

OpenVPN 如何 CentOS 5.5 amd 64



如何安装 OpenVPN 在 CentOS 5.5 amd 64 上。本文提供详细的步骤，包括安装 OpenVPN 服务器和客户端。本文使用 Text Mode 进行安装。

安装 OpenVPN 服务器。首先安装 `vpnservice` 和 `openvpn` 包。然后配置 `openvpn-as` 服务。创建 `vpn` 用户并设置密码。最后安装 `rpmforge` 包。

如何安装 OpenVPN 客户端。

1. Linux CentOS 5.5 amd 64 如何安装 OpenVPN 服务器
2. IP Server 192.168.1.10
3. Client 如何安装 Windows 7 (32bit 如何安装 OpenVPN 客户端 64 bit 如何安装 OpenVPN 客户端) 如何安装 OpenVPN 客户端 如何 Ping 如何 Server 如何安装 OpenVPN 客户端

如何安装 OpenVPN 服务器

1. 如何安装 OpenVPN 服务器 `repo` 如何安装 OpenVPN 服务器 <http://packages.sw.be/rpmforge-release/> 如何安装 OpenVPN 服务器 OS 如何安装 OpenVPN 服务器

```
[root@vpn ~]# wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
```

2. 如何安装 OpenVPN 服务器 `repo` 如何安装 OpenVPN 服务器 `rpm`

```

[root@vpn ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  mbox
rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
[root@vpn ~]# rpm -ivh rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
warning: rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm: Header V3 DSA signature: NOKEY, key ID 6b8d79e6
Preparing...
##### [100%]
1:rpmforge-release
##### [100%]
[root@vpn ~]#

```

3. `yum`

```

[root@vpn ~]# yum search openvpn
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* addons: mirror.issp.co.th
* base: mirror.issp.co.th
* extras: mirror.issp.co.th
* rpmforge: fr2.rpmfind.net
* updates: mirror.issp.co.th
===== Matched: openvpn
=====
kvpnc.x86_64 : Frontend for various VPN clients
openvpn.x86_64 : secure tunneling daemon

```

4. `yum`

```

[root@vpn ~]# yum -y install openvpn
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile

```

* addons: mirror.issp.co.th
* base: mirror.issp.co.th
* extras: mirror.issp.co.th
* rpmforge: apt.sw.be
* updates: mirror.issp.co.th
rpmforge

| 1.1 kB 00:00
rpmforge/primary

| 2.1 MB 00:02
rpmforge

10272/10272

Setting up Install Process

Resolving Dependencies

-> Running transaction check

-> Package openvpn.x86_64 0:2.1.4-1.el5.rf set to be updated

-> Processing Dependency: lzo for package: openvpn

-> Processing Dependency: liblzo2.so.2()(64bit) for package:
openvpn

-> Running transaction check

-> Package lzo.x86_64 0:2.04-1.el5.rf set to be updated

-> Finished Dependency Resolution

Dependencies Resolved

=====
=====

Package

Arch

Version

Repository

Size

=====
=====

Installing:

openvpn

x86_64
2.1.4-1.el5.rf
rpmforge 442 k
Installing for dependencies:
lzo
x86_64
2.04-1.el5.rf
rpmforge 139 k

Transaction Summary

=====

Install 2 Package(s)
Upgrade 0 Package(s)

Total download size: 581 k

Downloading Packages:

(1/2):

lzo-2.04-1.el5.rf.x86_64.rpm
| 139 kB 00:01

(2/2):

openvpn-2.1.4-1.el5.rf.x86_64.rpm
| 442 kB 00:01

Total

187 kB/s | 581 kB 00:03

Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
Installing
lzo

:


```
clean-all          list-crl          openssl-0.9.6.cnf
pkitool            revoke-full      vars
```

```
[root@vpn 2.0]# vi vars
```

7.0 編輯 vars 檔案 Cert (Certificate) 檔案 (Certificate) 使用 vi 編輯器或 pico 編輯器編輯 vars 檔案，將以下內容填入。

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="TH"
export KEY_PROVINCE="Chiangmai"
export KEY_CITY="Chiangmai"
export KEY_ORG="RMUTL"
export KEY_EMAIL="teppap@rmutl.ac.th"
```

8.0 設定 vars 檔案的執行權限。

```
[root@vpn 2.0]# chmod +x *
```

9.0 執行 Cert 檔案，將 vars 檔案的內容填入。執行 clean-all 命令，將 /usr/share/doc/openvpn-2.1.4/easy-rsa/2.0/keys 目錄下的所有檔案刪除。執行 build-ca 命令，生成 1024 位 RSA 私鑰。

```
[root@vpn 2.0]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on
/usr/share/doc/openvpn-2.1.4/easy-rsa/2.0/keys
[root@vpn 2.0]# ./clean-all
[root@vpn 2.0]# ls -l keys/
total 4
-rw-r--r-- 1 root root 0 Feb 10 13:21 index.txt
-rw-r--r-- 1 root root 3 Feb 10 13:21 serial
[root@vpn 2.0]# ./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) [TH]:

State or Province Name (full name) [Chiangmai]:

Locality Name (eg, city) [Chiangmai]:

Organization Name (eg, company) [RMUTL]:

Organizational Unit Name (eg, section) []:RMUTL

Common Name (eg, your name or your server's hostname) [RMUTL CA]:vpn.rmutl.ac.th

Name []:vpn.rmutl.ac.th

Email Address [teppap@rmutl.ac.th]:

[root@vpn 2.0]# **ls -l keys/**

total 12

-rw-r--r-- 1 root root 1424 Feb 10 13:22 ca.crt

-rw----- 1 root root 891 Feb 10 13:22 ca.key

-rw-r--r-- 1 root root 0 Feb 10 13:21 index.txt

-rw-r--r-- 1 root root 3 Feb 10 13:21 serial

[root@vpn 2.0]# **./build-key-server vpn.rmutl.ac.th**

Generating a 1024 bit RSA private key

.....+++++

.....+++++

writing new private key to 'vpn.rmutl.ac.th.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) [TH]:

State or Province Name (full name) [Chiangmai]:

Locality Name (eg, city) [Chiangmai]:

Organization Name (eg, company) [RMUTL]:

Organizational Unit Name (eg, section) []:RMUTL

Common Name (eg, your name or your server's hostname)
[vpn.rmutl.ac.th]:

Name []:vpn.rmutl.ac.th

Email Address [teppap@rmutl.ac.th]:

Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /usr/share/doc/openvpn-2.1.4/easy-
rsa/2.0/openssl.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName :PRINTABLE:'TH'

stateOrProvinceName :PRINTABLE:'Chiangmai'

localityName :PRINTABLE:'Chiangmai'

organizationName :PRINTABLE:'RMUTL'

organizationalUnitName:PRINTABLE:'RMUTL'

commonName :PRINTABLE:'vpn.rmutl.ac.th'

name :PRINTABLE:'vpn.rmutl.ac.th'

emailAddress :IA5STRING:'teppap@rmutl.ac.th'

Certificate is to be certified until Feb 7 06:23:57 2021 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@vpn 2.0]#

[root@vpn 2.0]# **ls -l keys/**

total 48

-rw-r--r-- 1 root root 4200 Feb 10 13:24 01.pem

-rw-r--r-- 1 root root 1424 Feb 10 13:22 ca.crt

-rw---- 1 root root 891 Feb 10 13:22 ca.key

-rw-r--r-- 1 root root 148 Feb 10 13:24 index.txt

-rw-r--r-- 1 root root 21 Feb 10 13:24 index.txt.attr

-rw-r--r-- 1 root root 0 Feb 10 13:21 index.txt.old

-rw-r--r-- 1 root root 3 Feb 10 13:24 serial

-rw-r--r-- 1 root root 3 Feb 10 13:21 serial.old

-rw-r--r-- 1 root root 4200 Feb 10 13:24 vpn.rmutl.ac.th.crt

-rw-r--r-- 1 root root 745 Feb 10 13:23 vpn.rmutl.ac.th.csr

-rw---- 1 root root 887 Feb 10 13:23 vpn.rmutl.ac.th.key

[root@vpn 2.0]# **cat keys/vpn.rmutl.ac.th.key**

—BEGIN RSA PRIVATE KEY—

MIICXQIBAAKBgQC3FvB9xhcMjFXl/H9cCA5fteVmHwu+BzioudyNMj33zRF11

WGK

wYmtp1C2biSHtSm66y4JqE3t6/oNBhKHhtAwpYmDHuHXPo15VKmH/DkaeouR0

rbc

CYy/eF0dmKc0ug0j4WwjY7233611mKY5wM9acGyEfbVQJioF1mjGV13oTwIDA

QAB

AoGAAzLSLsTILx5hfNU/YN17c0/+pBez2zrBUqdDLPFPigeAYTTKr0jPhdFGa

I/z

8LfVQYdWnjDqfmADXStYNC65h7oh/Ll5n4jM9nVLPf3R0B1zqGeP7k1ZuzfrQ

Nm0

yGsl870a3vDXUUiLs0A7GsQ4BvNnkb5acLCHjgnEY0oazgECQQDeHY4biDrwt

aBJ

cHKNlDo80hl4RpV55pFB6kxtgi03XnixCjLwHEYM97Gklw37/MPoNfIs7gINL

DKy

MK2BvaDPAKEA0wVHNkuh+lJ3Y0sn1N080fZIdZvJKScp2oDYDfGJFBaNcz33U

2gu

288ZmQb2rZNTqdEovP6Ico85VkkCw2oggQJBAJJ9XZcM7wqITzGARxzXEN3CF

2g6

7SSb1u0wjLlLLUiymjA/IbTLuQojHGn6mIyH6bLxXAafSHg74KUFirGPQMCQ
Ewy

gpj0VkuInURnpxpJkGMQ41HlCIYNJ2fCEppYYpw97q5Xky77RC7Zsmy2vhcKi
CGY

scnqkAq2f4ucIDCHBwECQQDIWxF7c4QIFdaf4ZWUZG0uo7L0/dsjPiUuyg0FB
sA1

l0FAhiCH8ZRErTejC3mLB/HdYL43futnhvix/YEDqoxr

—END RSA PRIVATE KEY—

[root@vpn 2.0]# **cat keys/vpn.rmutl.ac.th.crt**

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=TH, ST=Chiangmai, L=Chiangmai, O=RMUTL, OU=RMUTL,
CN=vpn.rmutl.ac.th/name=vpn.rmutl.ac.th/emailAddress=teppap@r
mutl.ac.th

Validity

Not Before: Feb 10 06:23:57 2011 GMT

Not After : Feb 7 06:23:57 2021 GMT

Subject: C=TH, ST=Chiangmai, L=Chiangmai, O=RMUTL, OU=RMUTL,
CN=vpn.rmutl.ac.th/name=vpn.rmutl.ac.th/emailAddress=teppap@r
mutl.ac.th

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:b7:16:f0:7d:c6:17:0c:8c:55:e5:fc:7f:5c:08:

0e:5f:b5:e5:66:1f:0b:be:07:38:a8:b9:dc:8d:32:

3d:f7:cd:11:75:d5:61:8a:c1:89:ad:a7:50:b6:6e:

24:87:b6:c9:ba:eb:2e:09:a8:4d:ed:eb:fa:0d:06:

12:87:86:d0:30:a5:89:83:1e:e1:d7:3e:8d:79:54:

a9:87:fc:39:1a:7a:8b:91:3a:b6:dc:09:8c:bf:78:

5d:1d:98:a7:34:ba:03:a3:e1:6c:23:63:bd:b7:df:

ad:75:98:a6:39:c0:cf:5a:70:6c:84:7d:b5:50:26:

2a:05:d6:68:c6:57:5d:e8:4f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Cert Type:

SSL Server

Netscape Comment:

Easy-RSA Generated Server Certificate

X509v3 Subject Key Identifier:

9B:37:63:86:89:D8:F5:9A:D6:A4:5F:8A:50:3A:E2:67:25:0D:18:14

X509v3 Authority Key Identifier:

keyid:8A:E7:4E:11:35:25:94:5E:F8:D3:E9:62:8E:E4:7B:00:32:57:80:5F

DirName:/C=TH/ST=Chiangmai/L=Chiangmai/O=RMUTL/OU=RMUTL/CN=vpn.rmutl.ac.th/name=vpn.rmutl.ac.th/emailAddress=teppap@rmutl.ac.th

serial:FC:A0:4D:C7:BE:EB:70:EA

X509v3 Extended Key Usage:

TLS Web Server Authentication

X509v3 Key Usage:

Digital Signature, Key Encipherment

Signature Algorithm: sha1WithRSAEncryption

5a:13:d3:d6:95:8c:5e:38:0e:1c:7a:a2:5d:8f:e2:40:0d:ab:

5d:6f:6b:bc:09:fe:bb:97:fc:35:d0:e4:76:e2:1c:6c:c8:75:

60:3f:44:e9:c2:ce:27:08:e4:18:b2:b2:5b:63:9c:6d:c5:36:

7f:5a:5f:d4:b3:dd:5e:2f:35:04:09:c8:11:92:12:a7:64:50:

56:18:cb:4a:f2:8d:b5:6d:b0:11:db:b8:1d:bb:44:9b:ec:11:

99:27:3c:01:8e:b6:a6:b3:ba:26:d1:a9:69:cc:7d:31:2d:bc:

d4:57:10:89:3a:8a:02:a9:da:fc:ca:94:0e:b8:d4:ac:3c:00:

c3:ce

—BEGIN CERTIFICATE—

MIIEtzCCA7igAwIBAgIBATANBgkqhkiG9w0BAQUFADCBrDELMAkGA1UEBhMCMCV
Egx

EjAQBgNVBAGTCUNoawFuZ21haTESMBAGA1UEBxMJQ2hpYW5nbWFpMQ4wDAYDV
QQK

EwVSTVVUTDE0MAwGA1UECxMFUk1VVEwxGDAWBgNVBAMTD3Zwbi5ybXV0bC5hY

y50

aDEYMBYGA1UEKRMPdnBuLnJtdXRSLmFjLnRoMSEwHwYJKoZIHvcNAQkBFhJ0Z
XBw

YXBACm11dGwuYWMudGgwHhcNMTEwMjEwMDYyMzU3WhcNMjEwMjA3MDYyMzU3W
jCB

rDELMakGA1UEBhMCVEgxEjAQBgNVBAgTCUNoaWfuZ21haTESMBAGA1UEBxMJQ
2hp

YW5nbWFPMQ4wDAYDVQKKEwVSTVVUTDEOMAwGA1UECxFUk1VVEwGDAWBgNVB
AMT

D3Zwbi5ybXV0bC5hYy50aDEYMBYGA1UEKRMPdnBuLnJtdXRSLmFjLnRoMSEwH
wYJ

KoZIHvcNAQkBFhJ0ZXBwYXBACm11dGwuYWMudGgwGZ8wDQYJKoZIHvcNAQE
BBQAD

gY0AMIGJAoGBALcW8H3GFwyMVeX8f1wIDl+15WYfC74H0Ki53I0yPffNEXXVY
YrB

ia2nULZuJIe2ybrLgmoTe3r+g0GEoeG0DCliYMe4dc+jXlUqYf80Rp6i5E6t
twJ

jL94XR2YpzS6A6PhbCNjvbfFrXWYpjnAz1pwbIR9tVAmKgXWaMZXXehPAgMBA
AGj

ggF9MIIBeTAJBgNVHRMEAjAAMBEGCWCgsAGG+EIBAQQEAwIGQDA0BgIghkgBh
vhC

AQ0EJxYlRWFzeS1SU0EgR2VuZXJhdGVkIFNlcnZlciBDZXJ0aWZpY2F0ZTAdb
gNV

HQ4EFgQUmzdjhonY9ZrWpF+KUDriZyUNGBQwgeEGA1UdIwSB2TCB1oAUiud0E
TUl

lF740+lijuR7ADJXgF+hgbKkga8wgawxCzAJBgNVBAYTAlRIMRIwEAYDVQQIE
wLD

aGlhbmdtYWkxEjAQBgNVBAcTCUNoaWfuZ21haTEOMAwGA1UEChMFUk1VVEwxD
jAM

BgNVBAStBVJNVVRMMRgwFgYDVQQDEw92cG4ucm11dGwuYWMudGgwGDAWBgNVB
CkT

D3Zwbi5ybXV0bC5hYy50aDEhMB8GCSqGSIB3DQEJARYSdGVwcGFwQHJtdXRSL
mFj

LnRoggkA/KBNx77rc0owEwYDVR0lBAwwCgYIKwYBBQUHAWewCwYDVR0PBAQDA
gWg

MA0GCSqGSIB3DQEBBQUAA4GBAFoT09aVjF44Dhx6o12P4kANq11va7wJ/ruX/
DXQ

5HbiHGzIdWA/R0nCzicI5BiyslTjnG3FNn9aX9Sz3V4vNQQJyBGSEqdkUFYYy
0ry

jbVtsBHbuB27RJvsEZknPAG0tqazuibRqWnMfTEtvNRXEIk6igKp2vzKlA641
Kw8

AMPO

—END CERTIFICATE—

[root@vpn 2.0]#

[root@vpn 2.0]#

[root@vpn 2.0]#

[root@vpn 2.0]# *./build-dh*

Generating DH parameters, 1024 bit long safe prime, generator
2

This is going to take a long time

.....++*++*++*

[root@vpn 2.0]#

[root@vpn 2.0]# *ls -l keys/*

total 52

-rw-r--r-- 1 root root 4200 Feb 10 13:24 01.pem

-rw-r--r-- 1 root root 1424 Feb 10 13:22 ca.crt

-rw----- 1 root root 891 Feb 10 13:22 ca.key

-rw-r--r-- 1 root root 245 Feb 10 13:25 dh1024.pem

-rw-r--r-- 1 root root 148 Feb 10 13:24 index.txt

-rw-r--r-- 1 root root 21 Feb 10 13:24 index.txt.attr

-rw-r--r-- 1 root root 0 Feb 10 13:21 index.txt.old

-rw-r--r-- 1 root root 3 Feb 10 13:24 serial

-rw-r--r-- 1 root root 3 Feb 10 13:21 serial.old

-rw-r--r-- 1 root root 4200 Feb 10 13:24 vpn.rmutl.ac.th.crt

-rw-r--r-- 1 root root 745 Feb 10 13:23 vpn.rmutl.ac.th.csr

-rw----- 1 root root 887 Feb 10 13:23 vpn.rmutl.ac.th.key

[root@vpn 2.0]#

[root@vpn 2.0]# *./build-key client*

Generating a 1024 bit RSA private key

.....++++++

.....++++++

writing new private key to 'client.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) [TH]:

State or Province Name (full name) [Chiangmai]:

Locality Name (eg, city) [Chiangmai]:

Organization Name (eg, company) [RMUTL]:

Organizational Unit Name (eg, section) []:RMUTL

Common Name (eg, your name or your server's hostname) [client]:

Name []:

Email Address [teppap@rmutl.ac.th]:

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /usr/share/doc/openssl-2.1.4/easy-rsa/2.0/openssl.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName :PRINTABLE:'TH'

stateOrProvinceName :PRINTABLE:'Chiangmai'

localityName :PRINTABLE:'Chiangmai'

organizationName :PRINTABLE:'RMUTL'

organizationalUnitName:PRINTABLE:'RMUTL'

commonName :PRINTABLE:'client'

emailAddress :IA5STRING:'teppap@rmutl.ac.th'

Certificate is to be certified until Feb 7 06:27:42 2021 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@vpn 2.0]#

10. `cp -rf /usr/share/doc/openvpn-2.1.4/easy-rsa/2.0/keys/* /etc/openvpn/`

```
[root@vpn 2.0]# cp -rf /usr/share/doc/openvpn-2.1.4/easy-rsa/2.0/keys/* /etc/openvpn/
```

11. `cp /usr/share/doc/openvpn-2.1.4/sample-config-files/server.conf /etc/openvpn/`

```
[root@vpn 2.0]# cd /etc/openvpn/
```

```
[root@vpn openvpn]# cp /usr/share/doc/openvpn-2.1.4/sample-config-files/server.conf /etc/openvpn/
```

12. `server.conf` `cert`

`)`

```
# Any X509 key manateppagement system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert vpn.rmutl.ac.th.crt
key vpn.rmutl.ac.th.key # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
# openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
```

```
# 2048 bit keys.  
dh dh1024.pem
```

13. `openvpn` を起動する

```
[root@vpn openvpn]# service openvpn start  
Starting openvpn:  
OK ]  
[root@vpn openvpn]#
```

15. `Interface tun` を設定する

```
[root@vpn openvpn]# ifconfig  
eth0      Link encap:Ethernet  HWaddr C2:DE:48:D6:36:24  
inet addr:192.168.1.10  Bcast:10.0.1.255  Mask:255.255.255.0  
inet6 addr: fe80::c0de:48ff:fed6:3624/64  Scope:Link  
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
RX packets:76748 errors:0 dropped:0 overruns:0 frame:0  
TX packets:8380 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:6582338 (6.2 MiB)  TX bytes:997841 (974.4 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:8 errors:0 dropped:0 overruns:0 frame:0  
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:560 (560.0 b)  TX bytes:560 (560.0 b)  
  
tun0      Link          encap:UNSPEC          HWaddr  
00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  
inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255  
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
```



```
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

```
[root@vpn openvpn]#
```

16. 設定 UTP 1194 (iptables -F)

設定

1. openvpn client 設定 <http://openvpn.se/download.html> (openvpn-2.0.9-gui-1.0.3-install.exe 実行)

2. 設定

3. windows explorer で C:\Program Files\OpenVPN\sample-config

4. client.vpn を C:\Program Files\OpenVPN\config

5. client.crt , client.key と ca.crt を C:\Program Files\OpenVPN\config

6. C:\Program Files\OpenVPN\config\client.vpn を text editor で

```
.
.
.
```

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
```

```

remote 192.168.1.10 1194
10
;remote my-server-2 1194

.

.

.

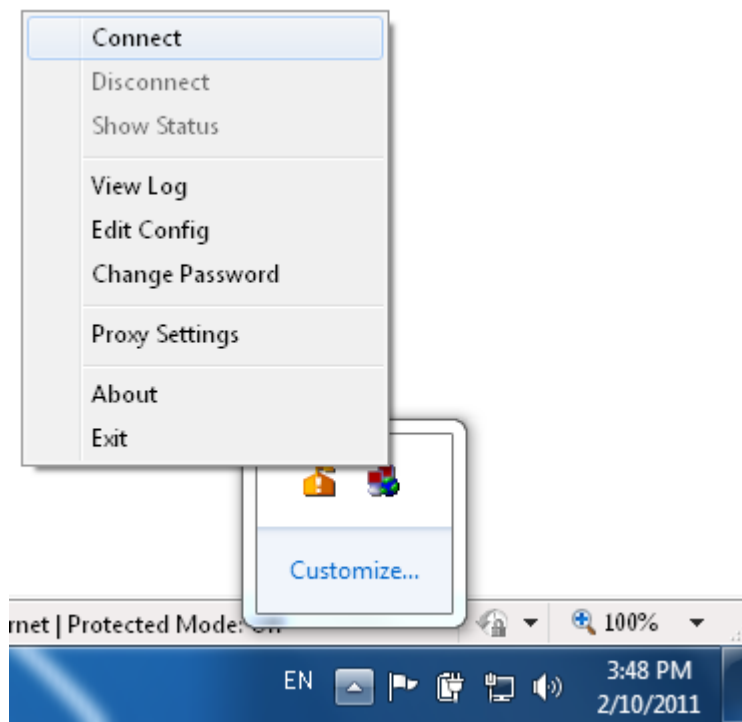
# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca ca.crt
cert client.crt
key client.key

```

server 3

7. system tray openvpn connect

8. openvpn



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d8e9:c148:f42:151b%23
    IPv4 Address. . . . . : 10.8.0.6
    Subnet Mask . . . . . : 255.255.255.252
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : rmutl.ac.th
    IPv4 Address. . . . . : 10.3.6.52
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.6.254

Tunnel adapter isatap.rmutl.ac.th:
```