Akuvox

OpenVPN Feature On Akuvox IP Phone

19/06/2015

Content

1. Overview

VPN（Virtual Private Network）is a private logical connection in public network. It uses virtual tunnel to implement data encryption、verification and user authentication ,which ensures the data not been falsified,replicated,snooped. Relating to the leased line, VPN works in Internet without the prohibitive costs. So it is possible to transmit the private data through Internet safely and economically for enterprises. VPN system includes VPN server, VPN client and virtual tunnel. A simply VPN system is shown in Fig.1.

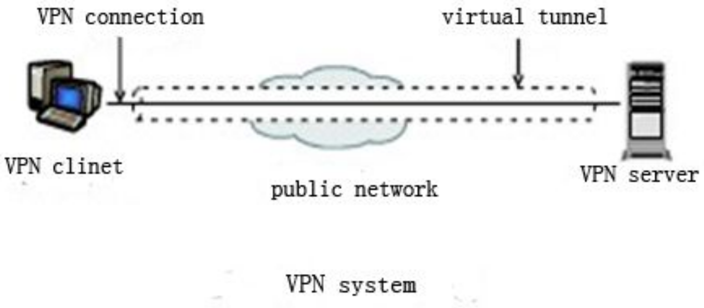


Fig.1

VPN is the equivalent to a bridge between internet and intranet. In IP telephone communication systems, VPN allows an IP phone from a public network to have secure remote access to a private network. For instance, a company's central private network which is not reachable publicly. The following topological graph shows a example of connecting an IP phone with a public address to a SIP PBX in company's intranet with the VPN server.

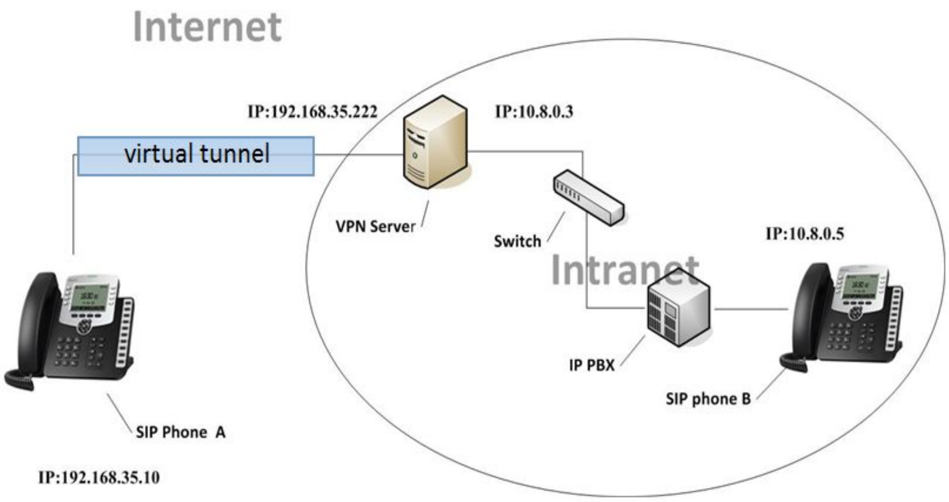


Fig.2

2. *OpenVPN*

OpenVPN is an open source third-party virtual private network configuration tool. It can be used for building VPN of Akuvox SIP Phone with inherent equipments and run in many operating systems.

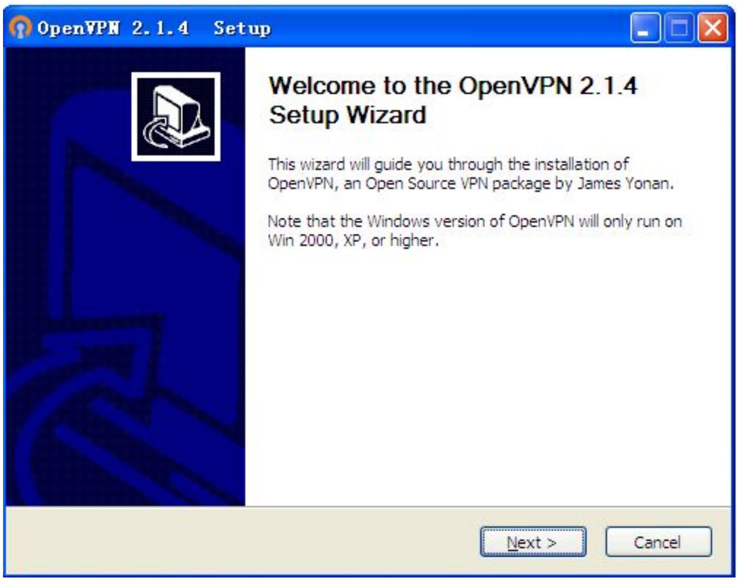
Note: SP-R50P does not support VPN currently.

Pre-requisites:

- OpenSSL

2.1 Install OpenVPN（Windows）

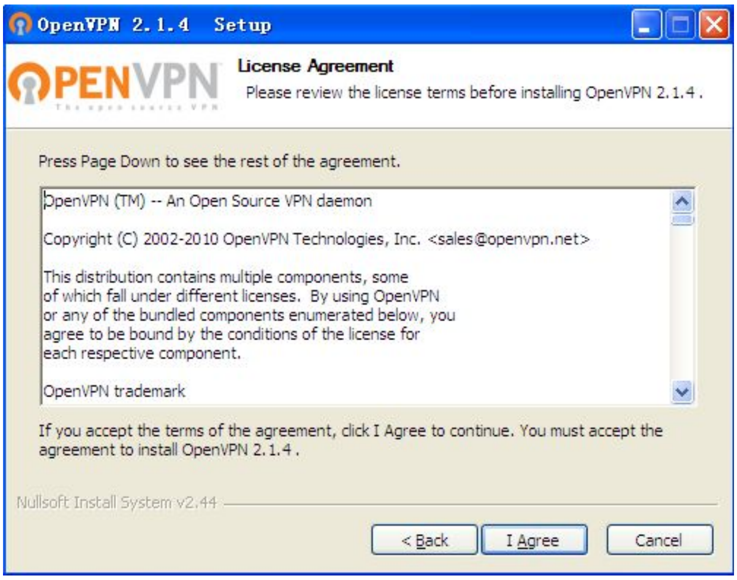
Download and install Open VPN(example: openvpn-2.1.4-install.exe). Please complete the following steps:



Welcome to the OpenVPN 2.1.4 Setup Wizard

This wizard will guide you through the installation of OpenVPN, an Open Source VPN package by James Yonan.

Note that the Windows version of OpenVPN will only run on Win 2000, XP, or higher.



License Agreement

Please review the license terms before installing OpenVPN 2.1.4 .

Press Page Down to see the rest of the agreement.

OpenVPN (TM) -- An Open Source VPN daemon

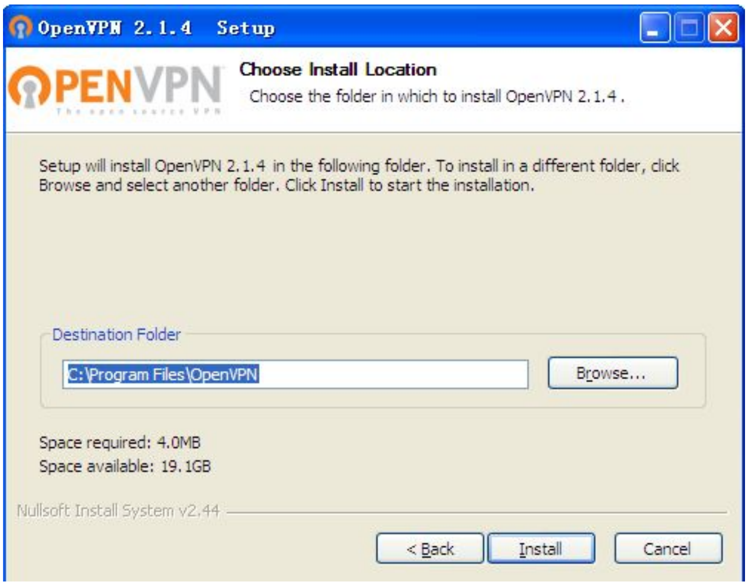
Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>

This distribution contains multiple components, some
of which fall under different licenses. By using OpenVPN
or any of the bundled components enumerated below, you
agree to be bound by the conditions of the license for
each respective component.

OpenVPN trademark

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenVPN 2.1.4 .

Nullsoft Install System v2.44



Choose Install Location

Choose the folder in which to install OpenVPN 2.1.4 .

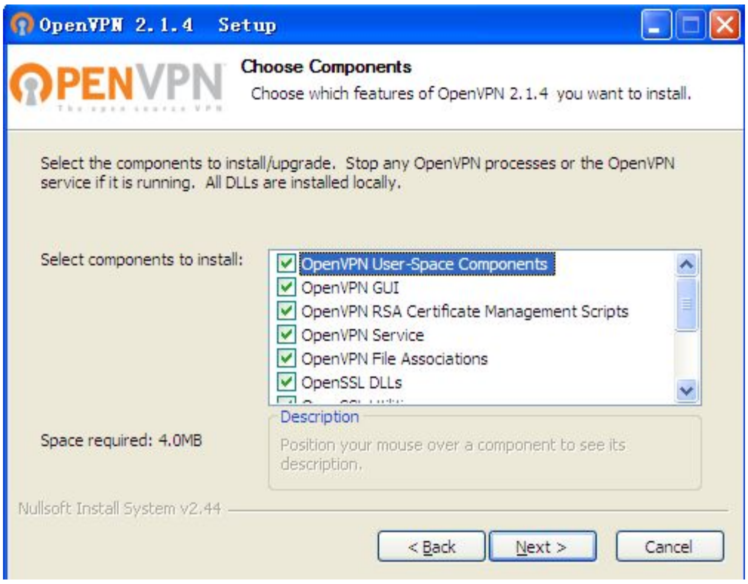
Setup will install OpenVPN 2.1.4 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files\OpenVPN

Space required: 4.0MB
Space available: 19.1GB

Nullsoft Install System v2.44



Choose Components

Choose which features of OpenVPN 2.1.4 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

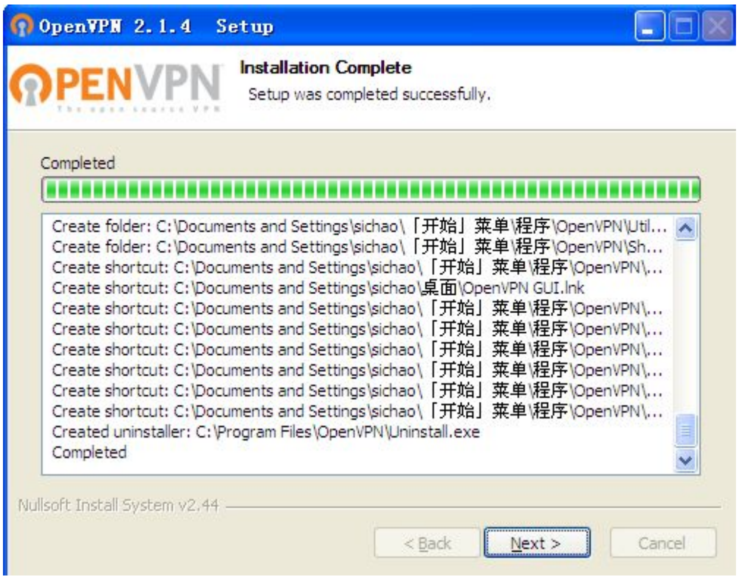
☑ OpenVPN User-Space Components
☑ OpenVPN GUI
☑ OpenVPN RSA Certificate Management Scripts
☑ OpenVPN Service
☑ OpenVPN File Associations
☑ OpenSSL DLLs

Space required: 4.0MB

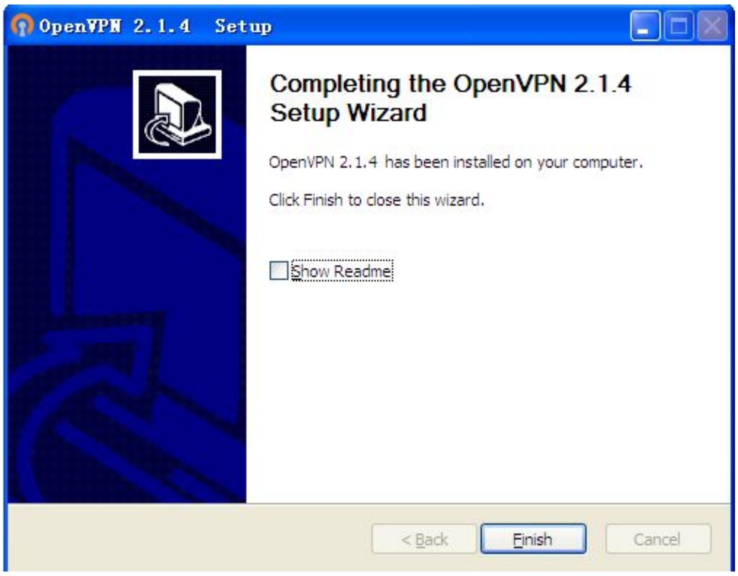
Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.44



```
Create folder: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\Util...
Create folder: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\Sh...
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Create shortcut: C:\Documents and Settings\sichao\桌面\OpenVPN GUI.lnk
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Create shortcut: C:\Documents and Settings\sichao\「开始」菜单\程序\OpenVPN\...
Created uninstaller: C:\Program Files\OpenVPN\Uninstall.exe
Completed
```



OpenVPN 2.1.4 has been installed on your computer.

Click Finish to close this wizard.

Installing is finished.

2.2 Create certification

2.2.1 Initial configuration：

1. Modify these details(as shown below) of **vars.bat.sample** in the folder named **easy-rsa**, then rename it **vars.bat** .

set KEY_COUNTRY=CN

set KEY_PROVINCE=FJ

set KEY_CITY=XM

set KEY_ORG=Akuvox

set KEY_EMAIL=support@akuvox.com

1.1 If install OpenVPN in other drives, it is necessary to modify the following details according to actual condition.

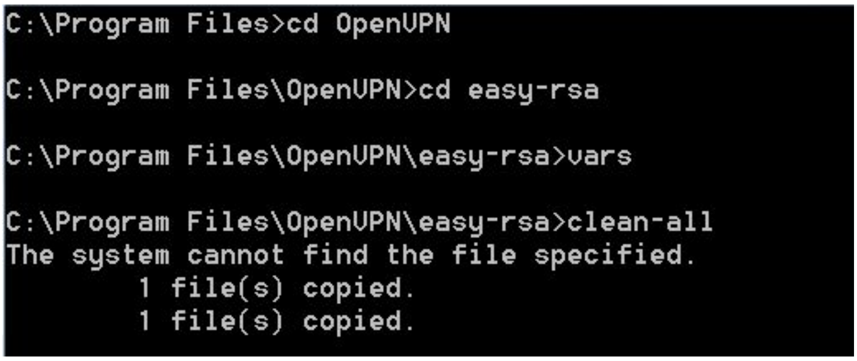
set HOME=E:\OpenVPN\easy-rsa
set KEY_DIR=E:\OpenVPN\easy-rsa
set KEY_DIR=E:\OpenVPN\easy-rsa\keys

2．Rename **openssl.cnf.sample** as **openssl.cnf** .Then open CMD to input these commands(as shown below).

C:\Documents and Settings\ThinkPad>cd "\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all



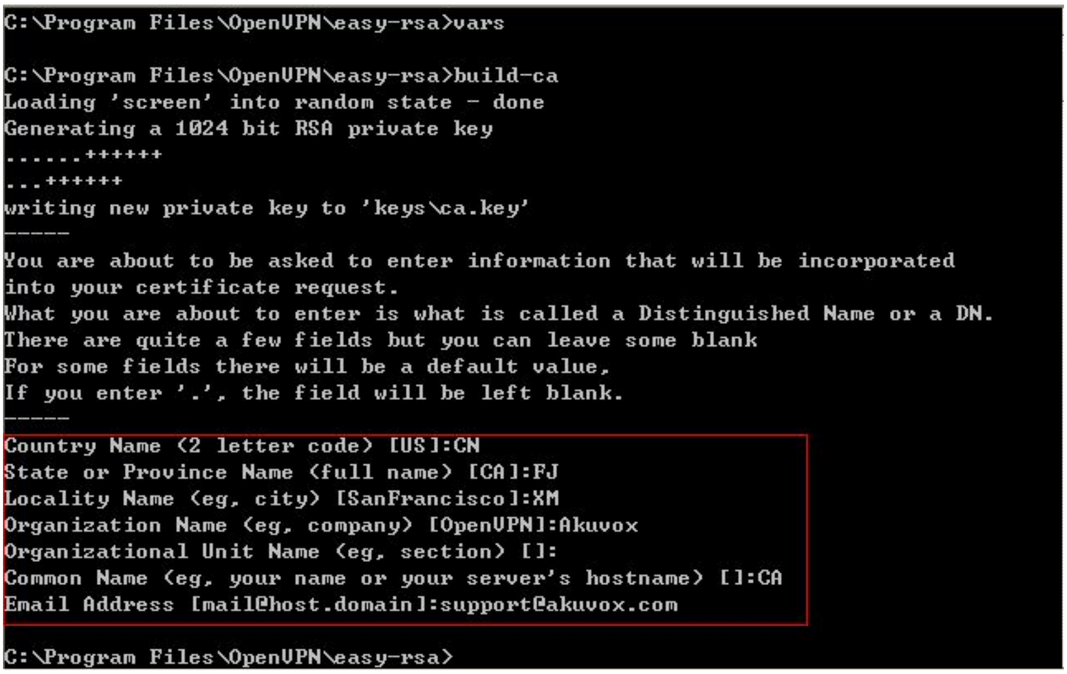
```
C:\Program Files>cd OpenVPN

C:\Program Files\OpenVPN>cd easy-rsa

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
The system cannot find the file specified.
        1 file(s) copied.
        1 file(s) copied.
```

2.2.2 Create Root CA：

Input these commands (as shown below)into CMD:

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>build-ca

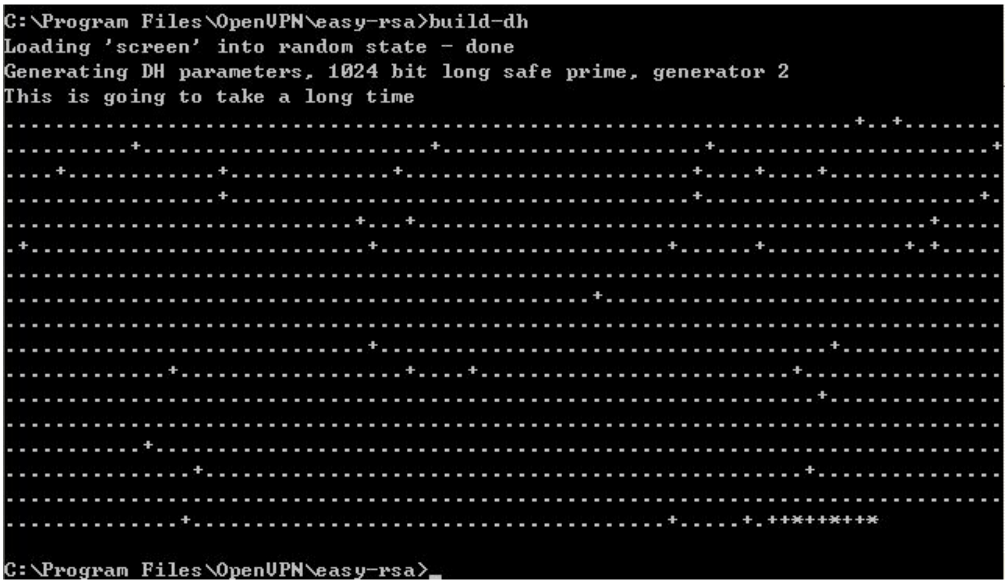


```
C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>build-ca
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......++++++
...++++++
writing new private key to 'keys\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) [US]:CN
State or Province Name (full name) [CA]:FJ
Locality Name (eg, city) [SanFrancisco]:XM
Organization Name (eg, company) [OpenVPN]:Akuvox
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:CA
Email Address [mail@host.domain]:support@akuvox.com

C:\Program Files\OpenVPN\easy-rsa>
```

2.2.3 Create dh1024.pem file

Input these commands (as shown below)into CMD:

C:\Program Files\OpenVPN\easy-rsa>build-dh

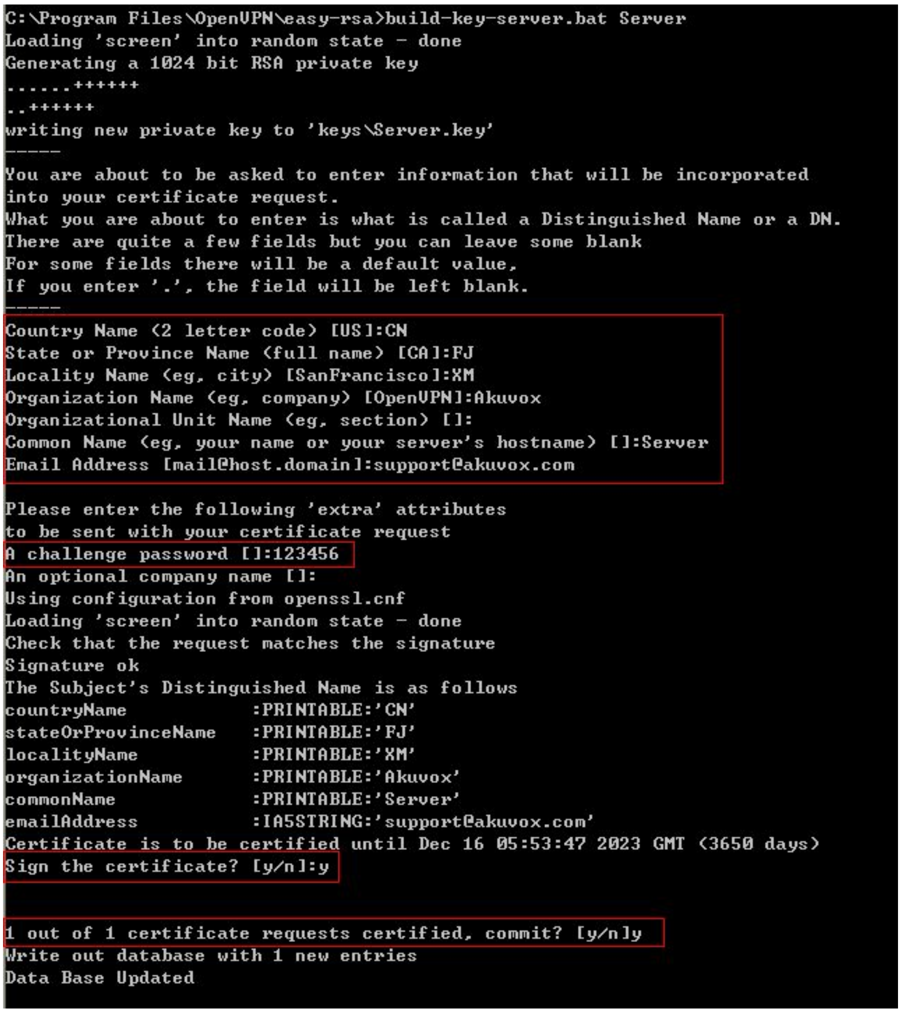


```
C:\Program Files\OpenVPN\easy-rsa>build-dh
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
....................................................................+..+........
..........+.......................+.....................+......................+
....+............+.............+.......................+....+....+..............
.................+.....................................+......................+.
............................+...+.........................................+.....
.+...........................+.......................+......+...........+.+.....
................................................................................
...............................................+................................
................................................................................
.............................+....................................+.............
.............+..................+....+.........................+................
.................................................................+..............
................................................................................
...........+....................................................................
...............+................................................+...............
................................................................................
..............+......................................+.....+.++*++*++*

C:\Program Files\OpenVPN\easy-rsa>_
```

2.2.4 Create certification of server

Input these commands (as shown below)into CMD:

C:\Program Files\OpenVPN\easy-rsa>build-key-server CdtsmServer



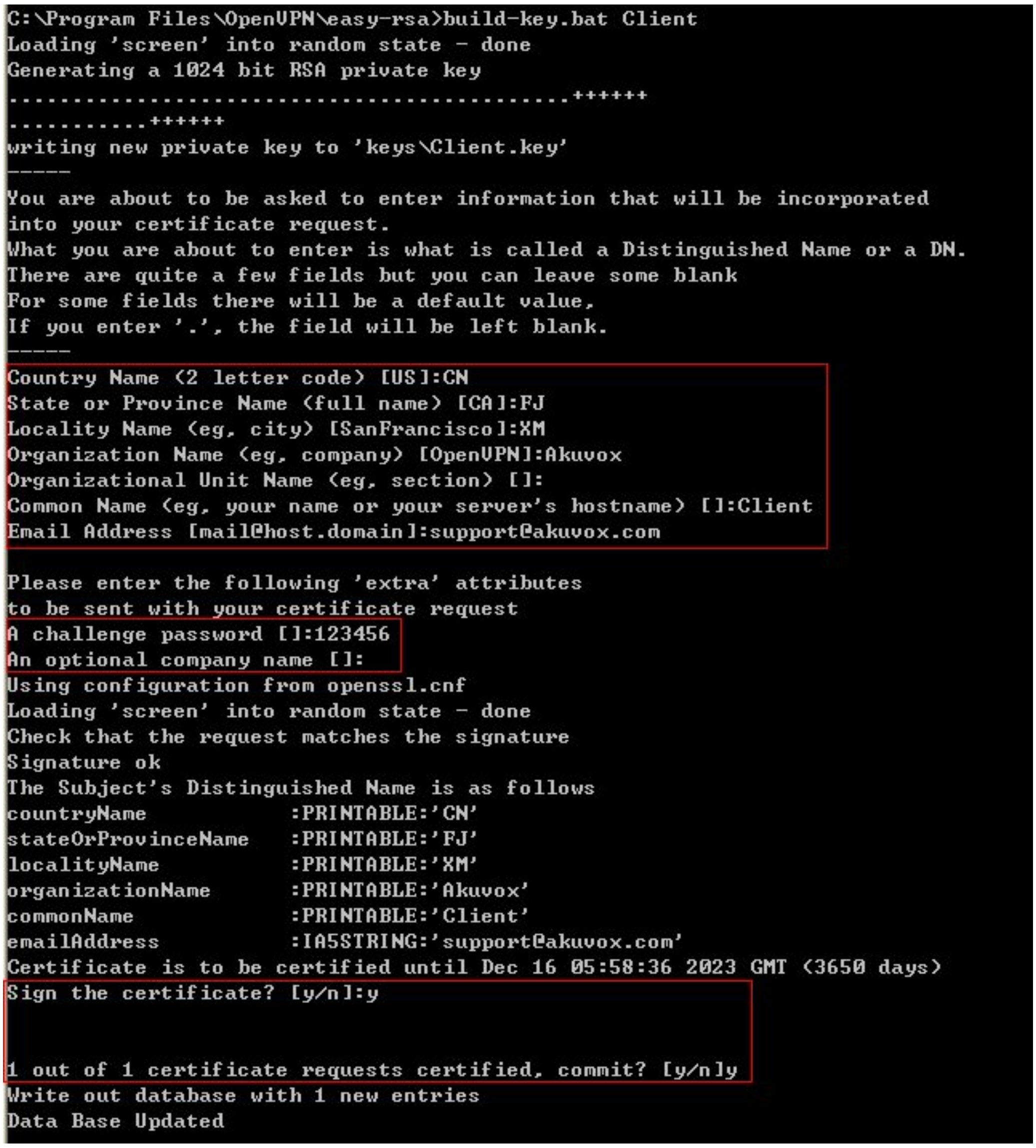
```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat Server
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......++++++
..++++++
writing new private key to 'keys\Server.key'
-----
You are about to be asked to enter information that will be incorporated
into your 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) [US]:CN
State or Province Name (full name) [CA]:FJ
Locality Name (eg, city) [SanFrancisco]:XM
Organization Name (eg, company) [OpenVPN]:Akuvox
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Server
Email Address [mail@host.domain]:support@akuvox.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'FJ'
localityName          :PRINTABLE:'XM'
organizationName      :PRINTABLE:'Akuvox'
commonName            :PRINTABLE:'Server'
emailAddress          :IA5STRING:'support@akuvox.com'
Certificate is to be certified until Dec 16 05:53:47 2023 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
```

The certification of server is finished.

2.2.5 Create certification of client

Input these commands (as shown below)into CMD:

C:\Program Files\OpenVPN\easy-rsa>build-key Client



```
C:\Program Files\OpenVPN\easy-rsa>build-key.bat Client
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
............................................++++++
...........++++++
writing new private key to 'keys\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) [US]:CN
State or Province Name (full name) [CA]:FJ
Locality Name (eg, city) [SanFrancisco]:XM
Organization Name (eg, company) [OpenVPN]:Akuvox
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Client
Email Address [mail@host.domain]:support@akuvox.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'FJ'
localityName          :PRINTABLE:'XM'
organizationName      :PRINTABLE:'Akuvox'
commonName            :PRINTABLE:'Client'
emailAddress          :IA5STRING:'support@akuvox.com'
Certificate is to be certified until Dec 16 05:58:36 2023 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
```

The certification of client is finished.

2.3 Configuration file

2.3.1 Configuration of server

Go to the path: **C:\Program Files\OpenVPN\sample-config** . Open **server.ovpn** and modify these details as shown in blue.

Note: Comments are preceded with '#' or ';' . This config should work on Windows or Linux/BSD systems. Remember on Windows to quote pathnames and use double backslashes.(e.g.:"C:\\Program Files\\OpenVPN\\config\\foo.key")

```
#################################################

 # Which local IP address should OpenVPN
 # listen on? (optional)
 ;local a.b.c.d

 # Which TCP/UDP port should OpenVPN listen on?
 # If you want to run multiple OpenVPN instances
 # on the same machine, use a different port
 # number for each one.  You will need to
 # open up this port on your firewall.
 # the default port 1194
 port 1194

 # TCP or UDP server?
 #Uncomment the line to enable TCP or UDP
 ;proto tcp
 proto udp

 # "dev tun" will create a routed IP tunnel,
 # "dev tap" will create an ethernet tunnel.
 # Use "dev tap0" if you are ethernet bridging
 # and have precreated a tap0 virtual interface
 # and bridged it with your ethernet interface.
 # If you want to control access policies
 # over the VPN, you must create firewall
 # rules for the the TUN/TAP interface.
 # On non-Windows systems, you can give
 # an explicit unit number, such as tun0.
 # On Windows, use "dev-node" for this.
 # On most systems, the VPN will not function
 # unless you partially or fully disable
 # the firewall for the TUN/TAP interface.
 #Typically, dev tap is used if VPN server is
 # running on windows
 #tap is for Windows and tun is for Linux
 dev tap
 ;dev tun

 # Windows needs the TAP-Win32 adapter name
 # from the Network Connections panel if you
 # have more than one.  On XP SP2 or higher,
 # you may need to selectively disable the
 # Windows firewall for the TAP adapter.
 # Non-Windows systems usually don't need this.
 ;dev-node MyTap

 # SSL/TLS root certificate (ca), certificate
 # (cert), and private key (key).  Each client
 # and the server must have their own cert and
 # key file.  The server and all clients will
 # use the same ca file.
 #
 # See the "easy-rsa" directory for a series
 # of scripts for generating RSA certificates
 # and private keys.  Remember to use
 # a unique Common Name for the server
 # and each of the client certificates.
 #
 # Any X509 key management system can be used.
 # OpenVPN can also use a PKCS #12 formatted key file
 # (see "pkcs12" directive in main page).
 #Please be sure the filename
```

```
#ROOT CA is generated by build-ca, and it is used to verify the legality of customer certification.
ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
#The certificate file of server
cert "C:\\Program Files\\OpenVPN\\config\\Cdtsmserver.crt"
#The key of certificate file.
key "C:\\Program Files\\OpenVPN\\config\\Cdtsmserver.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

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
#Launch VPN server on TAP/TUN interface with Specific IP address and net mask
;server 192.168.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt
```

```
# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
#If users want to launch the VPN server on bridge
server-bridge 10.8.0.2 255.255.255.0 10.8.0.50 10.8.0.100

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
```

```
;push "route 192.168.35.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"



# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
client-config-dir ccd
;route 192.168.40.128 255.255.255.248

# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2
# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 10.10.22.243"
;push "dhcp-option WINS 202.106.0.20"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.
duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
#( Openvpn can not connect again in mode server )
# The value can be modified by users.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key

# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
#We use DES-CBC as an example.
;cipher BF-CBC
;cipher AES-128-CBC
;cipher DES-EDE3-CBC
cipher DES-CBC



# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
;comp-lzo no

# The maximum number of concurrently connected
# clients we want to allow.
# The value can be modified by users.
max-clients 20

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
```

```
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nobody

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
#The value can be modified by users
verb 4

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

2.3.2 Connect to OpenVPN Server

Set Bridge Connections between Local Area Connection and the external network adapter . Then, setup IP address on Bridge interface.(Please be same as server-bridge IP in **server.ovpn**)

Copy **server.ovpn** of **C:\Program Files\OpenVPN\sample-config** and **ca.crt**、**ca.key**、**CdtsmServer.crt**、**CdtsmServer.csr**、**CdtsmServer.key**、**dh1024.pem** of **C:\Program Files\OpenVPN\easy-rsa\key** to **C:\Program Files\OpenVPN\config**. The configuration of server is finished. Then double click OpenVPN GUI to enable the server.

Click in the taskbar to connect to the server. As shown in Fig. 3.

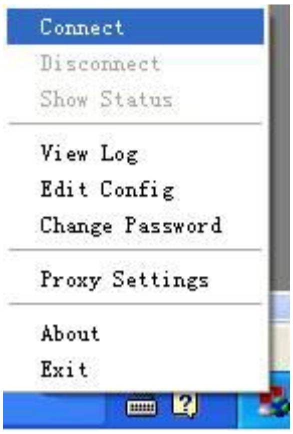
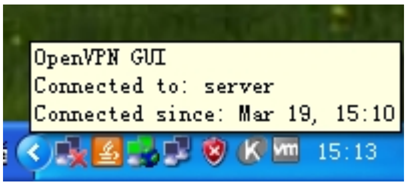


Fig.3

The icon will turn green after connecting successfully as shown in Fig.4.



OpenVPN GUI
Connected to: server
Connected since: Mar 19, 15:10

Fig.4

2.3.3 Configuration of client

Go to the path: **C:\Program Files\OpenVPN\sample-config**. Open **client.ovpn** and modify these details as shown in blue.

```
################################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.         #
#                                                #
# This configuration can be used by multiple #
# clients, however each client should have      #
# its own cert and key files.                    #
#                                                #
# On Windows, you might want to rename this    #
# file so it has a .ovpn extension                #
################################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
 #we use Tap as an example
dev tap
;dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.    On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap
```

```
# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
#Please be same as the server‘s protocol.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
#Outer network ip of OpenVPN
 remote 192.168.35.91 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody
```

```
# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.   See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.   Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# 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.
#Please be sure the file name
ca /config/openvpn/ca.crt
cert /config/openvpn/Client.crt
key /config/openvpn/Client.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".   This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".    The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x
# we use DES-CBC as an example
cipher DES-CBC

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
;comp-lzo no

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

2.3.4 Create client.tar file

Please complete the following steps:

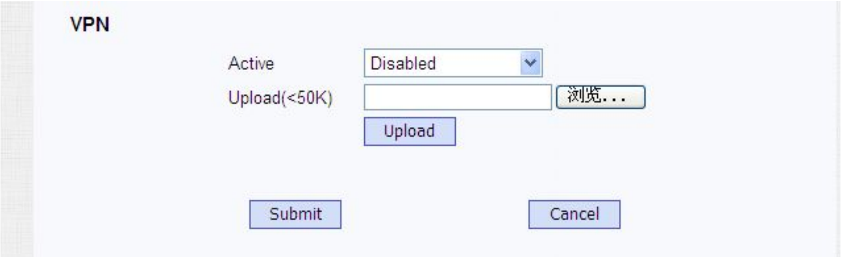
1. Copy **client.ovpn** of **C:\Program Files\OpenVPN\sample-config** and **Client.crt**、**Client.key**、**ca.crt** of **C:\Program Files\OpenVPN\easy-rsa\keys** to **client**.
2. Rename **client.ovpn** as **vpn.conf** .
3. Then select **vpn.conf**、**Client.crt**、**Client.key**、**ca.crt** at the same time.
4. Use compression software(example:7-Zip) to compress them into **client.tar** directly.

Note: Do not rename the format from **zip** or **rar** directly .

3. SIP Phone VPN

3.1 Configuration on web

Go to the path: Network->Advanced .Upload client.tar before enabling VPN, then click submit. SIP Phone will reboot.



VPN

Active: Disabled

Upload(<50K): 浏览...

Upload

Submit Cancel

3.2 Configuration on IP Phone

Go to the path: Menu->Settings->Advanced setting->Network->VPN. Upload **client.tar** in web before enable/disable VPN. SIP Phone will reboot.

After connecting VPN server successfully, the icon V (as shown in Fig.5) will show.

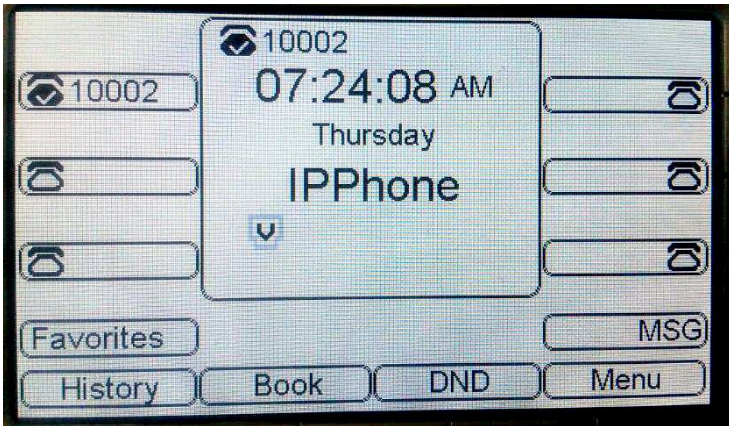


Fig.5