Openvpn Using and production of certificates

Version: 1.0
Release date: 2013-12-27

This document contains information that is proprietary to Fanvil Co., Ltd (Abbreviated as Fanvil hereafter). Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Specifications are subject to change without notice.

Liability Disclaimer

Fanvil may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked as reserved or undefined. Fanvil reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Fanvil sales office or your distributor to obtain the latest specification and before placing your product order.

Table of Contents

1 Introduction

1.1 Overview

A virtual private network (VPN) extends a private network across a public network. It is different from other network connections.It uses a proprietary tunneling protocol，implements data encryption 、integrity testing and user authentication. This ensuring that information cannot be peep、tampered and replicated. From the perspective of network connection security，it is similar to proprietary network. But it is logical private network instead of physical one, which let it be called virtual private network. VPN system including : VPN server，VPN client and Tunnel. As transmission through the internet is more economical than leased lines, it becomes a good choice for companies which want to transfer confidential information economic securely through the internet.

What will we introduce? Configuring VPN with OpenVPN on Windows OS. OpenVPN is an open source third party VPN configuration tool. It can build application Gateway with inherent devices.

The phones support OpenVPN are as follow：

- ◆ Fanvil C58/C60/C62/F66
- ◆ Fanvil E01/E52/E58/ E 62/E66
- ◆ Fanvil F01/F52/F58/ F 62/F66

1.2 Target Audience

This file is for customer and the ones who need to test the OpenVPN protocol.

2 Server Installation and Download

Windows version of OpenVPN software can be searched from internet and downloaded.The software can be installed by default, and the default path is “C:\Program Files\OpenVPN”。

3 Server Configuration

TheVPN server uses RSA Certificate and key authentication to verify the client. The client certificate matches the phone. When multiple phones use the same certificate，only one can connect to the server Successfully. So the first work is making certificate.

3.1 Initialization

Before the operating, we should do the Initialization.

Modify the statement in the file (C:\Program Files\OPENVPN\easy-rsa\vars.bat.sample):

```
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=FortFunston
set KEY_EMAIL=mail@domain.com
```

make the statement above become the statement follow

```
set HOME=C:\Program Files\OPENVPN\easy-rsa
set KEY_COUNTRY=CN                      #(country)
set KEY_PROVINCE=BEIJING                #(province)
set KEY_CITY= BEIJING                   #(city)
set KEY_ORG=WINLINE                     #( Organization)
set KEY_EMAIL=admin@winline.com.cn              #(email address)
```

The word after the “#” is explanation, please do not write to the file.

Then through the command line(Start->Run->enter cmd, Enter the DOS interface)：

Go into the “openvpn\easy-rsa”。

enter：

```
init-config
vars
clean-all
```

NOTE：The above content is initialization.When you make certificate later, you should initialize again. But the only thing you should do is enter the command ,vars, In the directory(openvpn\easy-rsa) in the DOS interface.

3.2 Making certificate

Command is as follows：

Make the root certificate：

Enter build-ca,

Country Name (2 letter code) [CN]:)（You cannot enter）

State or Province Name (full name) [BEIJING]: （You cannot enter）

Locality Name (eg, city) [BEIJING]: （You cannot enter）

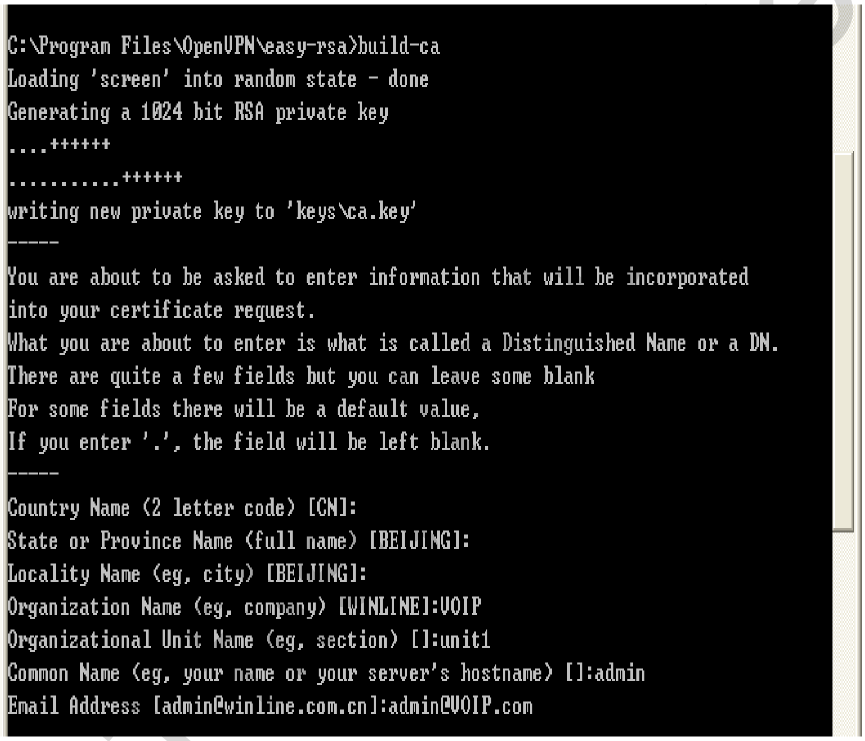
Organization Name (eg, company) [WINLINE]:（enter according to custom）

Organizational Unit Name (eg, section) []:unit1 #(Any input)

Common Name (eg, your name or your server's hostname) []:admin #(Any input)

Email Address [admin@winline.com.cn]:（Generally enter :Common Name@ Organization Name.com）

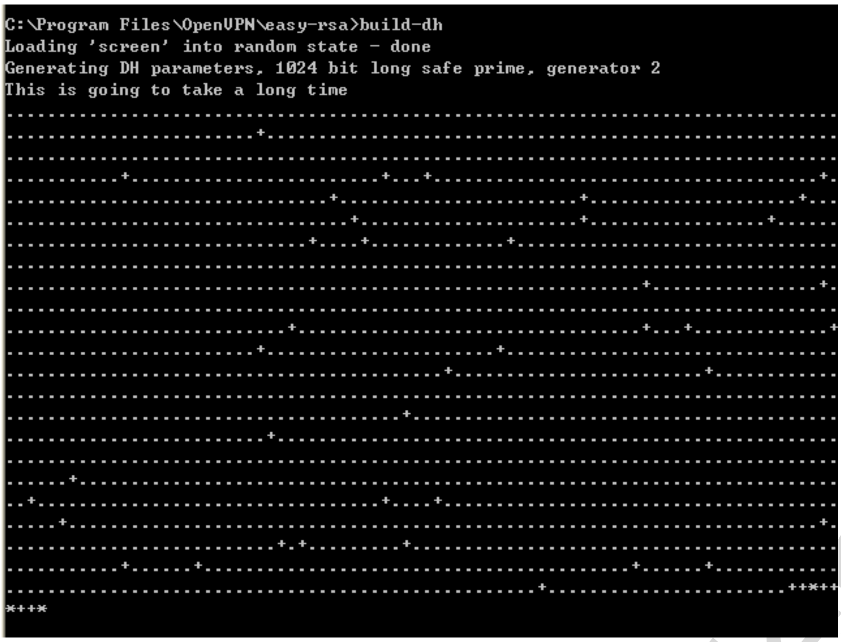
As follow：



```
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) [CN]:
State or Province Name (full name) [BEIJING]:
Locality Name (eg, city) [BEIJING]:
Organization Name (eg, company) [WINLINE]:VOIP
Organizational Unit Name (eg, section) []:unit1
Common Name (eg, your name or your server's hostname) []:admin
Email Address [admin@winline.com.cn]:admin@VOIP.com
```

Enter build-dh ，

This step need a long time ,you should be patience。As follows：



```
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
................................................................................
........................+.......................................................
................................................................................
...........+........................+...+.....................................+.
...............................+.......................+....................+...
.................................+.....................+.................+......
.............................+....+.............+...............................
................................................................................
.............................................................+................+.
................................................................................
...........................+.................................+...+.............+
........................+......................+................................
..........................................+........................+............
................................................................................
......................................+.........................................
.........................+......................................................
................................................................................
......+.........................................................................
..+.................................+....+......................................
.....+........................................................................+.
..........................+.+.........+.........................................
...........+......+.........................................+......+............
...................................................+.......................++*++
*++*
```

Build server key ：

Enter build-key-server server , （build-key-server is required，server is entered freely，but server is my suggestion）

You will find the information as follows：

Country Name (2 letter code) [CN]: #(the same as the root certificate)

State or Province Name (full name) [BEIJING]: #(the same as the root certificate)

Locality Name (eg, city) [BEIJING]: #(this can be modified)

Organization Name (eg, company) [WINLINE]: #(the same as the root certificate)

Organizational Unit Name (eg, section) []:unit1 #(entered freely)

Common Name (eg, your name or your server's hostname) []:adminServer #(entered freely)

Email Address [admin@winline.com.cn]: #(this can be modified)

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

A challenge password []:adminServer #(entered freely)

An optional company name []:winline #(entered freely)

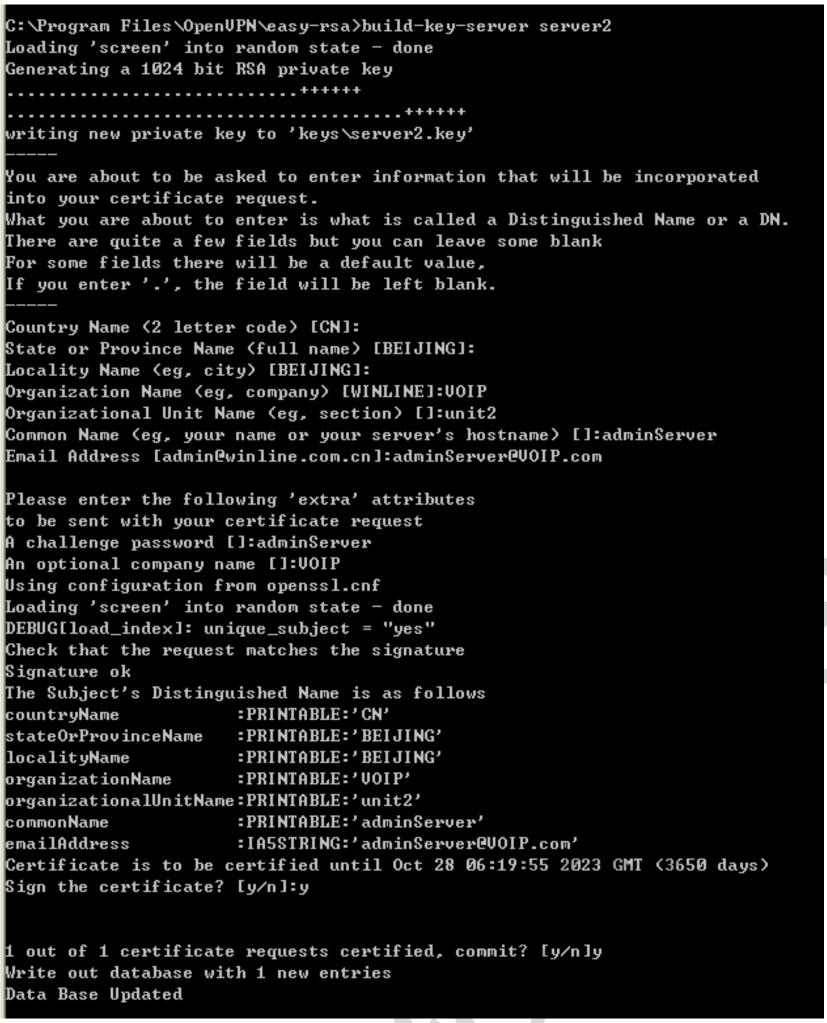
Certificate is to be certified until Nov 24 06:24:34 2018 GMT (3650 days)

Sign the certificate? [y/n]:y #(“y” means yes ,choose “y”)

1 out of 1 certificate requests certified, commit? [y/n]y #(“y” means yes ,choose “y”)

The produced key is in the directory,openvpn\easy-rsa\keys

As follows：



```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server2
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.............................++++++
........................................++++++
writing new private key to 'keys\server2.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) [CN]:
State or Province Name (full name) [BEIJING]:
Locality Name (eg, city) [BEIJING]:
Organization Name (eg, company) [WINLINE]:VOIP
Organizational Unit Name (eg, section) []:unit2
Common Name (eg, your name or your server's hostname) []:adminServer
Email Address [admin@winline.com.cn]:adminServer@VOIP.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:adminServer
An optional company name []:VOIP
Using configuration from openssl.cnf
Loading 'screen' into random state - done
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'BEIJING'
localityName          :PRINTABLE:'BEIJING'
organizationName      :PRINTABLE:'VOIP'
organizationalUnitName:PRINTABLE:'unit2'
commonName            :PRINTABLE:'adminServer'
emailAddress          :IA5STRING:'adminServer@VOIP.com'
Certificate is to be certified until Oct 28 06:19:55 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
```

Build client key：

Enter build-key client

You will find following information：

Country Name (2 letter code) [CN]: #(the same as the root certificate)

State or Province Name (full name) [BEIJING]: #(the same as the root certificate)

Locality Name (eg, city) [BEIJING]: #(this can be modified)

Organization Name (eg, company) [WINLINE]: #(the same as the root certificate)

Organizational Unit Name (eg, section) []:unit1 #(entered freely)

Common Name (eg, your name or your server's hostname) []:client1

＃(entered freely. For the different client ,you should use different name. If use the same name ,you should make a new client key for a client.)

Email Address [admin@winline.com.cn]: #(this can be modified)

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

A challenge password []:client1 #(entered freely)

An optional company name []:winline #(entered freely)

```
Certificate is to be certified until Nov 24 06:39:28 2018 GMT (3650 days)
Sign the certificate? [y/n]:y                                   #("y" means yes ,choose "y")
1 out of 1 certificate requests certified, commit? [y/n]y        #("y" means yes ,choose "y")
```

The produced key is in the directory,openvpn\easy-rsa\keys.

3.3 Server Settings

After Making a new directory in the path , C:\Program Files\OpenVPN\，you should copy the produced ca.crt,dh1024.pem,server.crt,server.key to the directory. The four is the required files for the server running.

Make file named server.ovpn in the path \OpenVPN\KEY\. You could make a txt suffix file，write contents into the file ,then save it as server.ovpn.

Server-side file example：(server.ovpn)

```
port 1194                     ＃This port is the specified port assigned by IANA for OpenVPN. But you
    can modify as needed.
    proto udp                           ＃You   also can use TCP yet
    dev tun
    ca ca.crt
    cert server.crt
    key server.key
    dh dh1024.pem
    server 10.8.0.0 255.255.255.0             ＃Virtual LAN Settings，you can modify as needed
    ifconfig-pool-persist ipp.txt
    keepalive 10 120
    client-to-client
    comp-lzo
    max-clients 100
    persist-key
    persist-tun
    status openvpn-status.log
    verb 3
```

Start the server：

Right-click on server.ovpn，choose start openvpn on this config file.

3.4 Client Settings

The client refers to the equipment supporting the OpneVPN. In order to connect to the OpenVPN server, the phone need to be upgraded the client certificate on the page，SECURITY->VPN. Making a folder named cert in the C:\Program Files\ OpenVPN，we can put all the client certificate in the floder.The certificate includes ca.crt, client.crt, client.key in the directory openvpn\easy\rsa\keys\. Then we can make a client file and the method is same as the server client .

Client-side file example：(client.ovpn)

```
client
dev tun
proto udp
remote 192.168.1.135 1194                                        #server domain/IP   and port
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
comp-lzo
verb 3
```

So far, the server and a client certificate are completed. They can be Verified by the 4.1 and 4.2.

3.5 Making the second client certificate

One server could certificate could match many client certificate，but one client certificate cannot be used by multiple phone at the same time. We must make other certificate for the other client.So, each phone can get different OpenVPN IP by different client certificate.

步骤：

```
C:\Documents and Settings\Administrator>cd C:\Program Files\OpenVPN\easy-rsa #go into the directory
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key client                          #build client key
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) [CN]:
State or Province Name (full name) [BEIJING]:
Locality Name (eg, city) [BEIJING]:
Organization Name (eg, company) [WINLINE]:
Organizational Unit Name (eg, section) []:unit1
Common Name (eg, your name or your server's hostname) []:client2    #client name ， different from client1
Email Address [admin@fanvil.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:client2
An optional company name []:winline
Using configuration from openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'BEIJING'
localityName          :PRINTABLE:'BEIJING'
organizationName      :PRINTABLE:'WINLINE'
organizationalUnitName:PRINTABLE:'unit1'
commonName            :PRINTABLE:'client2'
emailAddress          :IA5STRING:'admin@winline.com'
Certificate is to be certified until Dec 17 02:58:20 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
```

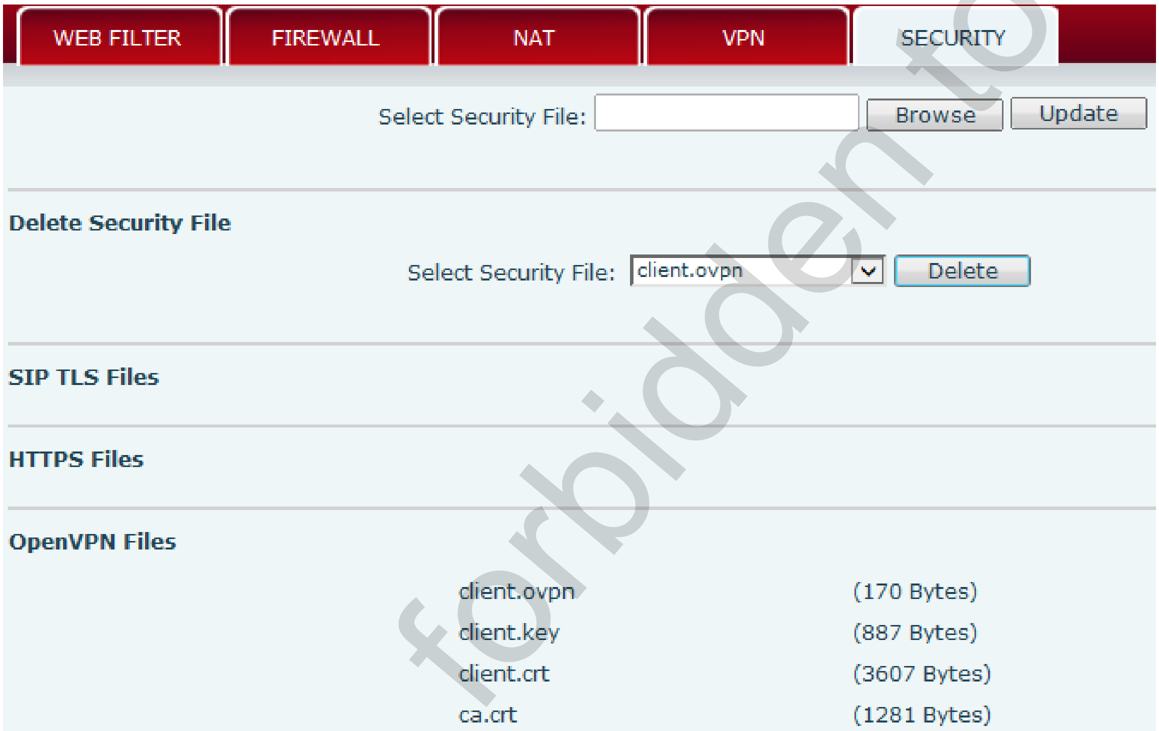
The remaining steps are same as 3.4.

4 OpenVPN for phone

证书制作完成后，我们需要验证制作的证书是否能够使话机连接上服务器，正常获得 OpenVPN IP。

4.1 Import the certificate

Logon WEB，as the path SECUTITY-SECURITY-Update Security File，click Browse，update client.ovpn, client.key, client.crt, ca.crt one by one.



Select Security File:

Delete Security File

Select Security File: client.ovpn

SIP TLS Files

HTTPS Files

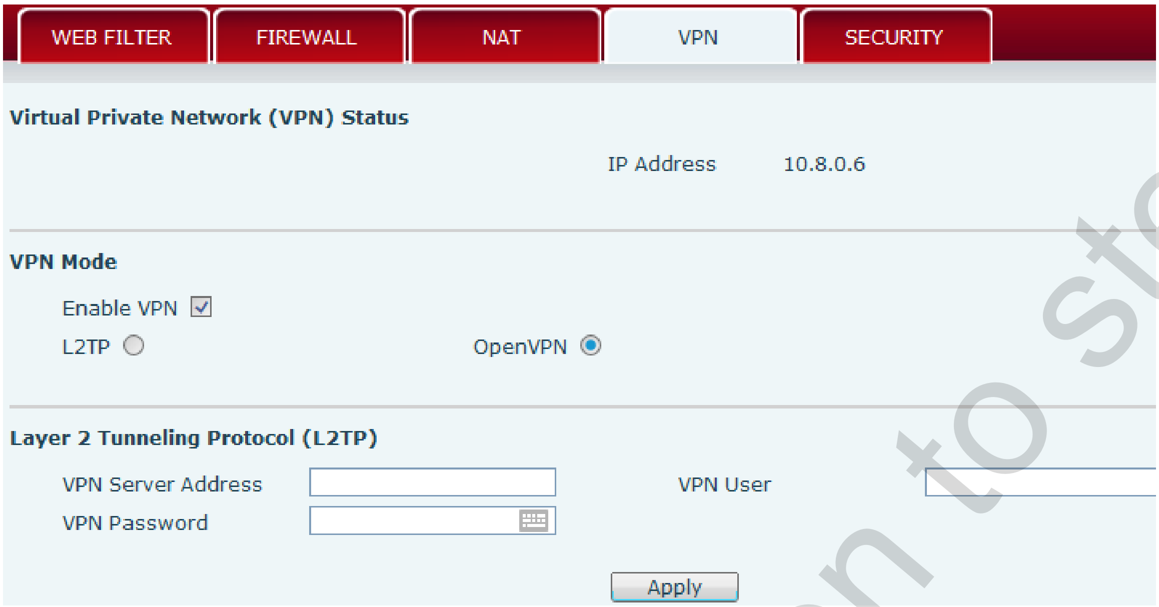
OpenVPN Files

client.ovpn	(170 Bytes)
client.key	(887 Bytes)
client.crt	(3607 Bytes)
ca.crt	(1281 Bytes)

After update ,there are the upadted certificate in the OpenVPN and Delete Security File drop-down box.

4.2 Enable OpenVPN

Open VPN page ,choose OpenVPN，check Enable VPN and click apply. When the phone connect to the server successfully, the VPN IP will be displayed. As shown in Figure,the received VPN IP is 10.8.0.6.



Virtual Private Network (VPN) Status

IP Address 10.8.0.6

VPN Mode

Enable VPN ☑

L2TP ○ OpenVPN ●

Layer 2 Tunneling Protocol (L2TP)

VPN Server Address VPN User

VPN Password