> <tr><td></td><td></td><td style="text-align: center;">1</td><td style="text-align: center;">2</td><td style="text-align: center;">3</td><td style="text-align: center;">4</td><td style="text-align: center;">5</td></tr> <tr><td style="text-align: center;">6</td><td style="text-align: center;">7</td><td style="text-align: center;">8</td><td style="text-align: center;">9</td><td style="text-align: center;">10</td><td style="text-align: center;">11</td><td style="text-align: center;">12</td></tr> <tr><td style="text-align: center;">13</td><td style="text-align: center;">14</td><td style="text-align: center;">15</td><td style="text-align: center;">16</td><td style="text-align: center;">17</td><td style="text-align: center;">18</td><td style="text-align: center;">19</td></tr> <tr><td style="text-align: center;">20</td><td style="text-align: center;">21</td><td style="text-align: center;">22</td><td style="text-align: center;">23</td><td style="text-align: center;">24</td><td style="text-align: center;">25</td><td style="text-align: center;">26</td></tr> <tr><td style="text-align: center;">27</td><td style="text-align: center;">28</td><td style="text-align: center;">29</td><td style="text-align: center;">30</td><td style="text-align: center;">31</td><td></td><td></td></tr> </tbody> </table> </div>	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		
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	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; width: 450px; margin-bottom: 10px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Start Time</td> <td style="width: 50%; padding: 5px;">Stop Time</td> </tr> <tr> <td style="padding: 5px;"> <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="8"/> Hr <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="00"/> Min </td> <td style="padding: 5px;"> <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="12"/> Hr <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="00"/> Min </td> </tr> </table> </div> <p>Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.</p>	Start Time	Stop Time	<input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="8"/> Hr <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="00"/> Min	<input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="12"/> Hr <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="00"/> Min																																						
Start Time	Stop Time																																										
<input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="8"/> Hr <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="00"/> Min	<input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="12"/> Hr <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="00"/> Min																																										
Time Range Description	sang You may enter a description here for your reference (not parsed).																																										
	<input style="border: 1px solid red; border-radius: 5px; padding: 2px 10px; margin-right: 10px;" type="button" value="Add Time"/> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="Clear Selection"/>																																										

Khai báo thông tin như hình, chọn **Add Time**

Nhập thôn tin buổi chiều

Month	October_14																																																	
<table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th colspan="7">October_2014</th> </tr> <tr> <th>Mon</th><th>Tue</th><th>Wed</th><th>Thu</th><th>Fri</th><th>Sat</th><th>Sun</th></tr> </thead> <tbody> <tr><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> <tr><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr> <tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr> <tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td></tr> <tr><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td><td></td></tr> </tbody> </table>		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		
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	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 50%;">Start Time</td> <td style="width: 50%;">Stop Time</td> </tr> <tr> <td>13 <input type="button" value="▼"/> Hr 00 <input type="button" value="▼"/> Min</td> <td>17 <input type="button" value="▼"/> Hr 00 <input type="button" value="▼"/> Min</td> </tr> </table>	Start Time	Stop Time	13 <input type="button" value="▼"/> Hr 00 <input type="button" value="▼"/> Min	17 <input type="button" value="▼"/> Hr 00 <input type="button" value="▼"/> Min																																													
Start Time	Stop Time																																																	
13 <input type="button" value="▼"/> Hr 00 <input type="button" value="▼"/> Min	17 <input type="button" value="▼"/> Hr 00 <input type="button" value="▼"/> 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 <p>You may enter a description here for your reference (not parsed).</p>																																																	
<input type="button" value="Add Time"/> <input type="button" value="Clear Selection"/>																																																		
Schedule repeat																																																		
Configured Ranges	<table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th>Day(s)</th> <th>Start Time</th> <th>Stop Time</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Mon - Sun</td> <td>8:00</td> <td>12:00</td> <td>sang</td> </tr> </tbody> </table>	Day(s)	Start Time	Stop Time	Description	Mon - Sun	8:00	12:00	sang																																									
Day(s)	Start Time	Stop Time	Description																																															
Mon - Sun	8:00	12:00	sang																																															
<input type="button" value="Save"/> <input type="button" value="Cancel"/>																																																		

Chọn save

Firewall: Schedules

Name	Time Range(s)			Description	
giolamviec	Mon - Sun	8:00-12:00	sang	gio lam viec	

Note:
Schedules act as placeholders for time ranges to be used in Firewall Rules.

B4. Tạo rules

Firewall, Rules, LAN, nhấp +

Firewall: Rules

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>		*	*	*	LAN Address 443 80 22	*	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Khai báo các thông tin sau:

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

Edit Firewall rule

Action	<input style="border: 1px solid red; width: 100px; height: 25px;" type="button" value="Pass"/> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the connection is closed.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input style="border: 1px solid red; width: 100px; height: 25px;" type="button" value="LAN"/> <p>Choose on which interface packets must come in to match this rule.</p>
TCP/IP Version	<input style="border: 1px solid red; width: 100px; height: 25px;" type="button" value="IPv4"/> Select the Internet Protocol version this rule applies to
Protocol	<input style="border: 1px solid red; width: 100px; height: 25px;" type="button" value="TCP"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="border: 1px solid red; width: 100px; height: 25px;" type="button" value="Single host or alias"/> Address: <input style="border: 1px solid red; width: 150px; height: 25px;" type="text" value="Gioi_han_bandwidth"/> / <input style="border: 1px solid red; width: 20px; height: 25px;" type="button" value="32"/> <input style="border: 1px solid blue; width: 100px; height: 25px;" type="button" value="Advanced"/> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="border: 1px solid red; width: 100px; height: 25px;" type="button" value="any"/> Address: <input style="width: 150px; height: 25px;" type="text"/> / <input style="width: 20px; height: 25px;" type="button" value="127"/>

Schedule giolamviec
 In: upload_100
 Out: download_1024

Advanced features

Source OS	<input type="button" value="Advanced"/> - Show advanced option
Schedule	<input type="text" value="giolamviec"/> <input type="button"/>
Leave as 'none' to leave the rule enabled all the time.	
Gateway	<input type="button" value="Advanced"/> - Show advanced option
In/Out	<input type="text" value="upload_100"/> <input type="button"/> / <input type="text" value="download_1024"/> <input type="button"/>
Choose the Out queue/virtual interface only if you have also selected In. The Out selection is applied to traffic leaving the interface where the rule is created, In is chosen interface. If you are creating a floating rule, if the direction is In then the same rules apply, if the dir reverted Out is for incoming and In is for outgoing.	

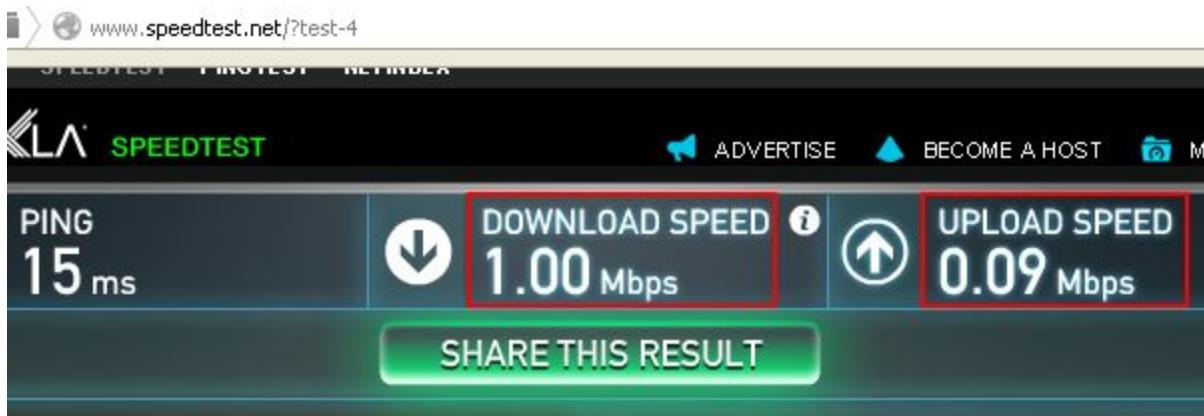
Chọn save

Rule vừa tạo phải di chuyển lên cùng

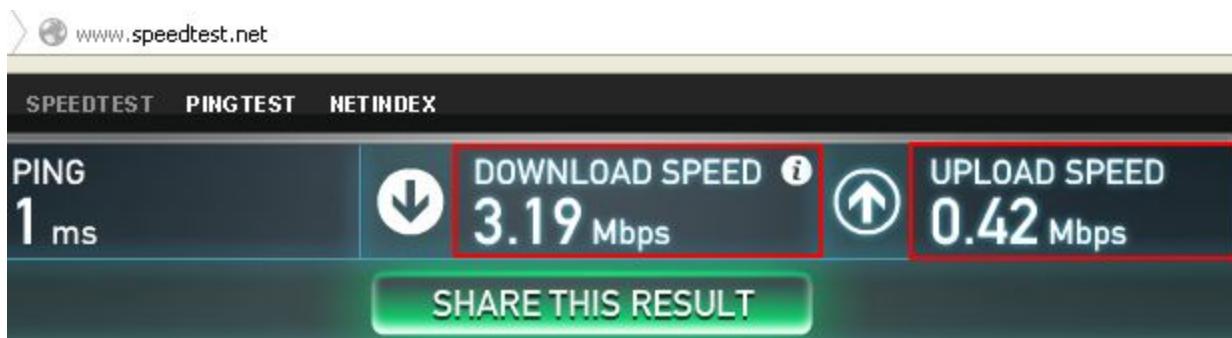
The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

Floating	WAN	LAN	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	<input type="button"/> <input type="button"/>
<input checked="" type="checkbox"/>				*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	<input type="button"/> <input type="button"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		a	IPv4 TCP	Gioi han bandwidth	*	*	*	*	none		Lan - Internet: gioi han bandwidth	<input type="button"/> <input type="button"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>			IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	<input type="button"/> <input type="button"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>			IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	<input type="button"/> <input type="button"/>

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	

Services: DHCP server

Pool Start	Pool End	Description
10.0.0.100	10.0.0.245	

WINS servers:

DNS servers: 10.0.0.10

NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, the servers configured on the General page.

Gateway: 10.0.0.10

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway not the correct gateway for your network.

B2. client xin IP

```
C:\>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:

#2      Connection-specific DNS Suffix  . . . . . : VMware Accelerate
    Description . . . . . : VMware Accelerator
    Physical Address. . . . . : 00-0C-29-26-1A-
    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 +

System: User Manager

Users	Groups	Settings	Servers
Username	Full name	Disabled	Groups
 admin	System Administrator		admins 

Username Nhập wifi
Password Nhập 123
Chọn Save

Defined by	USER
Disabled	<input type="checkbox"/>
Username	wifi
Password	<input type="password"/> <input type="password"/>
	(confirmation)

B4. Cấu hình Captiveportal

Service, Captiveportal, nhấn +

Captiveportal: Zones

Zone	Interfaces	Number of users	Description		

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

Edit Captiveportal Zones

Zone name	LAN Zone name. Can only contain letters, digits, and underscores (_).
Description	Ket noi wifi You may enter a description here for your reference (not parsed).

Continue

B5. Cấu hình Captiveportal

Enable captive portal check
 Interfaces chọn LAN

Services: Captive portal: LAN

Captive portal(s)	Pass-through MAC	Allowed IP addresses	Allowed Hostnames	Vouchers	File Manager
<input checked="" type="checkbox"/> Enable captive portal					
Interfaces	<input type="checkbox"/> WAN <input checked="" type="checkbox"/> LAN <small>Select the interface(s) to enable for captive portal.</small>				

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

Per-user bandwidth restriction **Enable per-user bandwidth restriction**

Default download	<input type="text" value="1024"/> Kbit/s
Default upload	<input type="text" value="512"/> Kbit/s

If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. override the default settings. Leave empty or set to 0 for no limit.

Authentication No Authentication Local User Manager / Vouchers Allow only users/groups with 'Captive portal login' privilege set RADIUS Authentication

Khai báo file chứa code trang web login

Portal page contents login.html

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make (POST to "") with a submit button (name="accept") and a hidden field with name="redirurl" an "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, fail. Example code for the form:

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

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



Thank you for connecting to our network.

Please enter your username and password to access the Internet

Username: wifi

Password: ***

Login

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 +

Services: Captive portal: wifi

IP address	Description
10.0.0.0/25	Khong yeu cau chung thuc

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

Chọn **Save**

Edit allowed ip rule

IP address	<input type="text" value="10.0.0.0"/> /25	IP address and subnet mask. Use /32 for a single IP.
Description	<input type="text" value="Khong yeu cau chung thuc"/> You may enter a description here for your reference (not parsed).	
Bandwidth up	<input type="text"/>	
Bandwidth down	<input type="text"/>	

Save

Kết quả:

Services: Captive portal: wifi

IP address	Description
10.0.0.0/25	Khong yeu cau chung thuc

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 yêu cầu nhập user/pass với các MAC address hoặc hostname chỉ định trong các mục: pass-through MACs, allowed Hostnames.

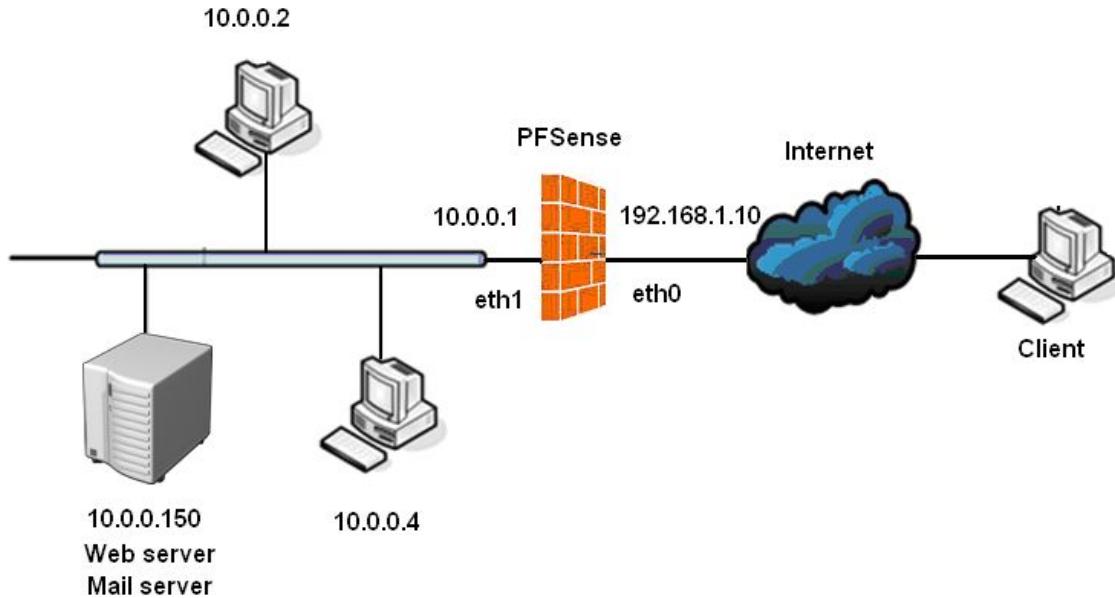
B8.

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

Status: Captive portal

Captiveportal status				
IP address	MAC address	Username	Session start	Last activity
10.0.0.123	00:0c:29:26:1a:7a	wifi	10/31/2014 11:02:36	10/31/2014 11:05:36
10.0.0.150	00:0c:29:26:1a:7a	wifi	10/31/2014 11:35:17	10/31/2014 11:54:57

SERVER PUBLISHING



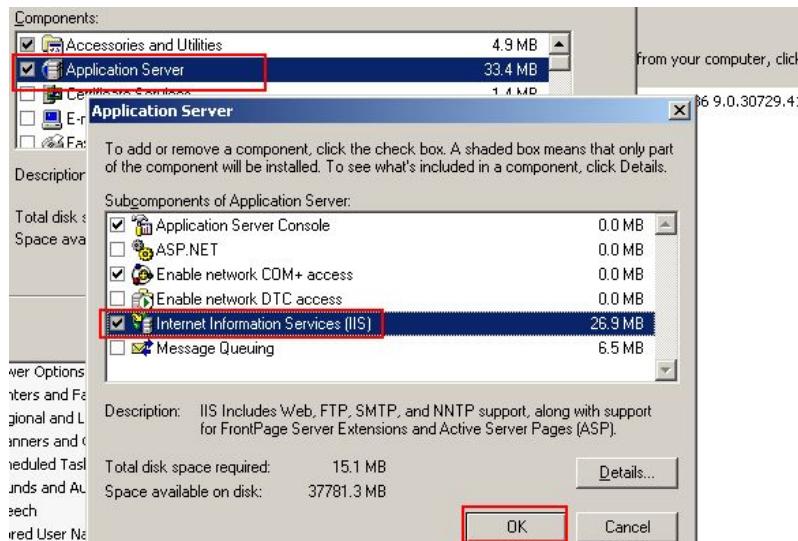
1. Publish Web server

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 +

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	Actions
pass									
linked rule									

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

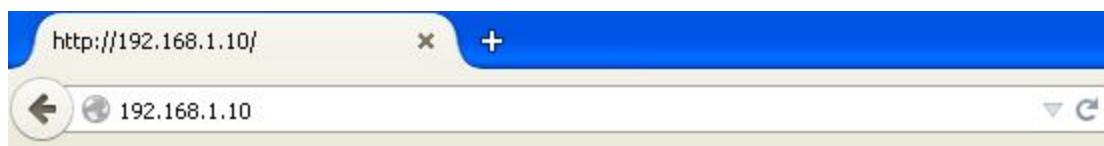
Edit Redirect entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
No RDR (NOT)	<input type="checkbox"/> Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	<input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="WAN"/> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	<input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="TCP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="any"/> Address: / 31
Source port range	from: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="any"/> to: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="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	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="WAN address"/> Address: / 31
Destination port range	from: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="HTTP"/> to: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="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	<input type="text" value="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	<input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="HTTP"/> Specify the port on the machine with the IP address entered above. In case of a port range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	<input type="text" value="Publish Web server"/>
	You may enter a description here for your reference (not parsed).

Chọn Save
Nhập Apply changes

Firewall: NAT: Port Forward

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>	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



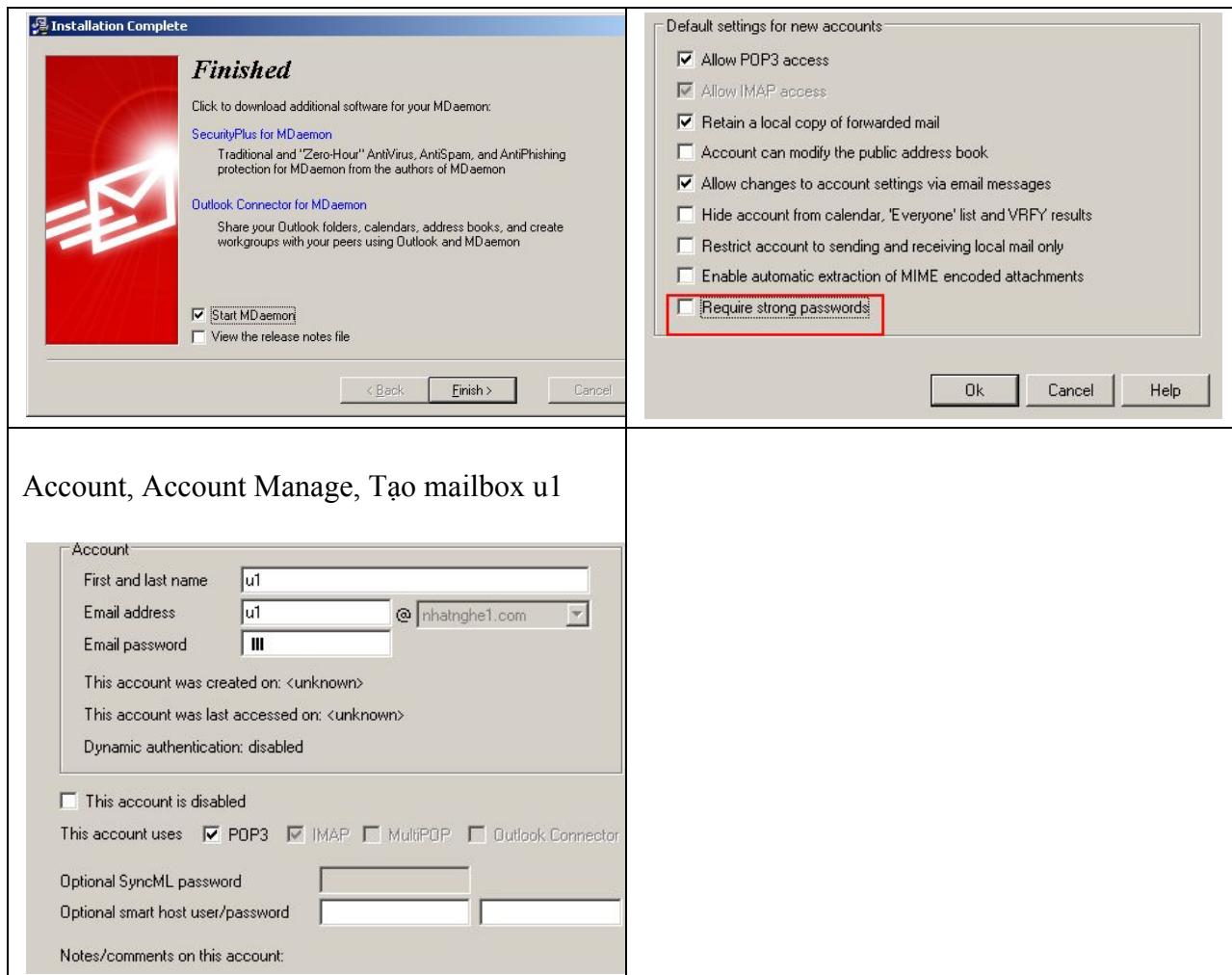
Web dat ben trong mang LAN

2. Publish Mail server (POP3 & SMTP)

Máy 10.0.0.150 cài Mdaemon làm mail server
B1.

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

<p>License Agreement</p> <p>Alt-N Technologies End-User License Agreement (EULA)</p> <p>LICENSE AGREEMENT</p> <p>Please read this entire agreement. If you do not agree to the terms of this agreement promptly return your distribution materials to the place you obtained them for a full refund or delete your trial package.</p> <p>ALT-N TECHNOLOGIES END-USER LICENSE AGREEMENT</p> <p>This End-User License Agreement ("EULA") is a legal agreement between you ("Customer" or "Sub Licensee") and Alt-N Technologies ("Licensor") for the Alt-N software product(s) you are installing which include(s) computer software, "online" or electronic documentation, and may include associated media and printed materials ("SOFTWARE PRODUCT" or "SOFTWARE").</p> <p>< Back Agree > Cancel</p>	<p>Select Destination Directory</p> <p>Please select the root directory where MDaemon Server files are to be installed.</p> <p>If you are upgrading an existing installation please provide the path to the previous installation's root MDaemon directory. For example, if the previous version's MDaemon.exe file is located in c:\mdaemon\app then just enter c:\mdaemon here.</p> <p>For new installations, this process will create a directory structure off the stem directory like this: c:\stem\app, c:\stem\remoted, etc... just enter the c:\stem part.</p> <p>C:\MDaemon Browse... < Back Next > Cancel</p>
<p>Nhấn Next bắt đầu cài đặt</p> <p>Ready to Install!</p> <p>You are now ready to install MDaemon Server.</p> <p>Press the Next button to begin the installation or the Back button to reenter the installation information.</p> <p>< Back Next > Cancel</p>	<p>Nhập tên domain: nhatnghe1.com</p> <p>What Is Your Domain Name?</p> <p>Please enter your domain name here. Your domain name is the part to the right of the @ symbol in your email address.</p> <p>Domain name nhatnghe1.com < Back Next > Cancel</p>
<p>Tạo mailbox admin</p> <p>Please Set Up Your First Account</p> <p>You can set up more accounts from within MDaemon later.</p> <p>This account will be set up with the RFC required 'Postmaster' alias.</p> <p>Full name (ex: Frank Thomas) admin Mailbox (ex: Frank - don't include a domain name) admin Password (ex: Swordfish - no spaces) ***</p> <p>Use upper and lower case letters and numbers in your password. Also, the password must be between 6 and 12 characters in length. Do not include the mailbox or full name as part of the password.</p> <p><input checked="" type="checkbox"/> This account is an administrator - full configuration access is granted</p> <p>< Back Next > Cancel</p>	<p>Khai báo DNS</p> <p>Please Set Up Your DNS</p> <p>If you want to use specific DNS servers you can configure them here. Otherwise, MDaemon can use the DNS settings already present in Windows.</p> <p><input checked="" type="checkbox"/> Use Windows DNS settings Primary DNS IP Address 8.8.8.8 (optional) Backup DNS IP Address (optional)</p> <p>< Back Next > Cancel</p>
<p>Nhấn Finish</p>	<p>Account, Account setting, bỏ check yêu cầu password phức tạp</p>



B2. Tạo rule
Firewall, NAT, chọn Port Forward WAN, nhấn +

Firewall: NAT: Port Forward

Port Forward									?	
	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.150	80 (HTTP)	Publish Web server	

Firewall: NAT: Port Forward: Edit

Edit Redirect entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
No RDR (NOT)	<input type="checkbox"/> 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	<input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="WAN"/> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	<input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="TCP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="any"/> Address: <input style="width: 20px;" type="text" value="1"/> / <input style="border: 1px solid red; padding: 2px;" type="button" value="31"/>
Source port range	from: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="any"/> to: <input style="border: 1px solid red; padding: 2px;" type="button" value="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	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="WAN address"/> Address: <input style="width: 20px;" type="text" value="1"/> / <input style="border: 1px solid red; padding: 2px;" type="button" value="31"/>
Destination port range	from: <input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="SMTP"/> to: <input style="border: 1px solid red; padding: 2px;" type="button" value="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	<input style="background-color: #e00; color: black; border: 1px solid black; width: 150px; height: 20px;" type="text" value="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	<input style="border: 1px solid red; padding: 2px; margin-right: 10px;" type="button" value="SMTP"/> Specify the port on the machine with the IP address entered above. In case of a port range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	<input style="border: 1px solid red; width: 150px; height: 20px;" type="text" value="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:

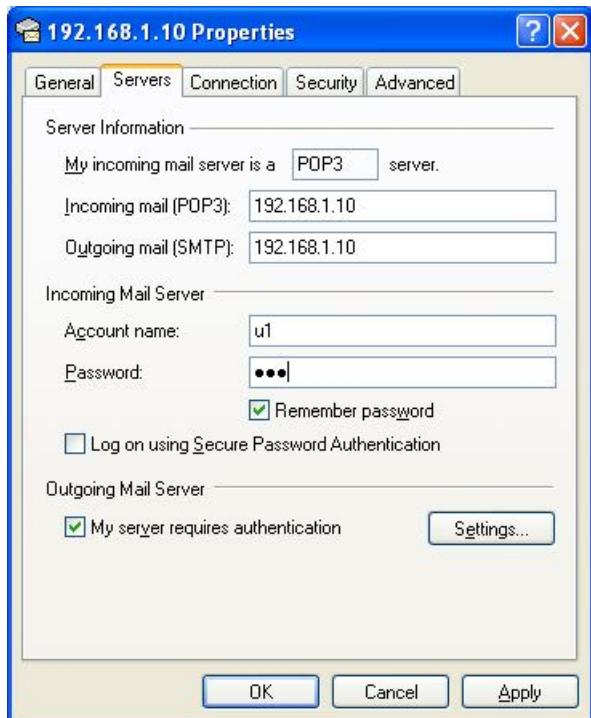
Interface	WAN
Protocol	TCP
Source	Any
Destination	Wan address
Redirect target port	pop3
Redirect target IP	10.0.0.150
Redirect target port	pop3
Description	Publish mail pop3

Firewall: NAT: Port Forward

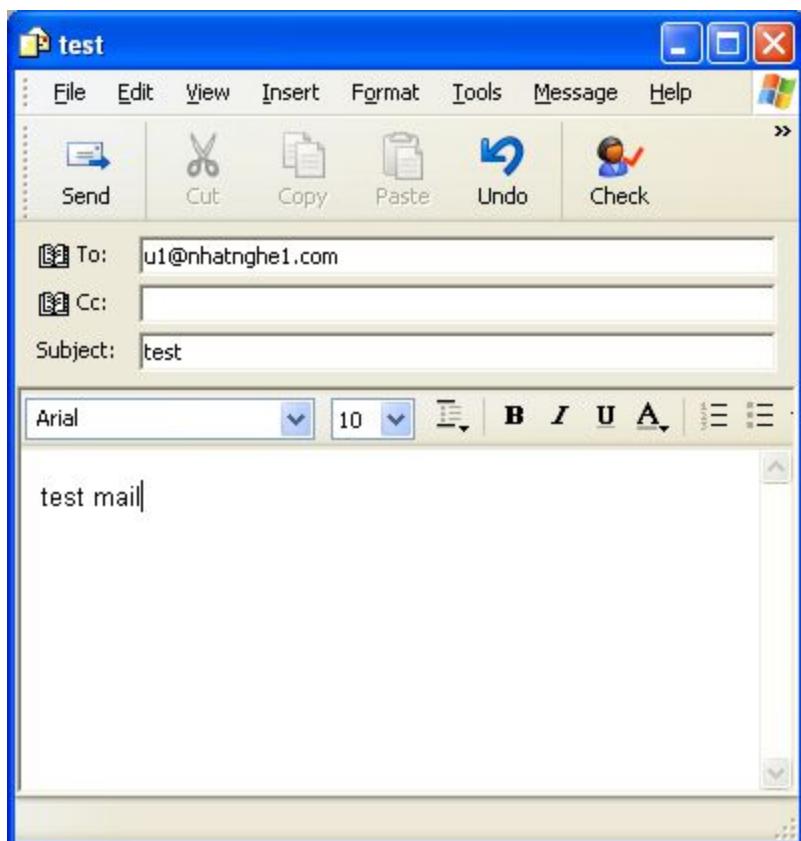
Port Forward									
1:1		Outbound		NPT					
If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	25 (SMTP)	10.0.0.150	25 (SMTP)	Publish mail smtp
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	110 (POP3)	10.0.0.150	110 (POP3)	Publish mail pop3
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.150	80 (HTTP)	Publish Web server

Nhấn Apply changes

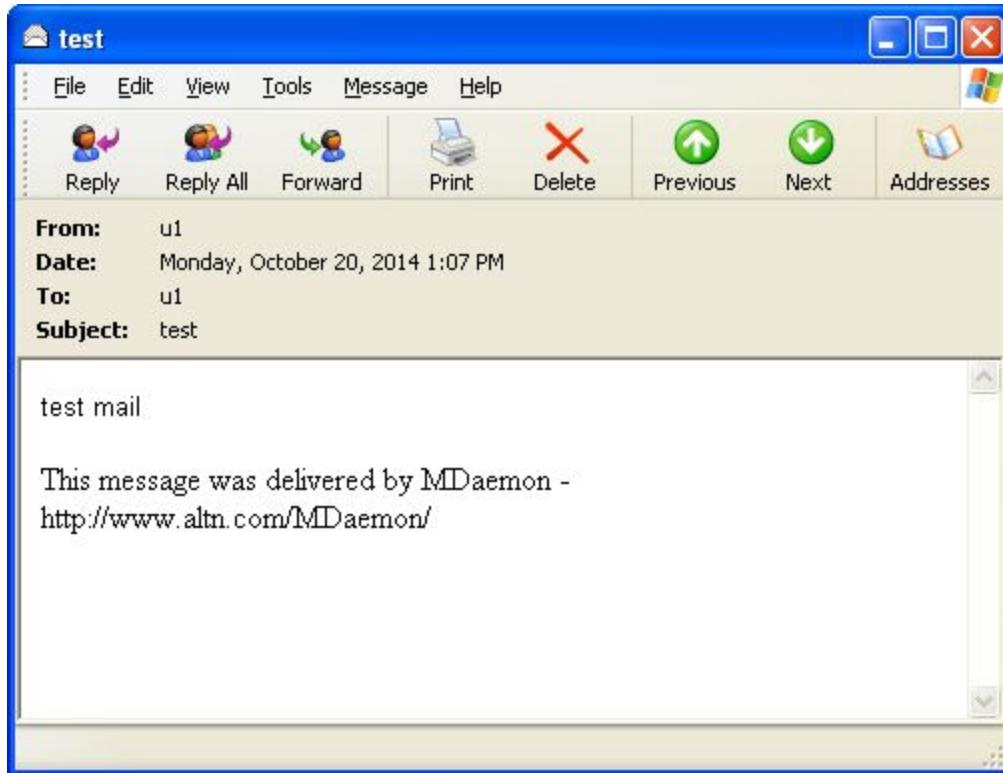
B4. Tại máy client từ bên ngoài Internet, mở Outlook Express
Cấu hình mail cho u1@nhatnghe1.com



Soạn email , nhấn send

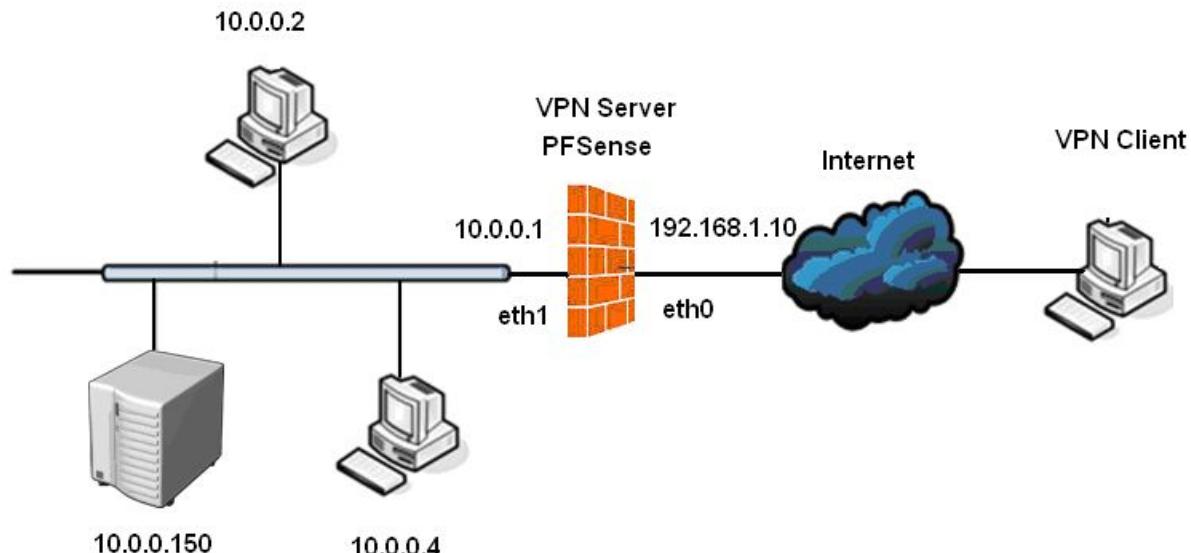


U1 nhận được mail do chính mình gửi



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*, nhấp +

System: Package Manager

Available Packages		Installed Packages	
Name	Category	Status	Description
Asterisk	Services	Beta 1.8.26.1 pkg v0.3.3 platform: 2.0	Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server.
OpenVPN Client Export Utility	Security	RELEASE 1.2.13 platform: 2.0	Allows a pre-configured OpenVPN Windows Client or Mac OSX's Viscosity configuration bundle to be exported directly from pfSense. No package info, check the forum

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

System: Certificate Authority Manager

CAs Certificates Certificate Revocation				
Name	Internal	Issuer	Certificates	Distinguished Name

Additional trusted Certificate Authorities can be added here.

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

The screenshot shows a configuration page for creating a new Certificate Authority (CA). The 'Certificates' tab is selected. The 'Descriptive name' field contains 'CA'. The 'Method' dropdown is set to 'Create an internal Certificate Authority'. Under the 'Internal Certificate Authority' section, the 'Key length' is 2048 bits, 'Digest Algorithm' is SHA256, and the 'Lifetime' is 3650 days. In the 'Distinguished name' section, the 'Country Code' is VN, 'State or Province' is hcm, 'City' is hcm, 'Organization' is nhatnghe, 'Email Address' is doquangngoc@yahoo.com, and 'Common Name' is internal-ca. A red box highlights the 'Distinguished name' group of fields.

CA đã được tạo

System: Certificate Authority Manager

CAs	Certificates	Certificate Revocation		
Name	Internal	Issuer	Certificates	Distinguished Name
CA	YES	self-signed'	0	emailAddress=doquangngoc@yahoo.com, ST=hcm, O=nhatnghe, L=hcm, CN=internal-ca, C=VN Valid From: Tue, 21 Oct 2014 09:28:01 +0700 Valid Until: Fri, 18 Oct 2024 09:28:01 +0700

B3. tạo user

System, User Manager, Users, nhập +

System: User Manager

Users	Groups	Settings	Servers
Username	Full name	Disabled	Groups
admin	System Administrator		admins

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

System: User Manager

Defined by

USER					
Disabled	<input type="checkbox"/>				
Username	<input type="text"/> vpnuser				
Password	<input type="password"/> <input type="password"/> (confirmation)				
Full name	<input type="text"/> vpnuser User's full name, for your own information only				
Expiration date	<input type="text"/> <input type="button"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following field.				
Group Memberships <table border="1"> <thead> <tr> <th>Not Member Of</th> <th>Member Of</th> </tr> </thead> <tbody> <tr> <td><input type="text"/> admins</td> <td><input type="text"/></td> </tr> </tbody> </table> <p>Hold down CTRL (pc)/COMMAND (mac) key to select multiple items</p>		Not Member Of	Member Of	<input type="text"/> admins	<input type="text"/>
Not Member Of	Member Of				
<input type="text"/> admins	<input type="text"/>				
Certificate	Descriptive name <input type="text"/> vpnuser Certificate authority CA Key length 2048 bits Lifetime <input type="text"/> 3650 days				
Authorized keys	<input type="checkbox"/> Click to paste an authorized key.				
IPsec Pre-Shared Key	<input type="text"/>				
<input type="button"/> Save					

User vpnuser đã được tạo

System: User Manager

Username	Full name	Disabled	Groups
admin	System Administrator		admins
vpnuser	vpnuser		

B4. Cấu hình openvpn

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

OpenVPN: Server

- Server**
- Client**
- Client Specific Overrides**
- Wizards** (highlighted with a red box)
- Client Export**
- Shared Key Export**

Disabled	Protocol / Port	Tunnel Network	Description

Additional OpenVPN servers can be added here.

B5. chọn kiểu chứng thực

Type of Server: chọn **Local user Access**

Nhấn Next

Select an Authentication Backend Type

Type of Server: Local User Access

NOTE: If you are unsure, leave this set to "Local User Access."

Next

B6. Chọn CA

Chọn CA, Nhấn Next

Choose a Certificate Authority (CA)

Certificate Authority: CA

Add new CA

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**

Create a New Server Certificate

Descriptive name:	<input type="text" value="vpnserver"/> A name for your reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length:	<input type="text" value="2048 bits"/> Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are slower to use.
Lifetime:	<input type="text" value="3650"/> Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code:	<input type="text" value="vn"/> Two-letter ISO country code (e.g. US, AU, CA)
State or Province:	<input type="text" value="hcm"/> Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City:	<input type="text" value="hcm"/> City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization:	<input type="text" value="nhatnghe"/> Organization name, often the Company or Group name.
E-mail:	<input type="text" value="doquangngoc@yahoo.com"/> E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)

[Create new Certificate](#)

B8. Cấu hình vpn

Chọn interface, giao thức, port cho kết nối VPN

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface:	<input type="text" value="WAN"/> The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol:	<input type="text" value="UDP"/> Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.
Local Port:	<input type="text" value="1194"/> Local port upon which OpenVPN will listen for connections. The default port is 1194. Leave this to use a different port.
Description:	<input type="text" value="vpnserver"/> A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff").

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

Cryptographic Settings

TLS Authentication:	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key:	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key:	<input type="text"/>
Paste in a shared TLS key if one has already been generated.	
DH Parameters Length:	1024 bit <input type="button" value="▼"/>
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communication with other such settings, the larger values are more secure, but may be slower in operation.	
Encryption Algorithm:	AES-128-CBC (128-bit) <input type="button" value="▼"/>
The method used to encrypt traffic between endpoints. This setting must match on the client and server, otherwise set however you like. Certain algorithms will perform better on different hardware, depending on availability of supported VPN accelerator chips.	

Cáu 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

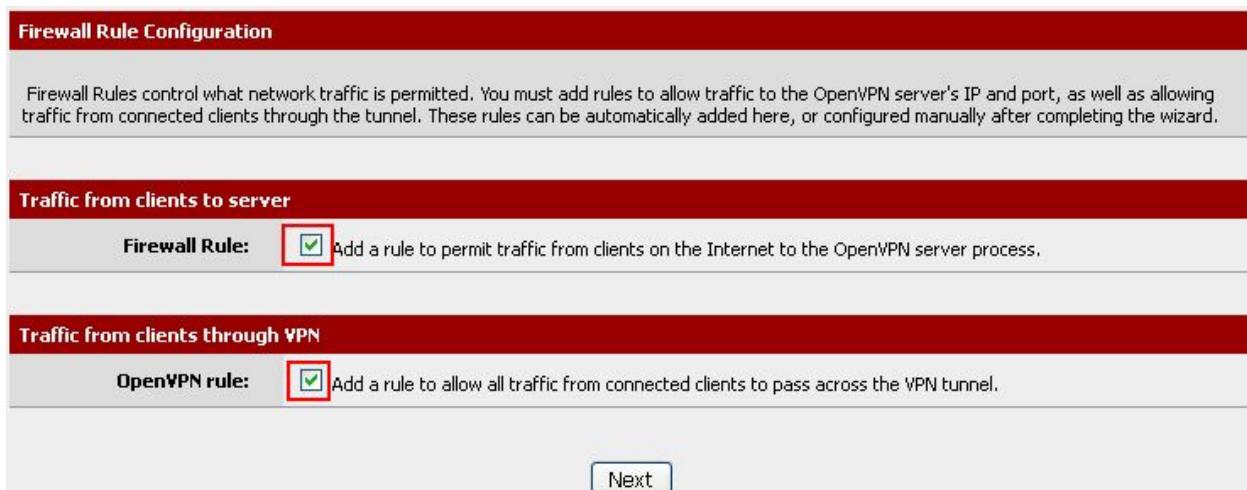
Tunnel Settings

Tunnel Network:	192.168.2.0/24	This is the virtual network used for private communications between this server and client hosts. CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface, remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway:	<input type="checkbox"/> Force all client generated traffic through the tunnel.	
Local Network:	10.0.0.0/24	This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. Leave blank if you don't want to add a route to the local network through this tunnel on the remote router. It is generally set to your LAN network.
Concurrent Connections:	50	Specify the maximum number of clients allowed to concurrently connect to this server.
Compression:	<input checked="" type="checkbox"/> Compress tunnel packets using the LZO algorithm.	

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

Firewall Rule:	Check
OpenVPN rule:	Check

Nhấn Next



B10. Nhận finish



B11. Xuất file cài đặt và cấu hình cho client

OpenVPN: Server

Server	Client	Client Specific Overrides	Wizards	Client Export	Shared Key Export
Disabled	Protocol / Port	Tunnel Network		Description	
NO	UDP / 1194	192.168.2.0/24		vpnserver	

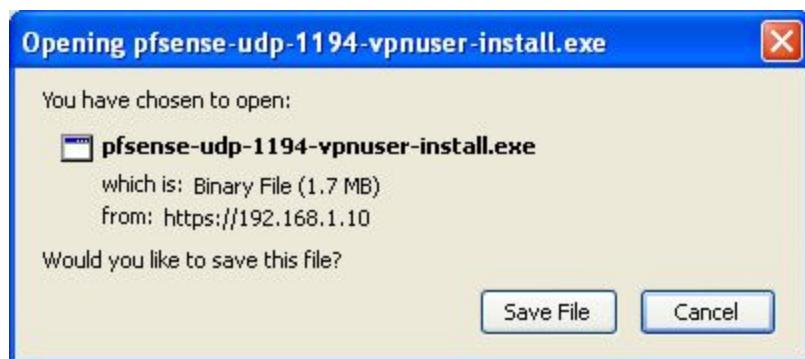
Chọn 2.3-x86

OpenVPN: Client Export Utility

The screenshot shows the 'Client Export' tab selected in the top navigation bar. A dropdown menu under 'Remote Access Server' is set to 'vpnserver UDP:1194'. Below this, a table titled 'Client Install Packages' lists a single entry for 'User: vpnuser' with 'Certificate Name: vpnuser'. To the right of the table, a list of export options is displayed:

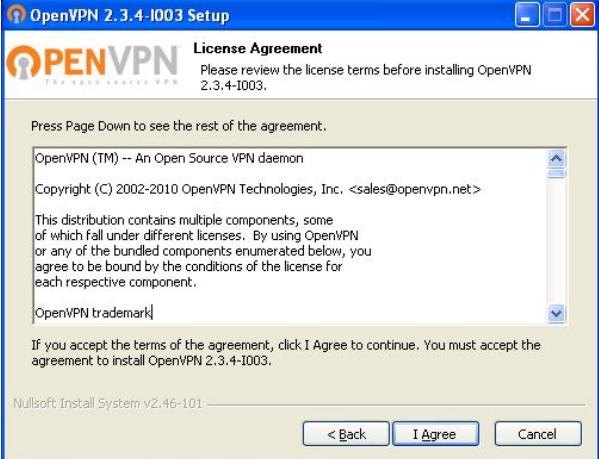
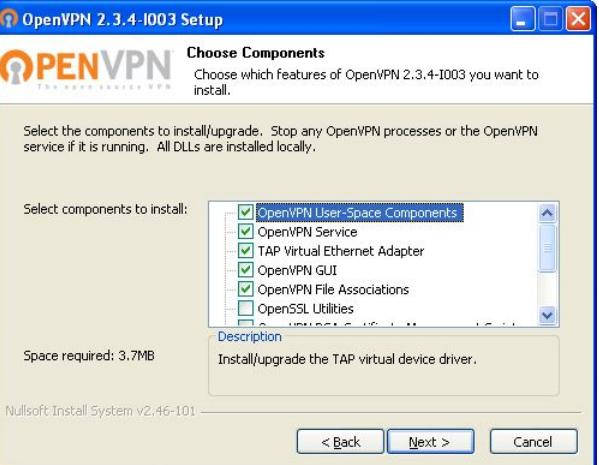
- Standard Configurations:
 - Archive Config Only
- Inline Configurations:
 - Android OpenVPN Connect (iOS/Android)
- Windows Installers:
 - 2.3-x86 (highlighted with a red box)
 - 2.3-x64
- Mac OSX: Viscosity Bundle

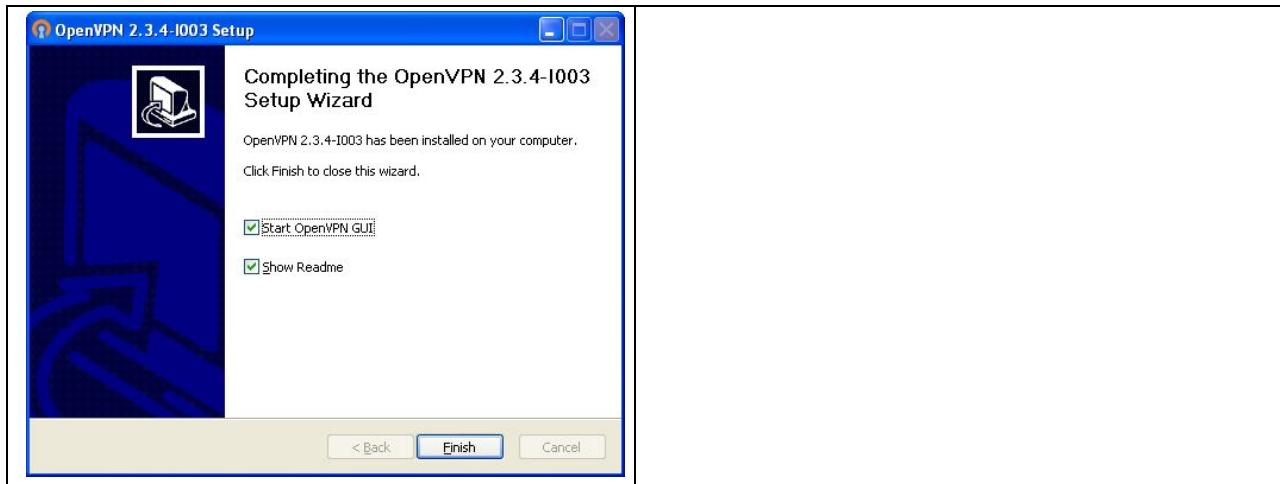
Chọn Save file



B12. Cài vpn client

<p>Thực thi file pfsense-udp-1194-vpnuser-install.exe vừa download</p> <p>The screenshot shows the 'OpenVPN Configuration Setup' window with the title 'Welcome to OpenVPN installer.' It includes a brief description of the wizard's purpose and the requirement to run on Windows XP or higher. Buttons for 'Install' and 'Cancel' are at the bottom.</p>	<p>Nhấn Next</p> <p>The screenshot shows the 'OpenVPN 2.3.4-I003 Setup' window with the title 'Welcome to the OpenVPN 2.3.4-I003 Setup Wizard'. It includes a note about the Windows version requirement and buttons for 'Next >' and 'Cancel'.</p>
--	--

<p>Chọn I Agree</p> 	<p>Nhấn Next</p> 
<p>Chọn Install</p> 	<p>Chọn continue Anyway</p> 
<p>Chọn start OpenVPN GUI Finish</p>	



B13. kết nối VPN

Mở OpenVPN GUI, connect



Kết nối thành công

```

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.1.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Local Area Connection 7:
  Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.2.6
    Subnet Mask . . . . . : 255.255.255.252
    Default Gateway . . . . . :

C:\Documents and Settings\quangngoc>ping 10.0.0.150
Pinging 10.0.0.150 with 32 bytes of data:
Reply from 10.0.0.150: bytes=32 time=1ms TTL=127
Reply from 10.0.0.150: bytes=32 time=1ms TTL=127

```

B14. Xem thông tin kết nối

Status, chọn OpenVPN

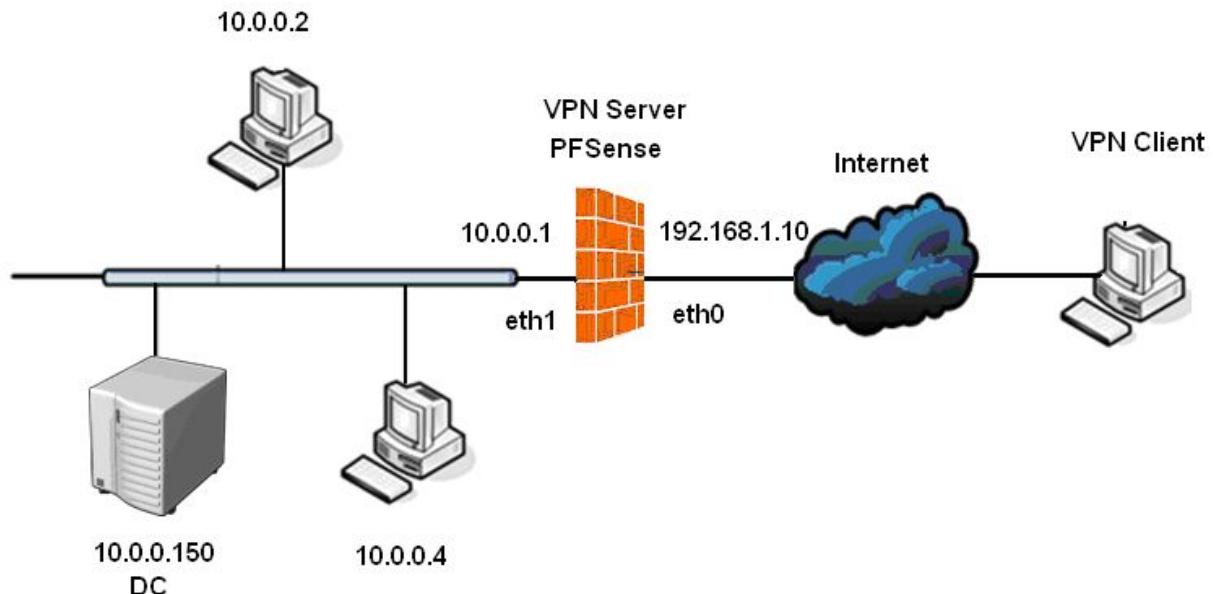
Status: OpenVPN



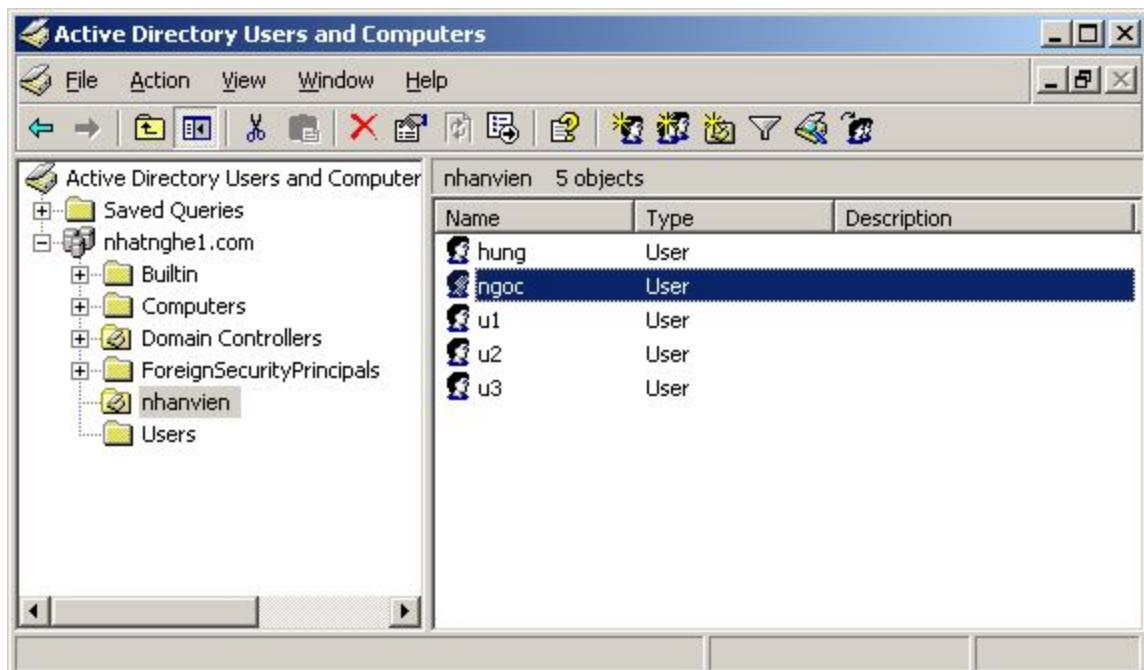
vpnserver UDP:1194 Client connections					
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
vpnuser	192.168.1.20:1946	192.168.2.6	Tue Oct 21 10:30:51 2014	9432	9318
Running					
vpnserver UDP:1194 Routing Table					
Common Name	Real Address	Target Network	Last Used		
vpnuser	192.168.1.20:1946	192.168.2.6	Tue Oct 21 10:33:05 2014		

An IP address followed by C indicates a host currently connected through the VPN.

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 +

Host	Domain	IP	Description
			May domain controller

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

Services: DNS forwarder: Edit host

Edit DNS Forwarder entry	
Host	may1 Name of the host, without domain part e.g. myhost
Domain	nhatnghe1.com Domain of the host e.g. example.com
IP address	10.0.0.150 IP address of the host e.g. 192.168.100.100 or fd00:abcd::1
Description	may domain controller You may enter a description here for your reference (not parsed).

B3. Ping kiểm tra phân giải tên

Ping may1.nhatnghe1.com

```
Enter an option: 8

[2.1.5-RELEASE][root@pfsense.nhatnghe1.com]# 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 +

System: Authentication Servers

Server Name	Type	Host Name
Local Database		pfsense

Additional authentication servers can be added here.

B5. Kết nối với máy DC

Nhập các thông tin

System: Authentication Servers

Users Groups Settings **Servers**

Descriptive name	<input type="text" value="AD"/>
Type	LDAP
LDAP Server Settings	
Hostname or IP address	<input type="text" value="may1.nhatnghe1.com"/>
NOTE: When using SSL, this hostname MUST match the Common Name (CN) of the LDAP server certificate.	
Port value	<input type="text" value="389"/>
Transport	TCP - Standard
Peer Certificate Authority	CA
This option is used if 'SSL Encrypted' option is chosen. It must match with the CA in the AD otherwise problems will arise.	
Protocol version	3
Search scope	Level: <input type="text" value="Entire Subtree"/> Base DN: <input type="text" value="dc=nhatnghe1,dc=com"/>
Authentication containers	<input type="text" value="ou=nhanvien,dc=nhatnghe1,dc=com"/> <input type="button" value="Select"/>
Containers: Note: Semi-Colon separated. This will be prepended to the search base dn above or you can enter a full dn. Example: CN=Users;DC=example Example: CN=Users,DC=example,DC=com;OU=OtherUsers,DC=example,DC=com	
Extended Query	<input type="checkbox"/> <input type="text" value="Example: CN=Groupname,OU=MyGroups,DC=example,DC=com;OU=OtherUsers,DC=example,DC=com"/>
Bind credentials	<input checked="" type="checkbox"/> Use anonymous binds to resolve distinguished names User DN: <input type="text" value="nhatnghe1\fpsense"/> Password: <input type="password" value="•••"/>
Initial Template	Microsoft AD

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

Please select which containers to Authenticate against:

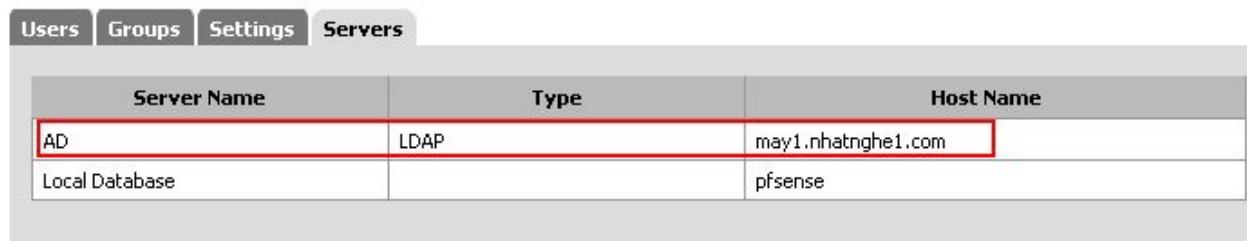
- CN=Users,DC=nhatnghe1,DC=com
- CN=Users,CN=Builtin,DC=nhatnghe1,DC=com
- OU=Domain Controllers,DC=nhatnghe1,DC=com
- OU=nhanvien,DC=nhatnghe1,DC=com

Save

Chọn **Save, Save**

B6. Pfsense đã chứng thực được user từ DC

System: Authentication Servers

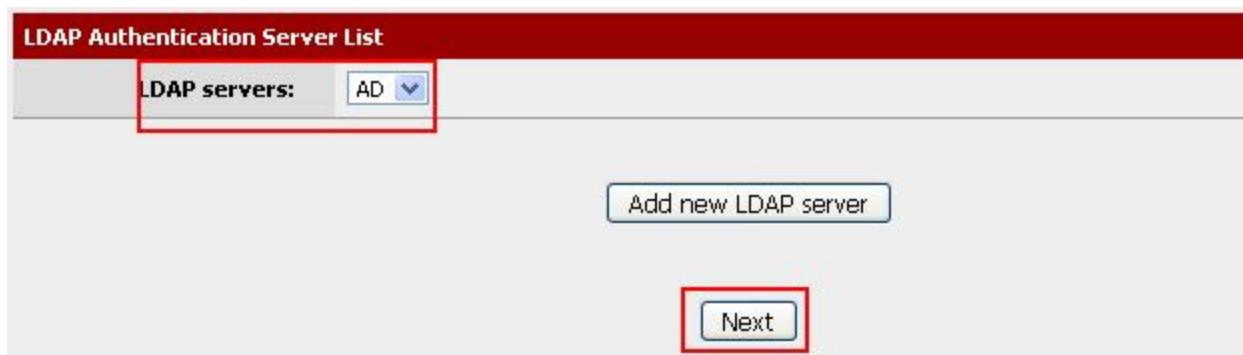


Server Name	Type	Host Name
AD	LDAP	may1.nhatnghe1.com
Local Database	Local Database	pfsense

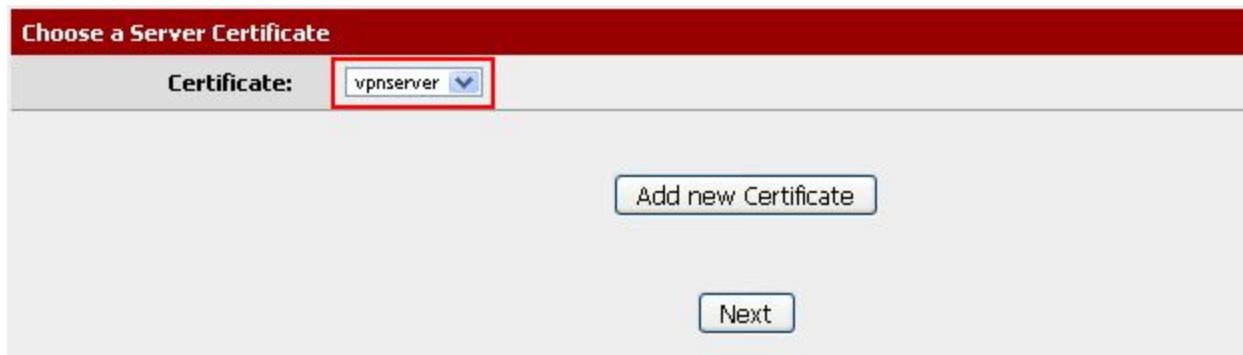
B7. Cấu hình openvpn
 VPN, Openvpn, **wizard**, chọn **Idap, next**



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)

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface:	WAN	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol:	UDP	Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.
Local Port:	1194	Local port upon which OpenVPN will listen for connections. The default port is 1194. Leave this to use a different port.
Description:	vpnserver	A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff").

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

Cryptographic Settings

TLS Authentication:	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key:	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key:	<input type="text"/>
Paste in a shared TLS key if one has already been generated.	
DH Parameters Length:	1024 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communication channel. With other such settings, the larger values are more secure, but may be slower in operation.	
Encryption Algorithm:	AES-128-CBC (128-bit)
The method used to encrypt traffic between endpoints. This setting must match on the client and server. It can be otherwise set however you like. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.	

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		

Tunnel Settings

Tunnel Network:	<input type="text" value="192.168.2.0/24"/>	This is the virtual network used for private communications between this server and client hosts. CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface, and remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway:	<input type="checkbox"/> Force all client generated traffic through the tunnel.	
Local Network:	<input type="text" value="10.0.0.0/24"/>	This is the network that will be accessible from the remote endpoint, expressed as a CIDR range or blank if you don't want to add a route to the local network through this tunnel on the remote router. It is generally set to your LAN network.
Concurrent Connections:	<input type="text" value="50"/>	Specify the maximum number of clients allowed to concurrently connect to this server.
Compression:	<input checked="" type="checkbox"/> Compress tunnel packets using the LZO algorithm.	

Chọn Save

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

Firewall Rule: Check
 OpenVPN rule: Check
 Nhấn Next

Firewall Rule Configuration

Firewall Rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule:	<input checked="" type="checkbox"/> Add a rule to permit traffic from clients on the Internet to the OpenVPN server process.
-----------------------	--

Traffic from clients through VPN

OpenVPN rule:	<input checked="" type="checkbox"/> Add a rule to allow all traffic from connected clients to pass across the VPN tunnel.
----------------------	---

Next

B12. Kết thúc

OpenVPN: Server

OpenVPN: Server					
Server	Client	Client Specific Overrides	Wizards	Client Export	Shared Key Export
Disabled	Protocol / Port	Tunnel Network			Description
NO	UDP / 1194	192.168.2.0/24			vpnserver
NO	UDP / 1195	192.168.2.0/24			vpnserver AD authentication
Additional OpenVPN servers can be added here.					

Quan sát các rule:

Firewall, chọn rule, chọn WAN

Firewall: Rules

Firewall: Rules										
Floating	WAN	LAN	OpenVPN							
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	1	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none		
<input type="checkbox"/>	2	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN vpnserver wizard
<input type="checkbox"/>	3	IPv4 UDP	*	*	WAN address	1195	*	none		OpenVPN vpnserver wizard

Firewall, chọn rule, chọn OpenVPN

Firewall: Rules

Firewall: Rules										
Floating	WAN	LAN	OpenVPN							
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	1	IPv4 *	*	*	*	*	*	none		OpenVPN vpnserver wizard
<input type="checkbox"/>	2	IPv4 *	*	*	*	*	*	none		OpenVPN vpnserver wizard

B13. Chọn client Export

Remote Access Server: Chọn **vpnserver UDP:1195**

OpenVPN: Client Export Utility

The screenshot shows the 'Client Export' tab selected in the top navigation bar. Under 'Remote Access Server', the dropdown menu is set to 'vpnserver UDP:1195'. Below it, 'Host Name Resolution' is set to 'Interface IP Address'. In the 'Verify Server CN' section, the dropdown is set to 'Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible'. A note below explains the verification process for various clients.

Chọn 2.3-x68, để download file cài đặt

Client Install Packages		
User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul style="list-style-type: none"> - Standard Configurations: Archive File Only - Inline Configurations: Android OpenVPN Connect (iOS) - Windows Installers: 2.3-x86 2.3-x64 - Mac OSX: Viscosity Bundle

B14. Cài VPN client

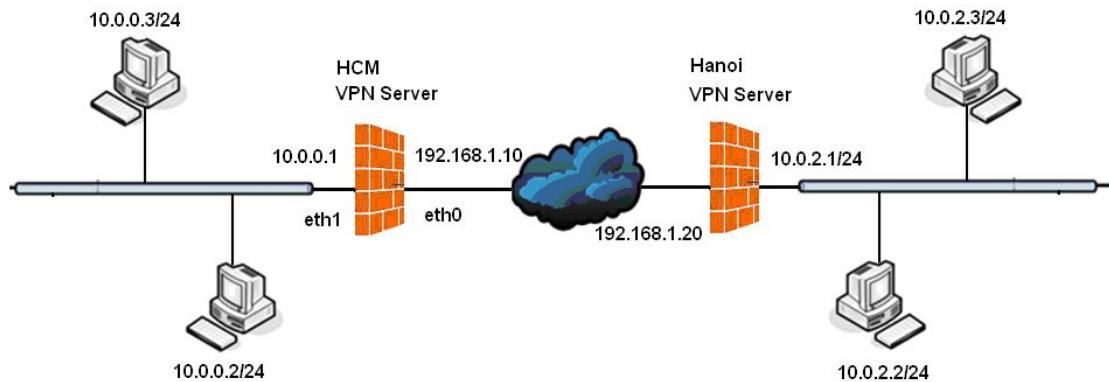
Tại máy windows, chạy file pfsense-udp-1195-install.exe
Tiến hành kết nối với user u2/123 từ AD



Kết nối thành công



3. Site to site with Shared key



B1. tại site HCM

VPN, OpenVPN, server, nhâñ +

OpenVPN: Server



Server	Client	Client Specific Overrides	Wizards	Client Export	Shared Key Export
Disabled	Protocol / Port	Tunnel Network	Description		

Additional OpenVPN servers can be added here.

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 <i>Automatically generate a shared key.</i>
IPv4 Tunnel Network	192.168.2.0/24
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	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> 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 clients. CIDR (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. Subsequent 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 as 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 VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of 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.

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

OpenVPN: Server

The screenshot shows the 'Server' tab selected in the top navigation bar. A table lists one tunnel configuration:

Disabled	Protocol / Port	Tunnel Network	Description
NO	UDP / 1194	192.168.2.0/24	vpn site to site

Below the table, a note says: "Additional OpenVPN servers can be added here." There are edit and add icons at the bottom right.

Shared Key: chọn và copy key này

The screenshot shows the 'Cryptographic Settings' interface. In the 'Shared Key' section, a 2048-bit OpenVPN static key is pasted into the text area. The key starts with "# 2048 bit OpenVPN static key" and includes a long string of hex digits. Below the text area is a note: "Paste your shared key here." At the bottom, the 'Encryption algorithm' is set to "AES-128-CBC (128-bit)".

B3. Site Hanoi tạo kết nối VPN đến site HCM

Chọn thẻ Client, nhấn +

OpenVPN: Client

The screenshot shows the 'Client' tab selected in the top navigation bar. A table lists clients, currently empty:

Disabled	Protocol	Server	Description
----------	----------	--------	-------------

Below the table, a note says: "Additional OpenVPN clients can be added here." There is an add icon at the bottom right.

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	Kết nối đến site HHCM
Shared Key	<input checked="" type="checkbox"/> <i>Automatically generate a shared key.</i> Dán nội dung key tạo ở site HCM

Server Client Client Specific Overrides Wizards

General information

Disabled **Disable this client**
Set this option to disable this client without removing it from the list.

Server Mode	Peer to Peer (Shared Key)
Protocol	UDP
Device mode	tun
Interface	WAN
Local port	<input type="text"/>
Server host or address	192.168.1.10
Server port	1194
Description	Kết nối đến site HHCM

You may enter a description here for your reference (not parsed).

Cryptographic Settings

Shared Key *Automatically generate a shared key.*

```
44d580b71047da38819ccaf45bd6112f
ee98fce924ccbfbcd3747a71e760c843
cd7e9bbb62bc87e7b2549cbdac85deaf
42f30128e2210859bc3c7e7c6235b886
1ae9775fafcz4d2d5abb24ef35c174b4
dd2056a445970f62adfa613378d4e113
-----END OpenVPN Static key V1-----
```

Paste your shared key here.

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		

Tunnel Settings

IPv4 Tunnel Network	<input type="text" value="192.168.2.0/24"/>	This is the virtual network used for private communications between this client and the server (eg. 10.0.8.0/24). The first network address is assumed to be the server address and the second will be assigned to the client virtual interface.
IPv4 Remote Network/s	<input type="text" value="10.0.0.0/24"/>	These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP networks. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with the server.
Compression	<input checked="" type="checkbox"/> Compress tunnel packets using the LZO algorithm.	
Save		

Kết nối VPN được tạo

OpenVPN: Client

Server	Client	Client Specific Overrides	Wizards
Disabled	Protocol	Server	Description
NO	UDP	<input type="text" value="192.168.1.10:1194"/>	ket noi den site HCM

B4. Site HCM - Tạo rule

Firewall, Rules, chọn WAN, nhấn +

Firewall: Rules

Floating	WAN	LAN	OpenVPN									
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description			
<input type="checkbox"/>	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none					

Khai báo các tham số:

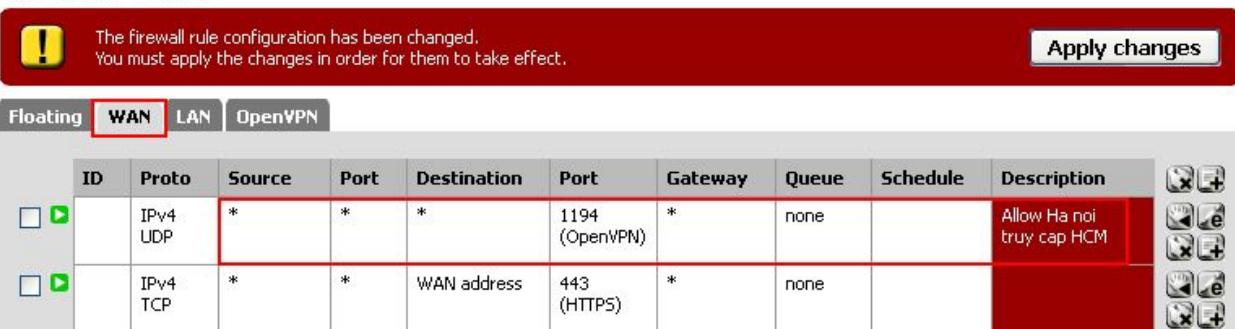
Action	Pass
Interface	WAN
Protocol	UDP
Source	any
Destination	any
Destination port range	OpenVPN
Description	Allow Ha noi truy cap HCM

Chọn Save

Firewall: Rules: Edit

Edit Firewall rule	
Action	<input type="button" value="Pass"/> <input type="button" value="Block"/> <input type="button" value="Reject"/>
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the packet is not delivered to the application.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="WAN"/> <input type="button" value="LAN"/> <input type="button" value="Mobile"/>
	Choose on which interface packets must come in to match this rule.
TCP/IP Version	<input type="button" value="IPv4"/> <input type="button" value="IPv6"/> Select the Internet Protocol version this rule applies to
Protocol	<input type="button" value="TCP"/> <input type="button" value="UDP"/> <input type="button" value="ICMP"/>
	Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match.
	Type: <input type="button" value="any"/> <input type="button" value="IP address"/> <input type="button" value="Range"/> <input type="button" value="Custom"/> Address: <input type="text" value=""/> / <input type="button" value="127"/> <input type="button" value="255"/>
	<input type="button" value="Advanced"/> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match.
	Type: <input type="button" value="any"/> <input type="button" value="IP address"/> <input type="button" value="Range"/> <input type="button" value="Custom"/> Address: <input type="text" value=""/> / <input type="button" value="127"/> <input type="button" value="255"/>
Destination port range	from: <input type="button" value="OpenVPN"/> <input type="button" value="Range"/> <input type="button" value="Custom"/> to: <input type="button" value="OpenVPN"/> <input type="button" value="Range"/> <input type="button" value="Custom"/>
	Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	<input type="text" value="Allow Ha noi truy cap HCM"/>
	You may enter a description here for your reference.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Nhấn **Apply changes**

Firewall: Rules


The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

Floating	WAN	LAN	OpenVPN								
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	1	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		Allow Hanoi access HCM	
<input type="checkbox"/>	2	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none			

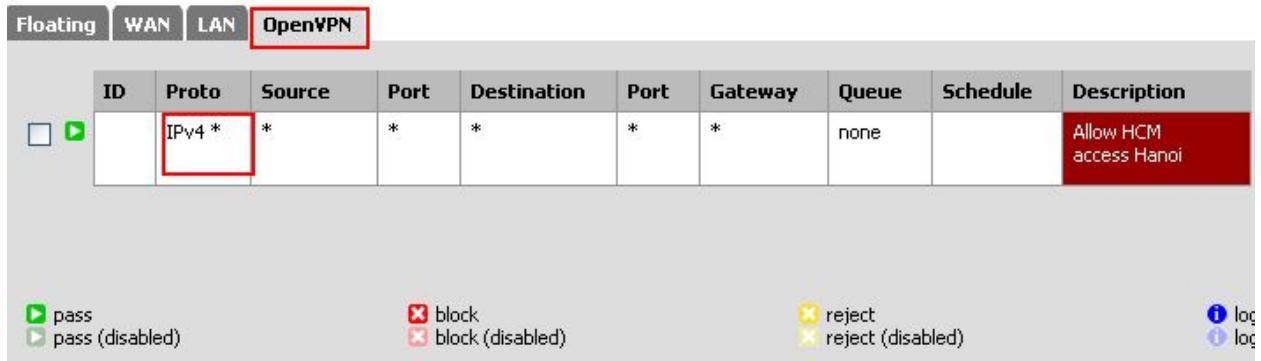
B5. Tương tự tạo rule trên tab OpenVPN:

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

Firewall: Rules: Edit

Edit Firewall rule

Interface	OpenVPN	Choose on which interface packets must come in to match this rule.
TCP/IP Version	IPv4	Select the Internet Protocol version this rule applies to
Protocol	any	Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<input checked="" type="checkbox"/> not	Use this option to invert the sense of the match. Type: any / 127
Destination	<input checked="" type="checkbox"/> not	Use this option to invert the sense of the match. Type: any / 127
Description	Allow HCM access Hanoi	
	Save	Cancel



The screenshot shows a table with columns: ID, Proto, Source, Port, Destination, Port, Gateway, Queue, Schedule, and Description. A single row is present, with the 'Proto' column value 'IPv4 *' highlighted by a red box. The 'Description' column contains the text 'Allow HCM access Hanoi'. Below the table, there are several status indicators: 'pass' (green), 'pass (disabled)' (grey), 'block' (red), 'block (disabled)' (grey), 'reject' (yellow), 'reject (disabled)' (grey), and two log icons.

Floating	WAN	LAN	OpenVPN						
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	none		Allow HCM access Hanoi

pass pass (disabled) block block (disabled) reject reject (disabled)

log log

B7. Site Hanoi tạo rule trên tab OpenVPN:

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

Firewall: Rules: Edit

Edit Firewall rule

Action	Pass <input type="button" value="▼"/>	Choose what to do with packets that match the criteria specified below.
Interface	OpenVPN <input type="button" value="▼"/>	Choose on which interface packets must come in to match this rule.
TCP/IP Version	IPv4 <input type="button" value="▼"/> Select the Internet Protocol version this rule applies to	
Protocol	any <input type="button" value="▼"/>	Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any <input type="button" value="▼"/> Address: / 127 <input type="button" value="▼"/>	
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any <input type="button" value="▼"/> Address: / 127 <input type="button" value="▼"/>	
Description	Allow access Hanoi to HCM You may enter a description here for your reference.	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Rule đã được tạo

Floating WAN LAN OpenVPN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>		IPv4 *	*	*	*	*	*	none		Allow access Hanoi to HCM

pass pass (disabled)
 block block (disabled)
 reject reject (disabled)

log log

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
Kết nối đến 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

```
C:\WINDOWS\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

  Connection-specific DNS Suffix . : 
  IP Address . . . . . : 10.0.2.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.2.1

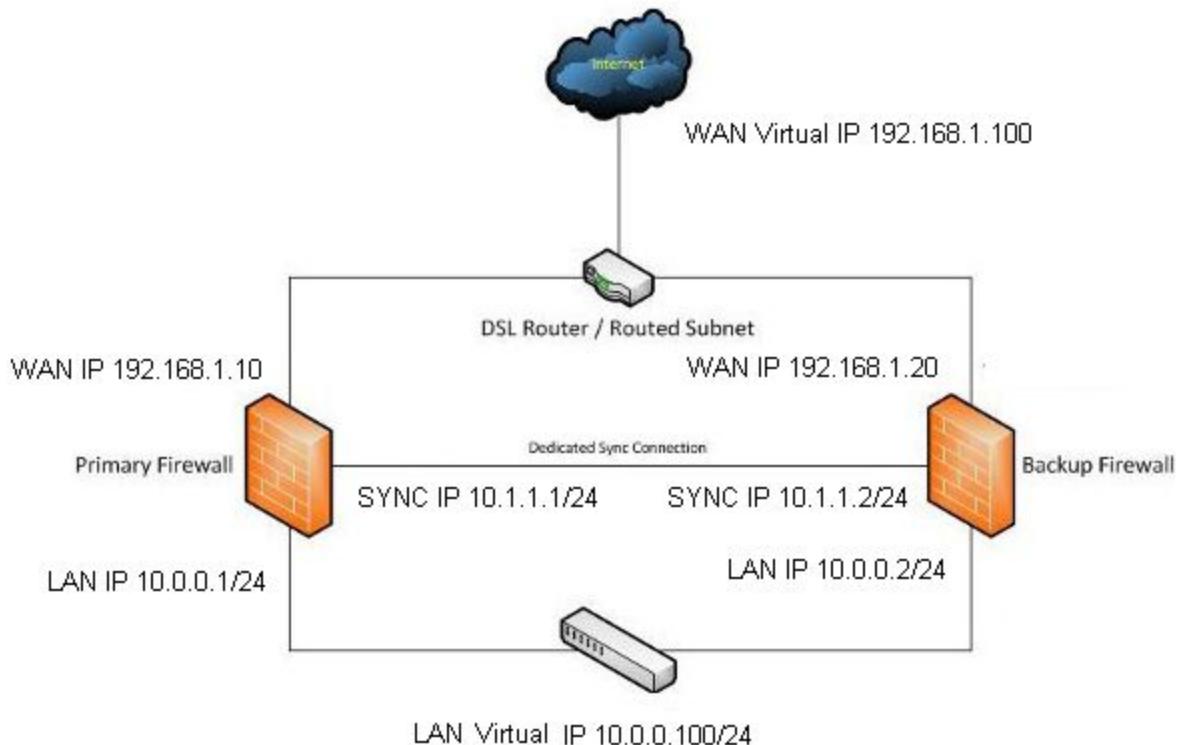
C:\Documents and Settings\Administrator>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=2ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1ms TTL=63

Ping statistics for 10.0.0.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

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

Interface assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GRE	GIF	Bridges	LAGG
Interface									
<u>WAN</u>					le0 (00:0c:29:45:db:bb)				
<u>LAN</u>					le1 (00:0c:29:45:db:c5)				
<u>syn</u>					le2 (00:0c:29:45:db:c6)				

B2. Tạo rule trên 2 firewall

Firewall, Rules, nhấn +

Firewall: Rules



Floating WAN LAN **SYNC** OpenVPN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
No rules are currently defined for this interface All incoming connections on this interface will be blocked until you add pass rules.									
Click the button to add a new rule.									
<input checked="" type="checkbox"/> pass <input type="checkbox"/> pass (disabled)		<input checked="" type="checkbox"/> block <input type="checkbox"/> block (disabled)		<input checked="" type="checkbox"/> reject <input type="checkbox"/> reject (disabled)		<input type="checkbox"/> log <input type="checkbox"/> log (disabled)			

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

Edit Firewall rule

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP
Interface	SYNC	Choose on which interface packets must come in to match this rule.
TCP/IP Version	IPv4	Select the Internet Protocol version this rule applies to
Protocol	any	Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<input type="checkbox"/> not	Use this option to invert the sense of the match. Type: any
Destination	<input type="checkbox"/> not	Use this option to invert the sense of the match. Type: any
Description	sync fw1 - fw2	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Nhấn **Apply changes**

Firewall: Rules

Floating	WAN	LAN	SYNC	OpenVPN							
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*	*	*	*	*	none		sync fw1 - fw2	

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

System: High Availability Sync

State Synchronization Settings (pfsync)

Synchronize States pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization Set below)

Synchronize Interface If Synchronize States is enabled, it will utilize this interface for communication.
NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best.
NOTE: You must define a IP on each machine participating in this failover group.
NOTE: You must have an IP assigned to the interface on any participating sync nodes.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
NOTE: XMLRPC sync is currently only supported over connections using the same protocol and port as the current connection - make sure the remote system's port and protocol are set accordingly!
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username Enter the webConfigurator username of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password Enter the webConfigurator password of the system entered above for synchronizing your configuration.

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

System: High Availability Sync

State Synchronization Settings (pfsync)

Synchronize States pfSync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 2) on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group.

NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization below)

Synchronize Interface **SYN** If Synchronize States is enabled, it will utilize this interface for communication.

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 +

Firewall: Virtual IP Addresses

Virtual IP address	Interface	Type	Description

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Firewall: Virtual IP Address: Edit

Edit Virtual IP

Type	<input type="radio"/> IP Alias <input checked="" type="radio"/> CARP <input type="radio"/> Proxy ARP <input type="radio"/> Other
Interface	WAN
IP Address(es)	Type: Single address Address: 192.168.1.100 / 24 <small>This must be the network's: specify a CIDR range.</small>
Virtual IP Password	***** Enter the VHID group password.
VHID Group	1 Enter the VHID group that the machines will share
Advertising Frequency	Base: 1 Skew: 0 The frequency that this machine will advertise. 0 means usually master. Otherwise of both values in the cluster determines the master.
Description	WAn Virtual IP You may enter a description here for your reference (not parsed).
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Thiết đặt 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 đặt 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

Firewall: Virtual IP Addresses

Virtual IPs			
Virtual IP address	Interface	Type	Description
192.168.1.100/24 (vhid 1)	WAN	CARP	WAn Virtual IP
10.0.0.100/24 (vhid 3)	LAN	CARP	LAN Virtual IP

Nhập Apply changes

B7. Enable CARP

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

Status: CARP



CARP Interface	Virtual IP	Status
wan_vip1	192.168.1.100	<input checked="" type="checkbox"/> DISABLED
lan_vip3	10.0.0.100	<input checked="" type="checkbox"/> DISABLED

2 virtual IP chuyển sang chế độ Master

Status: CARP



CARP Interface	Virtual IP	Status
wan_vip1	192.168.1.100	<input checked="" type="checkbox"/> MASTER
lan_vip3	10.0.0.100	<input checked="" type="checkbox"/> MASTER

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

Firewall, Virtual Ips, chọn Virtual Ips

Firewall: Virtual IP Addresses

Virtual IPs			
Virtual IP address	Interface	Type	Description
192.168.1.201/24 (vhid 1)	WAN	CARP	WAn Virtual IP
10.0.0.100/24 (vhid 3)	LAN	CARP	LAN Virtual IP

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

Status: CARP

CARP Interface		Virtual IP		Status	
wan_vip1		192.168.1.201		<input checked="" type="checkbox"/> BACKUP	
lan_vip3		10.0.0.100		<input checked="" type="checkbox"/> 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.

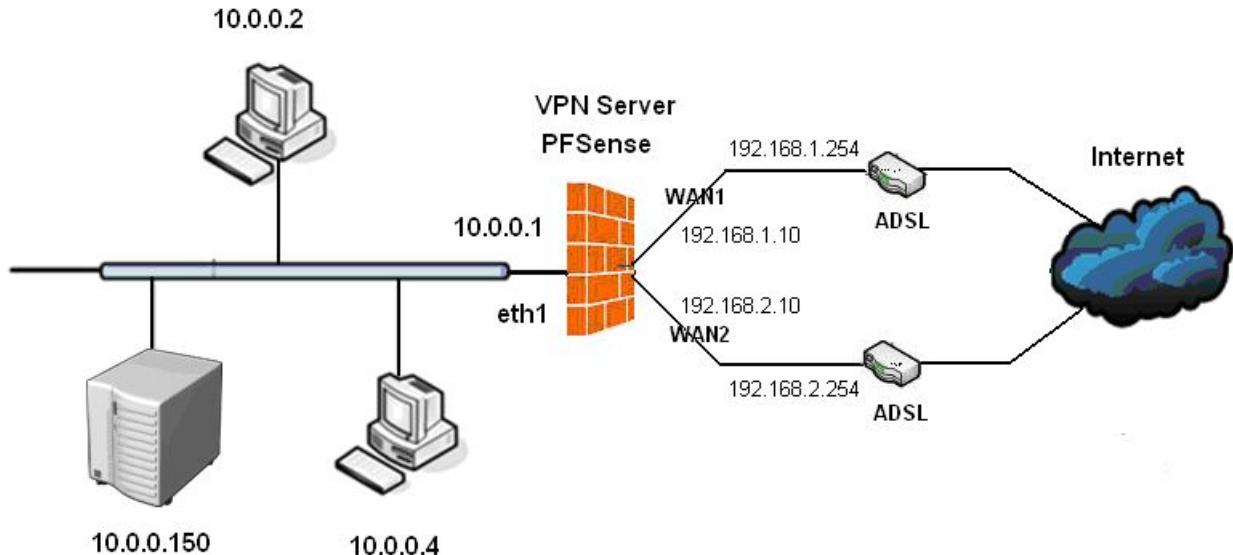
Tại FW2 quan sát thấy rule đã được đồng bộ

The screenshot shows a web-based firewall configuration interface for a device at 10.0.0.2. The main title is "Firewall: Rules". Below it, there are tabs for "Floating", "WAN", "LAN" (which is selected), and "SYN". A table lists a single rule:

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>		IPv4 TCP	*	*	*	22 (SSH)	*	none		

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

Interfaces: Assign network ports

Interface assignments		Interface Groups	Wireless	VLANs	QinQs	PPPs	GRE	GIF	Bridges	LAGG
Interface	Network port									
WAN	le0 (00:0c:29:1e:6d:31)									
LAN	le1 (00:0c:29:1e:6d:3b)									

Chọn Wan

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

Chọn Save

General configuration

Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text"/> WAN1 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4 <input type="button"/>

Static IPv4 configuration

IPv4 address	<input type="text"/> 192.168.1.10 <input type="button"/> 24 <input type="button"/>
IPv4 Upstream Gateway	<input type="text"/> GW_WAN - 192.168.1.254 <input type="button"/> - or add a new one. If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the On local LANs the upstream gateway should be "none".

B2. Cấu hình WAN2 interface

Chọn +

Interfaces: Assign network ports

Interface assignments		Interface Groups	Wireless	VLANs	QinQs	PPPs	GRE	GIF	Bridges	LAGG
Interface	Network port									
WAN1	<input type="text"/> le0 (00:0c:29:1e:6d:31) <input type="button"/>									
LAN	<input type="text"/> le1 (00:0c:29:1e:6d:3b) <input type="button"/>	<input type="button"/>	<input type="button"/>							

Lan card thứ 3 được thêm vào, chọn OPT1

Interface assignments		Interface Groups	Wireless	VLANs	QinQs	PPPs	GRE	GIF	Bridges	LAGG
Interface	Network port									
WAN1	<input type="text"/> le0 (00:0c:29:1e:6d:31) <input type="button"/>									
LAN	<input type="text"/> le1 (00:0c:29:1e:6d:3b) <input type="button"/>									
OPT1	<input type="text"/> le2 (00:0c:29:1e:6d:45) <input type="button"/>									

Nhập thông tin cho WAN2

Description	WAN2
Enable	Check
IPv4 Configuration Type	Static

Interfaces: WAN2

General configuration

Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text"/> WAN2
IPv4 Configuration Type	<input type="text"/> Static IPv4

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

Chọn Save

IPv4 Upstream Gateway - or **add a new one.**

Add new gateway:

Default gateway:	<input type="checkbox"/>
Gateway Name:	WAN2GW
Gateway IPv4:	192.168.2.254
Description:	
<input type="button" value="Save Gateway"/> <input type="button" value="Cancel"/>	

Chọn Save

B3. Quan sát các GW đã tạo
 System, routing

System: Gateways

Gateways	Routes	Groups		
Name	Interface	Gateway	Monitor IP	Description
WAN1GW (default)	WAN1	192.168.1.254	192.168.1.254	
WAN2GW	WAN2	192.168.2.254	192.168.2.254	

B4. Tạo Group

System, routing, chọn +

System: Gateway Groups

Gateways	Routes	Groups		
Group Name	Gateways	Priority	Description	
				 

Group Name

Loadbalancing

Gateway Priority

chọn Tier 1 cho 2 cổng WAN

Trigger Level

Chọn Packet Loss or High Latency

Chọn

Save

Edit gateway group entry

Group Name	Loadbalancing			
Group Name				
Gateway Priority	Gateway	Tier	Virtual IP	Description
	WAN1GW	Tier 1	Interface Address	
	WAN2GW	Tier 1	Interface Address	
Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple priority will balance connections until all links in the priority will be exhausted. If all links in a priority will use the next available link(s) in the next priority level.				
Virtual IP The virtual IP field selects what (virtual) IP should be used when this group applies to a local or OpenVPN endpoint				
Trigger Level	High Latency When to trigger exclusion of a member			
Description	Wan load balancing You may enter a description here for your reference (not parsed).			
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				

Tạo tiếp group Failover1

Edit gateway group entry

Group Name	Failover1			
Group Name				
Gateway Priority	Gateway	Tier	Virtual IP	Description
	WAN1GW	Tier 1	Interface Address	
	WAN2GW	Tier 2	Interface Address	
Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple priority will balance connections until all links in the priority will be exhausted. If all links in a priority will use the next available link(s) in the next priority level.				
Virtual IP The virtual IP field selects what (virtual) IP should be used when this group applies to a local or OpenVPN endpoint				
Trigger Level	Packet Loss When to trigger exclusion of a member			
Description	If WAN1 failed then go to WAN2 You may enter a description here for your reference (not parsed).			
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				

Tạo tiếp group Failover1

Edit gateway group entry

Group Name	<input type="text" value="Failover1"/> Group Name		
Gateway Priority	Gateway	Tier	Virtual IP
	WAN1GW	Tier 1	Interface Address
	WAN2GW	Tier 2	Interface Address
Link Priority The priority selected here defines in what order failover and balancing of links will be done. M priority will balance connections until all links in the priority will be exhausted. If all links in a pr will use the next available link(s) in the next priority level.			
Virtual IP The virtual IP field selects what (virtual) IP should be used when this group applies to a local I OpenVPN endpoint			
Trigger Level	Packet Loss		
When to trigger exclusion of a member			
Description	<input type="text" value="If WAN1 failed then go to WAN2"/> You may enter a description here for your reference (not parsed).		
Save Cancel			

Kết quả 3 group được tạo ra

Gateways Routes Groups			
Group Name	Gateways	Priority	Description
Loadbalancing	WAN1GW WAN2GW	Tier 1 Tier 1	Wan load balancing
Failover1	WAN1GW WAN2GW	Tier 1 Tier 2	If WAN1 Failed then go to WAN2
Failover2	WAN1GW WAN2GW	Tier 2 Tier 1	If WAN2 Failed then go to WAN1

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

Firewall: Rules

Floating	WAN1	LAN	WAN2							
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Protocol any
 Gateway chọn Loadbalancing
 Chọn Save

Advanced features

Gateway	<input type="button" value="default"/> <input type="button" value="default"/> <input type="button" value="GW_WAN - 192.168.1.254"/> <input type="button" value="GW_WAN2 - 192.168.2.254"/> <input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px; margin-left: 10px;" type="button" value="Loadbalancing"/>	System routing table. Or choose
In/Out	<input type="button" value="Advanced"/>	- show advanced option

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

Kết quả 3 rule được tạo:

Floating	WAN1	LAN	WAN2							
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	IPv4 *	LAN net	*	*	*	Loadbalancing	none		WAN load balancing	
<input checked="" type="checkbox"/>	IPv4 *	LAN net	*	*	*	Failover1	none		WAN Failover 1	
<input checked="" type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	*		WAN Failover 2	

B7. Gán DNS cho mỗi Gateway
 System, General Setup

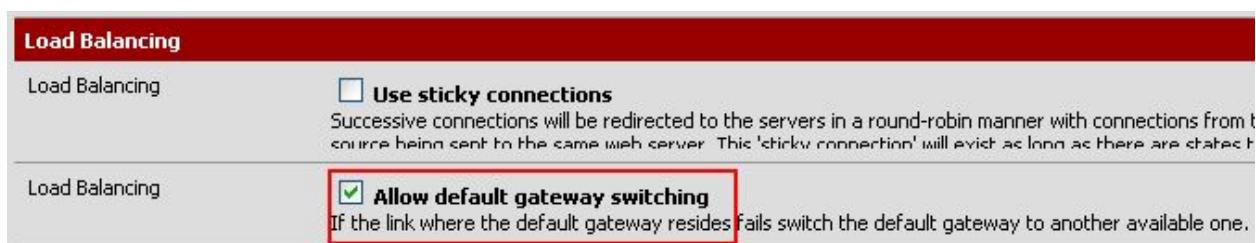


Chọn Save

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

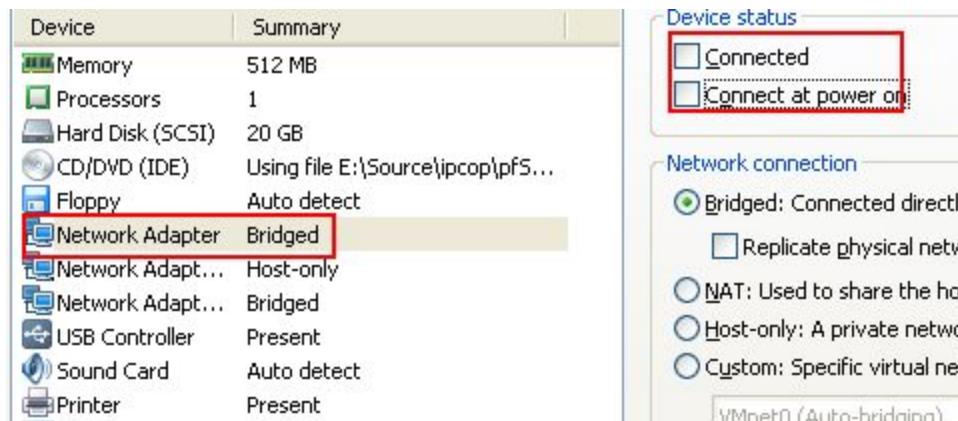
Status: Gateways

Gateways					
Name	Gateway	Monitor	RTT	Loss	Status
WAN1GW	192.168.1.254	192.168.1.254	1.1ms	0%	Online Last check: Wed, 29 Oct 2014 10:19:13 +0700
WAN2GW	192.168.2.254	192.168.2.254	4.2ms	0%	Online Last check: Wed, 29 Oct 2014 10:19:13 +0700

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**

Status: Gateways

Gateways						
Name	Gateway	Monitor	RTT	Loss	Status	
WAN1GW	192.168.1.254	192.168.1.254	0.9ms	86%	Offline	Last check: Wed, 29 Oct 2014 10:24:00 +0700
WAN2GW	192.168.2.254	192.168.2.254	0.5ms	0%	Online	Last check: Wed, 29 Oct 2014 10:25:04 +0700

Chọn Gateway Groups

Gateway Groups						
Group Name	Gateways			Description		
Loadbalancing	Tier 1 WAN1GW, Offline WAN2GW, Online			Wan load balancing		
Failover1	Tier 1 WAN1GW, Offline Tier 2 WAN2GW, Online			If WAN1 Failed then go to WAN2		
Failover2	Tier 1 WAN2GW, Online Tier 2 WAN1GW, Offline			If WAN2 Failed then go to WAN1		

IDS – IPS

Xây dựng hệ thống phát hiện và ngăn chặn xâm nhập mạng

B1. Cài gói Snort

System, Package Manager

Available Packages			
Name	Category	Version	Description
AutoConfigBackup	Services	1.27	Automatically backs up your pfSense configuration. All contents are encrypted before being sent to the server. Requires Gold Subscription from https://portal.pfsense.org Package info
snort	Security	Available: 2.9.6.2 pkg v3.1.3 Installed: 2.9.6.2 pkg v3.1.2	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package info

B2. Lấy mã Oinkcode từ trang snort.org

Truy cập trang snort.org

Click địa chỉ email, chọn Oinkcode, copy đoạn mã : 7c4175eb1383e7e7e133253bf5f20bcb251e5527

doquangngoc@yahoo.com

doquangngoc@yahoo.com

1

2

3

Oinkcode

7c4175eb1383e7e7e133253bf5f20bcb251e5527

B3. Kết nối đến Snort

Service, Snort, chọn thẻ **Global Settings**

Install **Snort VRT** rules Check

Code: Dán đoạn 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 để 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 thông kê bandwidth

Chọn **Access bandwidthD**

Nhấp chọn **Daily**, xem thông kê theo ngày

Nhấp chọn **Weekly**, xem thông kê 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 Client 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

Chọn ALL

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

