

# TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM

## BÁO CÁO HỆ ĐIỀU HÀNH LINUX

### ĐỀ TÀI: OPENVPN TRÊN LINUX

GIẢNG VIÊN HƯỚNG DẪN: HỒ HỮU TRUNG

SINH VIÊN THỰC HIỆN: BÙI ĐỨC VŨ

NGUYỄN VĂN MINH

LỚP: 11DTHM

#### I. OPENVPN LÀ GÌ ?

- OpenVPN là một phần mềm mạng riêng ảo mã nguồn mở dành cho việc tạo các đường ống (tunnel) điểm tới điểm được mã hóa giữa các máy chủ.
- OpenVPN cho phép các máy đồng đẳng xác thực lẫn nhau bằng một khóa bí mật được chia sẻ từ trước, chứng chỉ mã công khai (public key certificate), hoặc tên người dùng/mật khẩu. Phần mềm này được cung cấp kèm theo các hệ điều hành Solaris, Linux, OpenBSD, Windows,... Nó có nhiều tính năng bảo mật và kiểm soát. Nó không phải là một mạng riêng ảo web, không tương thích với IPSec hay các gói VPN khác. Toàn bộ phần mềm gồm có một file nhị phân cho cả các kết nối client và server, một file cấu hình, và một hoặc nhiều file khóa tùy theo phương thức xác thực.

#### II. ƯU ĐIỂM CỦA OPENVPN

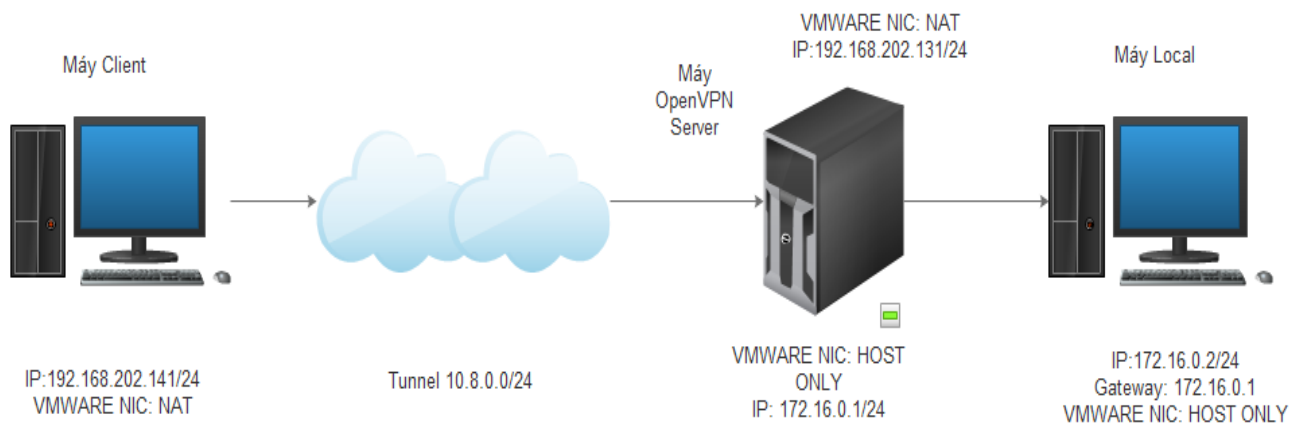
- Bảo vệ người làm việc bên ngoài bằng tường lửa nội bộ.
- Các kết nối OpenVPN có thể đi qua được hầu hết mọi tường lửa và proxy. OpenVPN có hỗ trợ ủy quyền đầy đủ bao gồm xác thực.
- Hỗ trợ UDP và TCP: OpenVPN có thể được cấu hình để chạy dịch vụ TCP hoặc UDP trên máy chủ hoặc client. Là một máy chủ, OpenVPN chỉ đơn giản là chờ đợi cho đến khi một user yêu cầu kết nối, kết nối này được thiết lập theo cấu hình của khách hàng.
- Chỉ cần một cổng tường lửa được mở là cho phép nhiều kết nối vào: Kể từ phần mềm OpenVPN 2.0, máy chủ đặc biệt này cho phép nhiều kết nối vào trên cùng một cổng TCP hoặc UDP, đồng thời vẫn sử dụng các cấu hình khác nhau cho mỗi một kết nối.

- Không có vấn đề gì với NAT: Cả máy chủ và máy khác OpenVPN có thể nằm trong cùng một mạng và sử dụng các địa chỉ IP riêng. Mỗi tường lửa có thể được dung để gửi lưu lượng tới điểm cuối đường hầm.
- Giao diện ảo chấp nhận các quy tắc về tường lửa: Tất cả các quy tắc, các cơ chế chuyển tiếp, và NAT có thể dung chung đường hầm OpenVPN
- Độ linh hoạt cao: OpenVPN cung cấp nhiều điểm trong quá trình thiết lập kết nối để bắt đầu các kịch bản riêng. Những kịch bản có thể được sử dụng cho một loạt các mục đích từ xác thực, chuyển đổi dự phòng và nhiều hơn nữa.
- Hỗ trợ khả năng hoạt động cao, trong suốt cho IP động: Hai đầu đường hầm có thể sử dụng IP động và ít bị thay đổi. Nếu bị đổi, cả phiên làm việc của Windows Terminal Server và SSH có thể chỉ bị ngưng lại trong vài giây và sẽ tiếp tục hoạt động bình thường.
- Cài đặt đơn giản trên bất kì hệ thống nào.

### III. CÀI ĐẶT OPENVPN TRÊN LINUX

*Hướng dẫn VPN Client to Site with OpenVPN on CentOS*

**Mô tả:**



User (VPN Client) từ bên ngoài hệ thống thực hiện quay VPN đến Server OpenVPN theo cơ chế chứng thực Certificate dùng Key + Password bảo vệ Key (khác với Password của Key).

Quá trình kết nối VPN thành công:

- 1 đường hầm (Tunnel ảo) có Subnet 10.8.0.0/24 được tạo ra, VPN Client sẽ kết nối đến hệ thống mạng công ty theo đường hầm này. (bảo mật)
- VPN Client sẽ được Server cấp phát 1 địa chỉ IP tĩnh thuộc subnet 10.8.0.0/24 để có thể giao tiếp với các Local Computer bên trong hệ thống.

**Bước 1:** Chuẩn bị

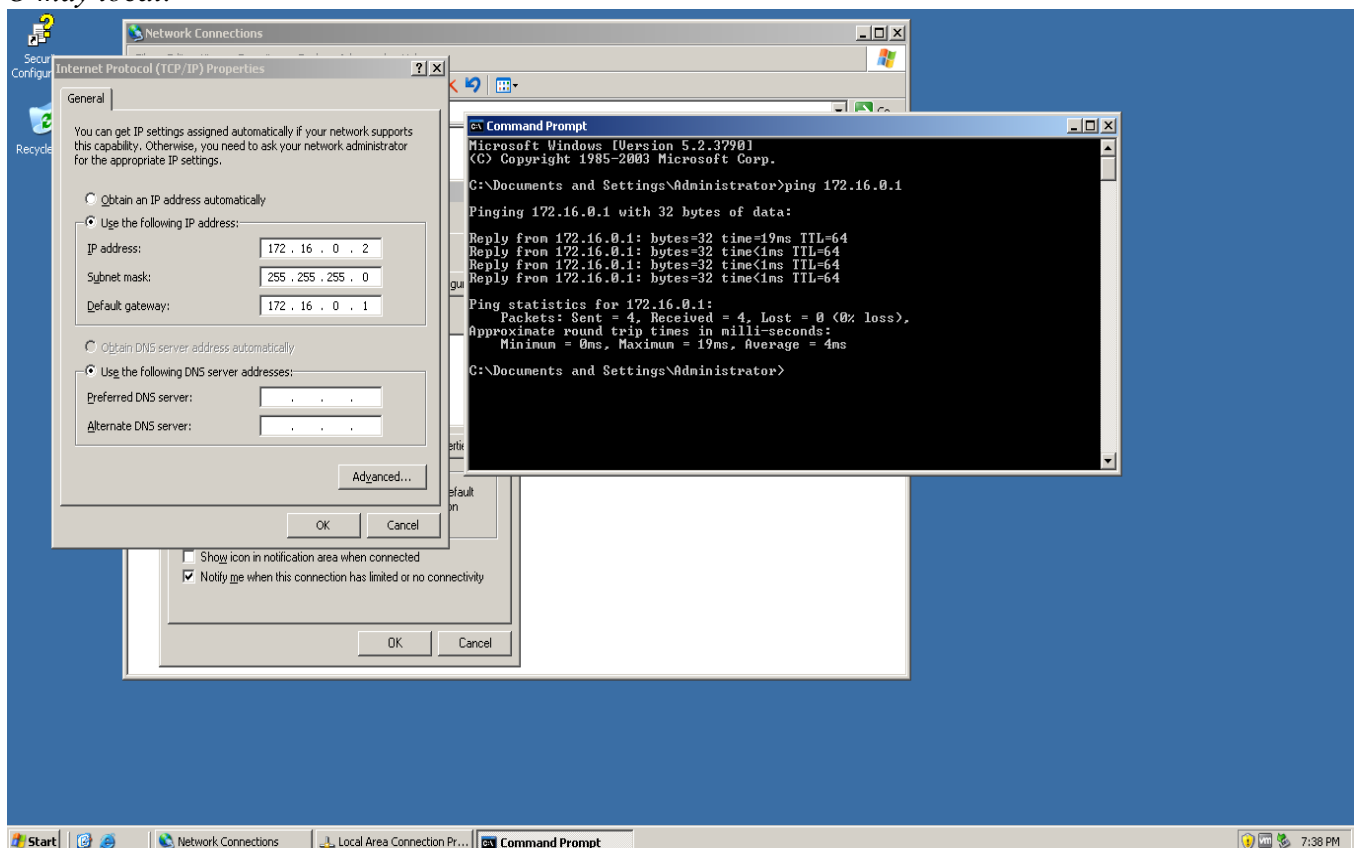
**Thiết lập, đặt IP theo mô hình.**

```
File Edit View Search Terminal Help
[root@vu Desktop]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:83:96:C5
          inet addr:192.168.202.131  Bcast:192.168.202.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:96c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:321 errors:0 dropped:0 overruns:0 frame:0
          TX packets:307 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39392 (38.4 KiB)  TX bytes:31168 (30.4 KiB)

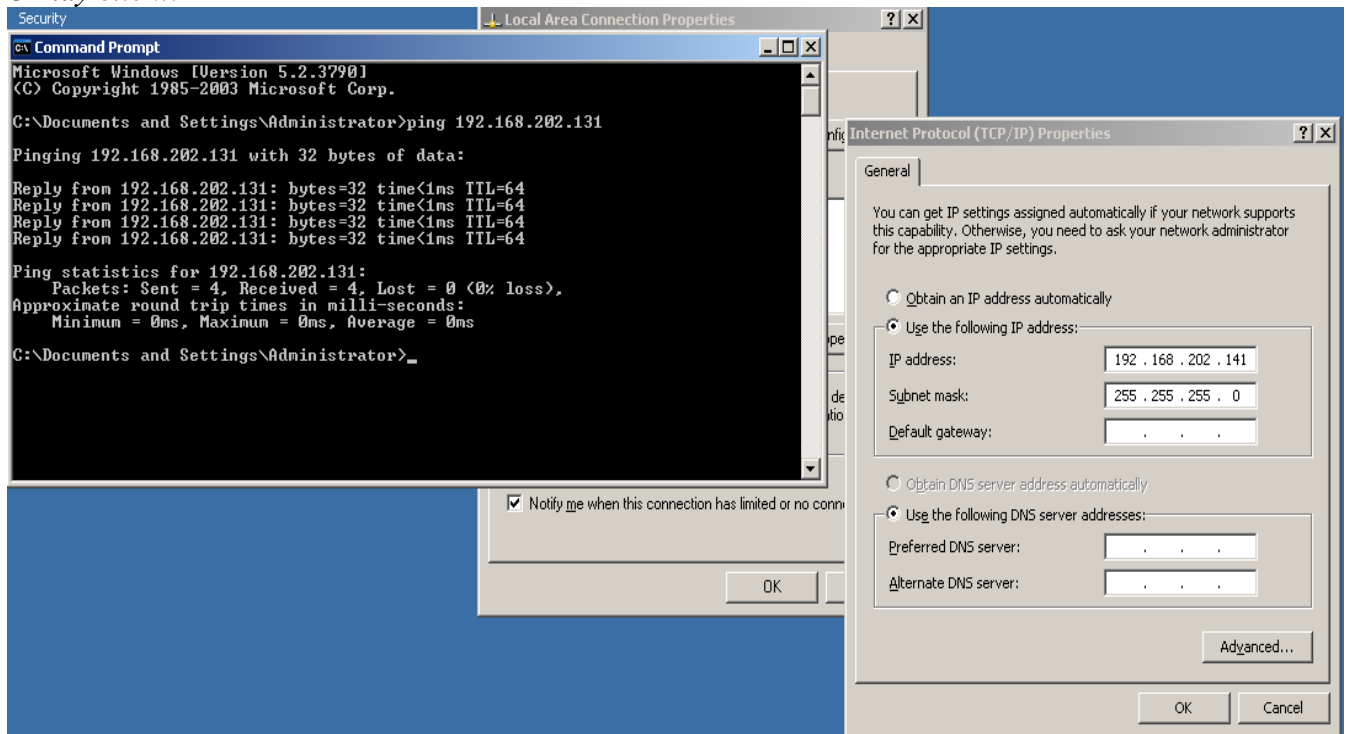
eth1      Link encap:Ethernet  HWaddr 00:0C:29:83:96:CF
          inet addr:172.16.0.1  Bcast:172.16.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:96cf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2389 (2.3 KiB)  TX bytes:1438 (1.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:720 (720.0 b)  TX bytes:720 (720.0 b)
```

*Ở máy local:*



Ở máy client:



### Đảm bảo:

Local Computer kết nối được với OpenVPN Server

VPN Client kết nối của OpenVPN Server (để quay VPN)

Softs: OpenVPN GUI: cài đặt trên VPN Client dùng để quay VPN đến Server

Gói lzo: cài đặt trên Server dùng để nén dữ liệu trên đường truyền

Gói openvpn: cài đặt trên Server làm OpenVPN Server.

Các softs này có thể download trên trang chủ hoặc đã để sẵn ở đây

<http://www.mediafire.com/?ir9fdp8nybzcyc8n>

### **Bước 2:** Cài đặt VPN Server

- Copy các gói cài đặt lzo-1.08, openvpn-2.0.9 vào thư mục cá nhân của root (/root)

- Giải nén và cài đặt gói lzo-1.08.tar.gz trước :

**tar -xvzf lzo-1.08.tar.gz :**

**cd lzo-1.08**

**./configure** (kiểm tra các thư viện đã đủ chưa)

**make** (thực hiện biên dịch)

**make install** (thực hiện cài đặt)

- Giải nén và cài đặt openvpn :

**tar -xvzf openvpn-2.0.9.tar.gz**

**cd openvpn-2.0.9**

**./configure**

**make**

**make install**

- Tạo thư mục /etc/openvpn:

**mkdir /etc/openvpn**

**Bước 3:** Tạo CA Certificate Server và Key

- Copy thư mục easy-rsa từ thư mục giải nén vào /etc/openvpn  
**cp /root/openvpn-2.0.9/easy-rsa/ /etc/openvpn/**

- Tạo CA Certificate Server:

**cd /etc/openvpn/easy-rsa/2.0/**

**mv \* ../** (move toàn bộ file trong thư mục 2.0/ ra thư mục easy-rsa/)



```
root@vu:/etc/openvpn/easy-rsa/2.0
File Edit View Search Terminal Help
[root@vu Desktop]# cd /etc/op
openldap/ openvpn/ opt/
[root@vu Desktop]# cd /etc/op
openldap/ openvpn/ opt/
[root@vu Desktop]# cd /etc/openvpn/easy-rsa/2.0/
[root@vu 2.0]# mv * ../
mv: overwrite './build-ca'? y
mv: overwrite './build-dh'? y
mv: overwrite './build-inter'? y
mv: overwrite './build-key'? y
mv: overwrite './build-key-pass'? y
mv: overwrite './build-key-pkcs12'? y
mv: overwrite './build-key-server'? y
mv: overwrite './build-req'? y
mv: overwrite './build-req-pass'? y
mv: overwrite './clean-all'? y
mv: overwrite './list-crl'? y
mv: overwrite './openssl.cnf'? y
mv: overwrite './README'? y
mv: overwrite './revoke-full'? y
mv: overwrite './sign-req'? y
mv: overwrite './vars'? y
[root@vu 2.0]#
```

**cd ..** (chuyển đến thư mục easy-rsa/)

**mkdir keys** (tạo thư mục /etc/openvpn/easy-rsa/keys để chứa keys, certificate)

**vi vars** (sửa các thông số mặc định)

```
export KEY_COUNTRY="VN"
export KEY_PROVINCE="TP HCM"
export KEY_CITY="HCM"
export KEY_ORG="hutech"
export KEY_EMAIL=openvpn@hutech.com
```

- Cấu hình CA:

**./vars** (dùng khởi tạo các biến môi trường đã thiết lập ở bước trên)

Khi chạy lệnh này, yêu cầu hệ thống là không có file nào trong thư mục keys cả, sẽ hiện ra dòng thông báo chạy lệnh ./clean-all để xóa trống thư mục /etc/openvpn/easy-rsa/keys nếu có.

## **./clean-all**

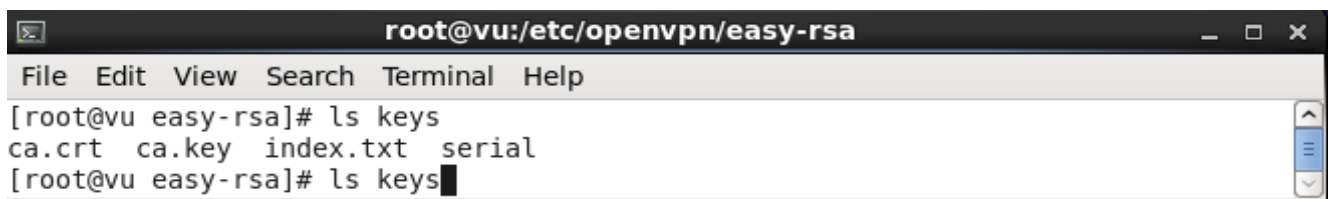
```
[root@vu easy-rsa]# mkdir keys
[root@vu easy-rsa]# vi vars
[root@vu easy-rsa]# . ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@vu easy-rsa]# ./clean-all
[root@vu easy-rsa]# █
```

- Tạo CA server: Tạo private key lưu trong file 'ca.key' cho CA

**./build-ca**, nhập các thông số vào, lưu ý: phần common name là xác định duy nhất do đó cần nhớ nhập **caserver**

```
[root@vu easy-rsa]# ./build-ca
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VN]:
State or Province Name (full name) [TP HCM]:
Locality Name (eg, city) [HCM]:
Organization Name (eg, company) [hutech]:
Organizational Unit Name (eg, section) []:OpenVPN
Common Name (eg, your name or your server's hostname) [hutech CA]:caserver
Email Address [openvpn@hutech.com]:
[root@vu easy-rsa]# █
```

Thực thi lệnh **ls keys** sẽ thấy có các file được tạo ra



```
root@vu:/etc/openvpn/easy-rsa
File Edit View Search Terminal Help
[root@vu easy-rsa]# ls keys
ca.crt ca.key index.txt serial
[root@vu easy-rsa]# ls keys█
```

- Tạo certificate và private key cho server (xin CA cho server)

Ở bước trên chúng ta đã tạo CA Server tương tự như server của các tổ chức bán Certificate (Verizon,...), trong bước này ta sẽ tạo Private Key cho các server có nhu cầu sử dụng việc chứng thực bằng Certificate (các ngân hàng, ..) ở đây server chúng ta là OpenVPN.

**./build-key-server openvpnsrver**

```
root@vu:/etc/openvpn/easy-rsa
File Edit View Search Terminal Help
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VN]:
State or Province Name (full name) [TP HCM]:
Locality Name (eg, city) [HCM]:
Organization Name (eg, company) [hutech]:
Organizational Unit Name (eg, section) []:Linux
Common Name (eg, your name or your server's hostname) [openvpnserver]:openvpnserver
Email Address [openvpn@hutech.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'VN'
stateOrProvinceName     :PRINTABLE:'TP HCM'
localityName            :PRINTABLE:'HCM'
organizationName        :PRINTABLE:'hutech'
organizationalUnitName  :PRINTABLE:'Linux'
commonName              :PRINTABLE:'openvpnserver'
emailAddress            :IA5STRING:'openvpn@hutech.com'
Certificate is to be certified until Nov 14 05:14:56 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

ls keys/ xem có thêm vài file được tạo ra

```
root@vu:/etc/openvpn/easy-rsa
File Edit View Search Terminal Help
[root@vu easy-rsa]# ls keys/
01.pem  index.txt      openvpnserver.crt  serial
ca.crt  index.txt.attr openvpnserver.csr  serial.old
ca.key  index.txt.old  openvpnserver.key
```

- Tạo Diffie Hellman ( DH ): bấm keys

**./build-dh**

Quá trình bấm keys có thể diễn ra chậm.

- Tạo Client Certificate và Private key cho Client (để thực hiện chứng thực 2 chiều). Ở đây tạo keys cho user kuti và kuteo.

**./build-key kuti** (common name: **kuti**)



```
root@vu:/etc/openvpn/easy-rsa
File Edit View Search Terminal Help
writing new private key to 'kuti.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VN]:
State or Province Name (full name) [TP HCM]:
Locality Name (eg, city) [HCM]:
Organization Name (eg, company) [hutech]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [kuti]:kuti
Email Address [openvpn@hutech.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'VN'
stateOrProvinceName  :PRINTABLE:'TP HCM'
localityName         :PRINTABLE:'HCM'
organizationName     :PRINTABLE:'hutech'
commonName           :PRINTABLE:'kuti'
emailAddress         :IA5STRING:'openvpn@hutech.com'
Certificate is to be certified until Nov 14 05:21:30 2024 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@vu easy-rsa]#
```

### Ta làm tương tự với user kuteo.

Xong bước này là chúng ta đã hoàn thành việc tạo các Certificate và Keys cần thiết cho việc chứng thực

ls keys/ ra xem kết quả ở bước này



```
root@vu:/etc/openvpn/easy-rsa
File Edit View Search Terminal Help
[root@vu easy-rsa]# ls keys/
01.pem dh1024.pem kuteo.crt kuti.key serial.old
02.pem index.txt kuteo.csr openvpnserver.crt
03.pem index.txt.attr kuteo.key openvpnserver.csr
ca.crt index.txt.attr.old kuti.crt openvpnserver.key
ca.key index.txt.old kuti.csr serial
[root@vu easy-rsa]#
```

#### **Bước 4:** Cấu hình chức năng Forwarding (dùng để thực hiện Lan Routing)

Ta thực thi lệnh : **vi /etc/sysctl.conf**

Chỉnh sửa ở hàng 7: **net.ipv4.ip\_forward = 1**

**sysctl -p** (để cho các thông số có hiệu lực)

**echo 1 > /proc/sys/net/ipv4/ip\_forward**

#### **Bước 5:** Cấu hình VPN Server

- Copy file cấu hình server.conf mẫu từ source cài đặt vào /etc/openvpn/

**cp /root/openvpn-2.0.9/sample-config-files/server.conf /etc/openvpn/**

- Chỉnh sửa file cấu hình:

**cd /etc/openvpn/**

**vi server.conf**

**Dòng 25:** local 192.168.202.131 (chọn card mạng user quay VPN đến, có thể không cần option này)

**Dòng 32:** port 1723 (default là 1194, thường port này bị firewall block nên đặt 1723 cho giống port VPN Server của Windows Server)

**Dòng 36:** proto udp (protocol udp)

**Dòng 53:** dev tun

**Dòng 78:** ca /etc/openvpn/easy-rsa/keys/ca.crt (khai báo đường dẫn cho file ca.crt)

**Dòng 79:** cert /etc/openvpn/easy-rsa/keys/openvpnserver.crt

**Dòng 80:** key /etc/openvpn/easy-rsa/keys/openvpnserver.key

**Dòng 87:** dh /etc/openvpn/easy-rsa/keys/dh1024.pem

**Dòng 96:** server 10.8.0.0 255.255.255.0

**Dòng 103:** ;ifconfig-pool-persist ipp.txt (dùng để cho VPN Client lấy lại IP trước đó nếu bị đứt kết nối với VPN server, do chúng ta dùng IP tĩnh nên không sử dụng thông số này)

**Dòng 124:** push "route 172.16.0.0 255.255.255.0" (lệnh này sẽ đẩy route mạng 172.16.0.0 đến Client, hay còn gọi là Lan Routing trong Windows Server, giúp cho VPN Client thấy được mạng bên trong của công ty)

**Dòng 125:** ;push "route 192.168.202.131 255.255.255.0" Client đã connect được nên không cần add route dòng này (nếu có sẽ không chạy được)

**Dòng 138:** client-config-dir ccd (dùng để khai báo cấp IP tĩnh cho VPN Client)

**Dòng 196:** client-to-client (cho phép các VPN client nhìn thấy nhau, mặc định client chỉ thấy server)

- Cấu hình file IP tĩnh tương ứng với từng User:

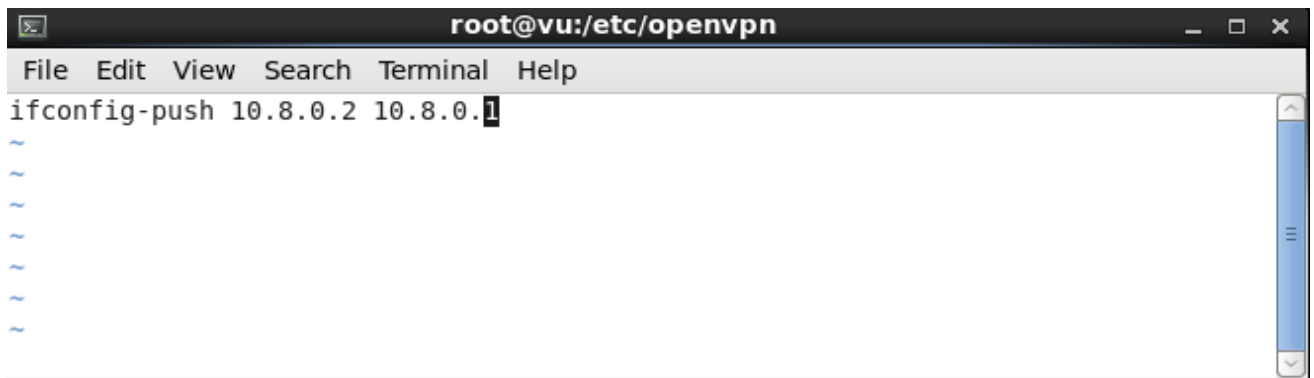
+ Tạo thư mục ccd (/etc/openvpn/ccd)

**mkdir /etc/openvpn/ccd**

+ Tạo profile cho user kuti

**vi /etc/openvpn/ccd/kuti**

**1: ifconfig-push 10.8.0.2 10.8.0.1**



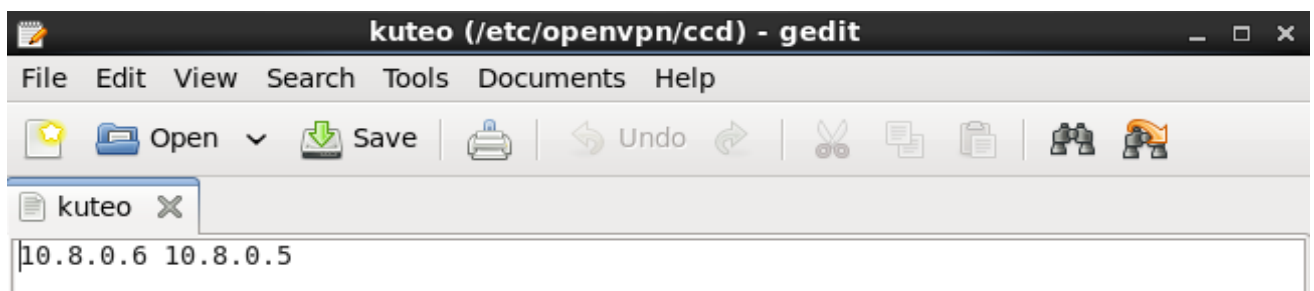
```
root@vu:/etc/openvpn
File Edit View Search Terminal Help
ifconfig-push 10.8.0.2 10.8.0.1
~
~
~
~
~
~
```

theo file cấu hình trên user kuti sẽ nhận IP là 10.8.0.2

+ Tạo profile cho user kuteo

**vi /etc/openvpn/ccd/kuteo**

**1: ifconfig-push 10.8.0.6 10.8.0.5**



```
kuteo (/etc/openvpn/ccd) - gedit
File Edit View Search Tools Documents Help
[Icons: Open, Save, Undo, etc.]
kuteo x
10.8.0.6 10.8.0.5
```

theo file cấu hình trên user kuti sẽ nhận IP là 10.8.0.6

Bước 6: Start VPN Server và tiến hành quay VPN, test với các user kuti, kuteo làm tương tự.

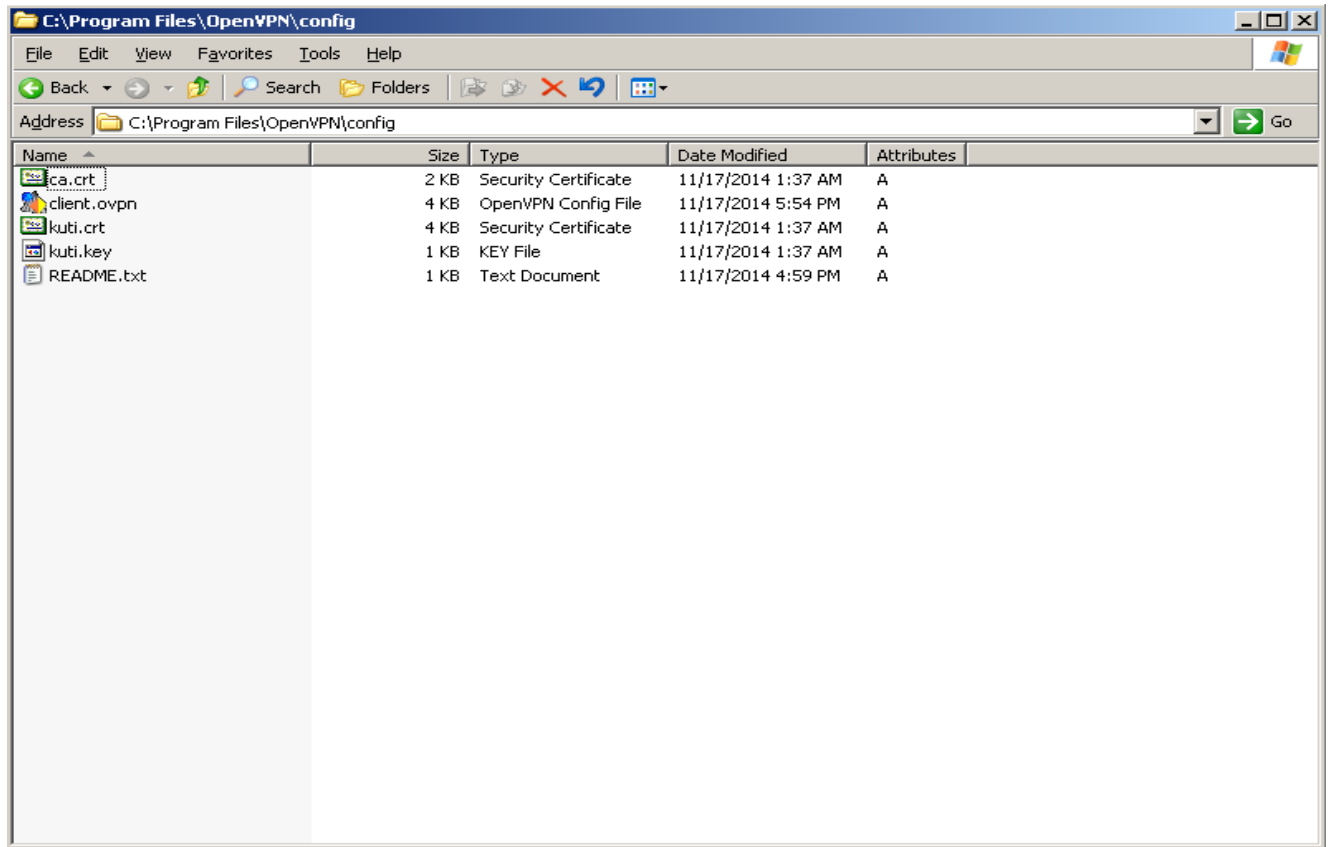
- Start OpenVPN Server

**cd /etc/openvpn**

**openvpn server.conf**

```
root@vu:/etc/openvpn
File Edit View Search Terminal Help
[root@vu Desktop]# cd /etc/openvpn
[root@vu openvpn]# openvpn server.conf
Mon Nov 17 02:11:16 2014 OpenVPN 2.0.9 i686-pc-linux [SSL] [LZO] [EPOLL] built on Nov 16 2014
Mon Nov 17 02:11:16 2014 Diffie-Hellman initialized with 1024 bit key
Mon Nov 17 02:11:16 2014 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Mon Nov 17 02:11:16 2014 TUN/TAP device tun0 opened
Mon Nov 17 02:11:16 2014 /sbin/ifconfig tun0 10.8.0.1 pointopoint 10.8.0.2 mtu 1500
Mon Nov 17 02:11:16 2014 /sbin/route add -net 10.8.0.0 netmask 255.255.255.0 gw 10.8.0.2
Mon Nov 17 02:11:16 2014 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
Mon Nov 17 02:11:16 2014 UDPv4 link local (bound): [undef]:1723
Mon Nov 17 02:11:16 2014 UDPv4 link remote: [undef]
Mon Nov 17 02:11:16 2014 MULTI: multi_init called, r=256 v=256
Mon Nov 17 02:11:16 2014 IFCONFIG POOL: base=10.8.0.4 size=62
Mon Nov 17 02:11:16 2014 Initialization Sequence Completed
```

- Cài đặt, config OpenVPN GUI cho Client
- + Chạy file **openvpn-2.0.9-gui-1.0.3-install.exe**, cài đặt mặc định.
- + Chép các file key, certificate cần thiết là: **ca.crt**, **kuti.crt**, **kuti.key** vào đường dẫn **C:\Program Files\OpenVPN\config**
- + Copy file **client.ovpn** từ đường dẫn **C:\Program Files\OpenVPN\sample-config** vào **C:\Program Files\OpenVPN\config**



#### + Edit file client.ovpn:

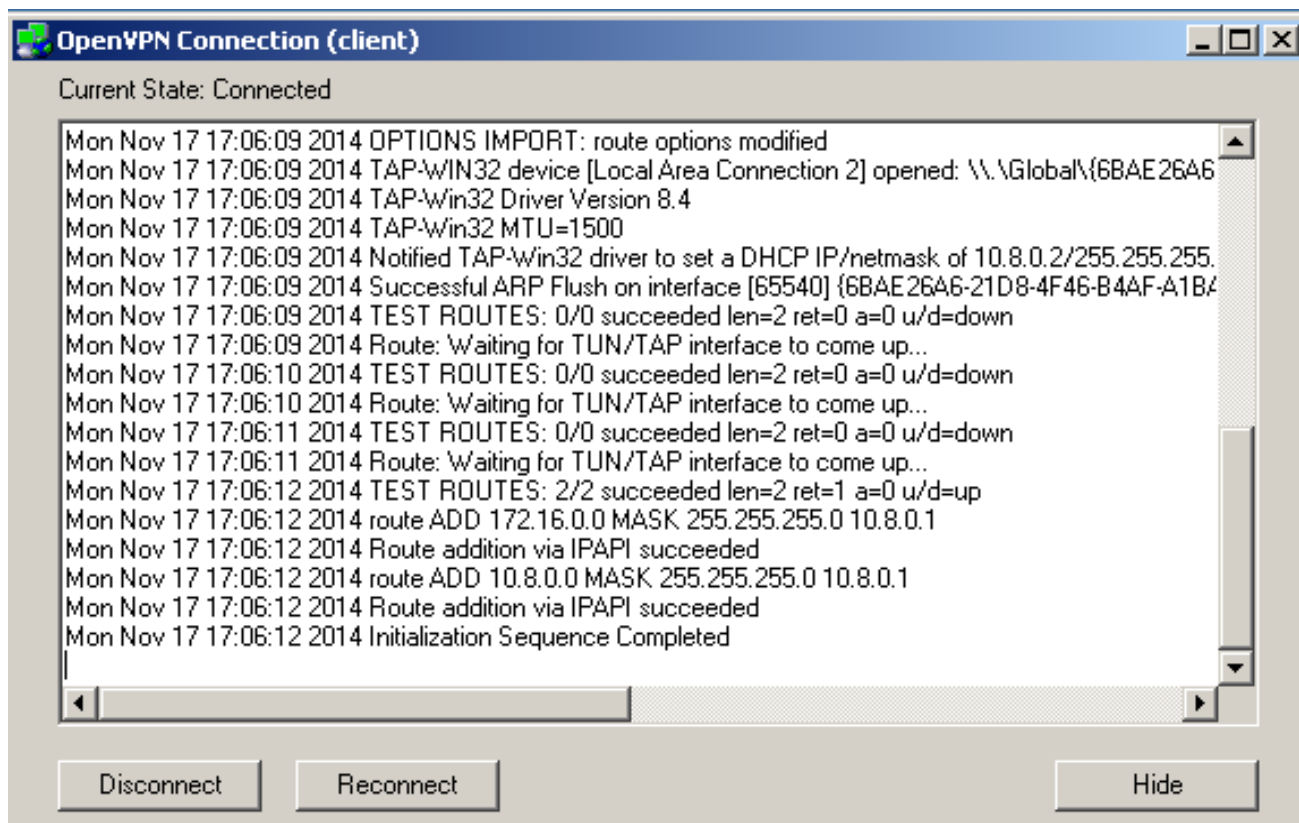
```

client
dev tun (tunnel)
proto udp
remote 192.168.202.131 1723
nobind
persist-key
persist-tun
ca ca.crt (khai báo CA server)
cert kuti.crt (certificate user kuti)
key kuti.key (private key kuti)
comp-lzo
verb 3

```

#### - Quay VPN

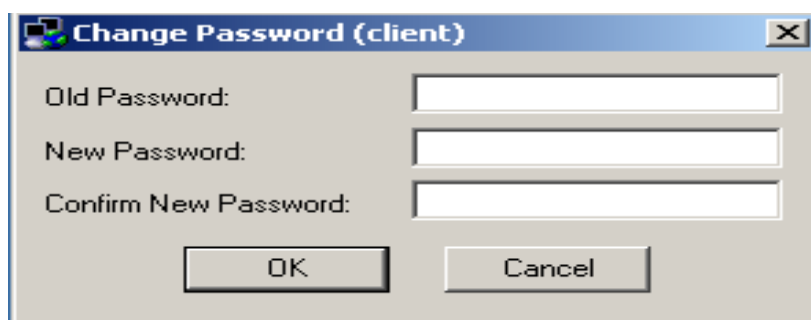
Right Click vào biểu tượng Card mạng mới sau khi cài OpenVPN GUI, **chọn Connects**



Như vậy là đã quay VPN thành công, nhận IP 10.8.0.2, các route cần thiết cũng được add vào.

#### - Set password bảo vệ Key:

Right click vào Icon OpenVPN Chọn Change Password



Sau này khi quay VPN, hệ thống sẽ yêu cầu nhập password đã đặt.

#### - Test:

+ Kiểm tra Route print: start --> run --> cmd --> route print

```
C:\ Command Prompt
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 ff 6b ae 26 a6 ..... TAP-Win32 Adapter U8
0x10004 ...00 0c 29 31 6a 46 ..... Intel(R) PRO/1000 MT Network Connection
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface           Metric
10.8.0.0                    255.255.255.252   10.8.0.2            10.8.0.2            30
10.8.0.0                    255.255.255.0     10.8.0.1            10.8.0.2            1
10.8.0.2                    255.255.255.255   127.0.0.1           127.0.0.1           30
10.255.255.255              255.255.255.255   10.8.0.2            10.8.0.2            30
127.0.0.0                   255.0.0.0         127.0.0.1           127.0.0.1           1
172.16.0.0                  255.255.255.0     10.8.0.1            10.8.0.2            1
192.168.202.0               255.255.255.0     192.168.202.141     192.168.202.141     10
192.168.202.141             255.255.255.255   127.0.0.1           127.0.0.1           10
192.168.202.255             255.255.255.255   192.168.202.141     192.168.202.141     10
224.0.0.0                   240.0.0.0         10.8.0.2            10.8.0.2            30
224.0.0.0                   240.0.0.0         192.168.202.141     192.168.202.141     10
255.255.255.255             255.255.255.255   10.8.0.2            10.8.0.2            1
255.255.255.255             255.255.255.255   192.168.202.141     192.168.202.141     1
=====
Persistent Routes:
None
```

Ok, đã thấy server đã add route cho client kuti

+ Kiểm tra kết nối với mạng bên trong (máy local) bằng lệnh ping và thành công !!!

```
C:\Documents and Settings\Administrator>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=3ms TTL=127
Reply from 172.16.0.2: bytes=32 time=1ms TTL=127
Reply from 172.16.0.2: bytes=32 time=1ms TTL=127
Reply from 172.16.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

+ Quay VPN với user kuteo

Làm các bước tương tự như user kuti

Như vậy chúng ta đã hoàn thành bài Lab này.