OpenVPN Usage and Certificate Generation Instructions

Version: <2.0>
Release date: <2020-03-30>

Contents

1 Introduction to OpenVPN

1.1 Overview

A virtual private network (VPN) is a secure network established in the public network. Different from conventional networks, the VPN implements data encryption, integrity check, and user identity authentication over a proprietary tunneling protocol, so as to protect information from being disclosed, tampered, and copied during transmission. From the perspective of network connection security, the VPN is similar to a private wire network established in the public network. The only difference is that the VPN is a logical network rather than a physical network. The VPN system consists of a VPN server, a VPN client, and a tunnel. Internet transmission is extremely inexpensive compared to leased line transmission. Therefore, the VPN makes it possible for enterprises to transmit private and confidential information securely and economically over the Internet.

This document describes how to configure the VPN on Windows by using OpenVPN. OpenVPN is an open-source third-party VPN configuration tool that can build a VPN application gateway by using the inherent equipment.

2 Server Installation and Configuration

OpenVPN is an open-source third-party VPN configuration tool that can build a VPN application gateway by using the inherent equipment. This chapter describes how to deploy and configure servers on Ubuntu and Windows.

2.1 Deploying the OpenVPN Server on Ubuntu

2.1.1 Installing the OpenVPN Server

Enter the following commands on Ubuntu:

```
sudo apt-get -y install openvpn libssl-dev openssl
sudo apt-get -y install easy-rsa
```

2.1.2 Generating Certificates

To generate certificates required for OpenVPN, perform the following steps:

Run the following commands to perform initial configuration:

```
sudo mkdir /etc/openvpn/easy-rsa/
sudo cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
sudo su
sudo vi /etc/openvpn/easy-rsa/vars
```

-----> Modify certificate configurations as follows:

```
        export KEY_COUNTRY="CN"
        export KEY_PROVINCE="BJ"
        export KEY_CITY="BeiJing"
        export KEY_ORG="fanvil"
        export KEY_EMAIL="fanvil@fanvil.com"
        export KEY_OU="fanvil"
        export KEY_NAME="server"
```

Run the vars command:	source vars
Clear all data if this is the first time to run OpenVPN:	./clean-all
Generate a CA certificate:	./build-ca
Generate a server certificate:	./build-key-server server
Generate a client certificate:	./build-key client
Build a dynamic password library:	./build-dh

2.2 Starting the Server

Configure the server environment, and save the certificate configuration files in the specified directory:

```
cp keys/ca.crt /etc/openvpn/
cp keys/server.crt   keys/server.key keys/dh2048.pem /etc/openvpn
mv /etc/openvpn/dh2048.pem /etc/openvpn/dh1024.pem
cp keys/client.key keys/client.crt   /etc/openvpn/
cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
cd /etc/openvpn
gzip -d server.conf.gz
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf   /etc/openvpn/
```

Start the server:

```
/etc/init.d/openvpn restart
```

2.3 Deploying the OpenVPN Server on Windows

2.3.1 Installing the OpenVPN Server

Download the OpenVPN software for Windows from the Internet. This document uses the software available at openVPN GUI.

Double-click the software to download and install it. Select **easy-rsa** during the installation. The default path is C:\Program Files\OpenVPN.

2.3.2 Generating Certificates

Before generating certificates, perform initialization.

Modify the following configurations in **vars.bat.sample** under C:\Program Files\OPENVPN\easy-rsa as required:

```
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 characters marked with # are comments. Do not write them into the file.

Run **cmd** as an administrator to enter DOS, and run the following commands:

In the openvpn\easy-rsa directory:

```
init-config
```

vars

clean-all

Generate a root certificate:	build-ca (Press **Enter** repeatedly to retain default settings.)
Build a dynamic password library:	build-dh
Generate a server certificate:	build-key-server server (Press **Enter** repeatedly to retain default settings.)
Generate a client certificate:	build-key client (Press **Enter** repeatedly to retain default settings.)

2.3.3 Starting the Server

The generated keys are stored in the OpenVPN\easy-rsa\keys directory.

Copy the generated certificates to the OpenVPN\config directory.

Copy the server configuration files from the OpenVPN\sample-config directory to the OpenVPN\config directory.

Start the OpenVPN software.

2.4 Server Configuration

In the OpenVPN installation directory, open the **server.ovpn** or **server.conf** file on a notepad++ to view the server files. For example:

```
port 1194         # Allocated by IANA and can be changed as needed.
proto udp          # TCP is alternative.
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0   # VLAN network segment, which can be changed as required.
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
```

3 Client Configuration and Use

3.1 Client Configuration

The client refers to any Fanvil device that supports OpenVPN. A certificate file is required for Fanvil phones to connect to the OpenVPN server.

Modify the client configuration file **client.ovpn** or **client.conf**. The following is an example of the client configuration file:

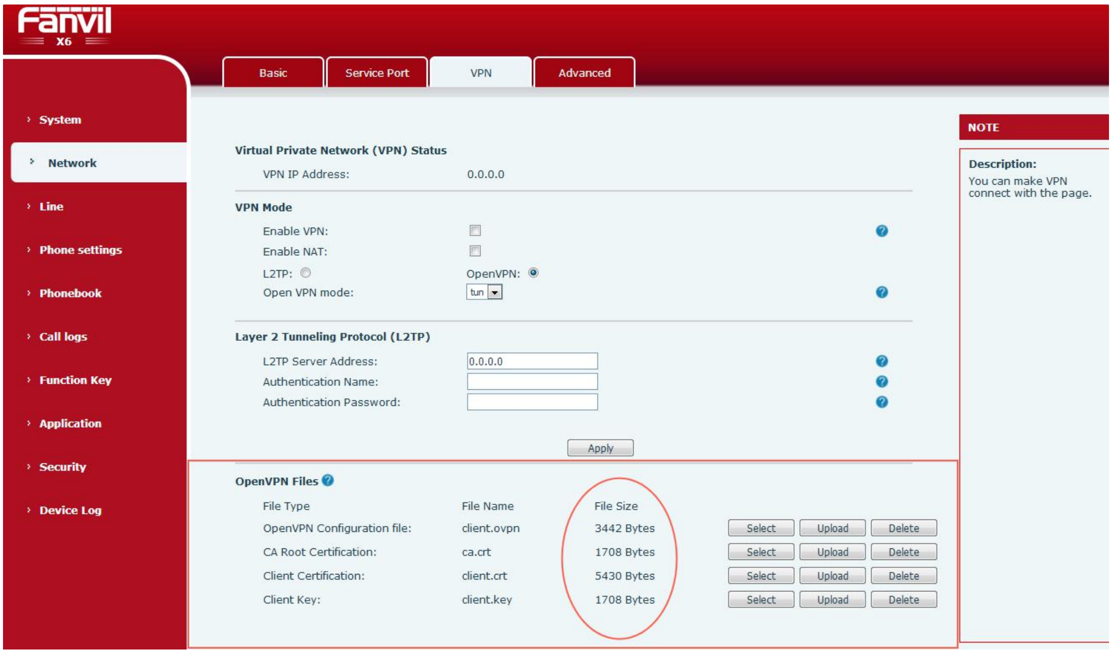
```
client
dev tun
proto udp
remote 192.168.1.135 1194          # Server domain name/IP address and port
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
comp-lzo
verb 3
```

Modify the file based on server configurations.

Export the generated client files **ca.crt**, **client.crt**, and **client.key** for your client upgrade.

3.2 Using OpenVPN on the Phone

Log in to the phone web page, choose **Network** > **VPN,** and upgrade the certificate files **client.ovpn**, **client.key**, **client.crt**, and **ca.crt** one by one in the **OpenVPN Files** pane. After the upgrade is complete, the sizes of the upgraded files are displayed in the **OpenVPN Files** pane, as shown in the following figure.



Virtual Private Network (VPN) Status

VPN IP Address: 0.0.0.0

VPN Mode

Enable VPN: □

Enable NAT: □

L2TP: ○ OpenVPN: ●

Open VPN mode: tun

Layer 2 Tunneling Protocol (L2TP)

L2TP Server Address: 0.0.0.0

Authentication Name:

Authentication Password:

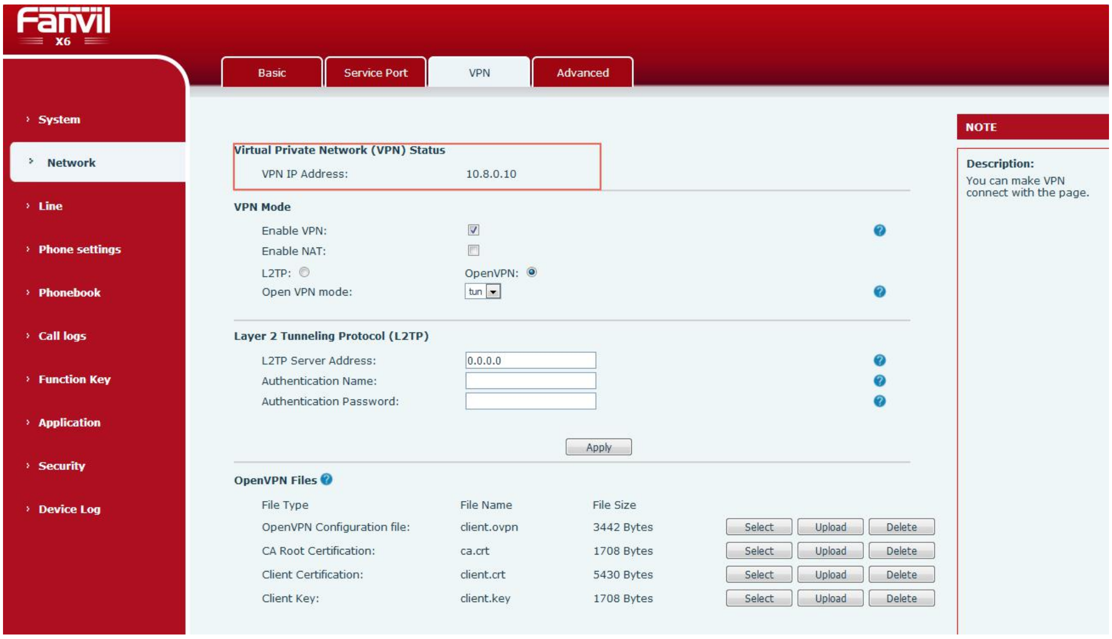
OpenVPN Files

File Type	File Name	File Size
OpenVPN Configuration file:	client.ovpn	3442 Bytes
CA Root Certification:	ca.crt	1708 Bytes
Client Certification:	client.crt	5430 Bytes
Client Key:	client.key	1708 Bytes

NOTE

Description:
You can make VPN connect with the page.

On the **VPN** tab page, select **OpenVPN** in VPN mode, select **Enable VPN**, and click **Apply**. After you successfully connect to the server, the obtained IP address is displayed in the **Virtual Private Network (VPN) Status** pane on the **VPN** tab page. As shown in the following figure, the IP address is **10.8.0.10**.



Virtual Private Network (VPN) Status

VPN IP Address: 10.8.0.10

VPN Mode

Enable VPN: ☑

Enable NAT: □

L2TP: ○ OpenVPN: ●

Open VPN mode: tun

Layer 2 Tunneling Protocol (L2TP)

L2TP Server Address: 0.0.0.0

Authentication Name:

Authentication Password:

OpenVPN Files

File Type	File Name	File Size
OpenVPN Configuration file:	client.ovpn	3442 Bytes
CA Root Certification:	ca.crt	1708 Bytes
Client Certification:	client.crt	5430 Bytes
Client Key:	client.key	1708 Bytes

NOTE

Description:
You can make VPN connect with the page.

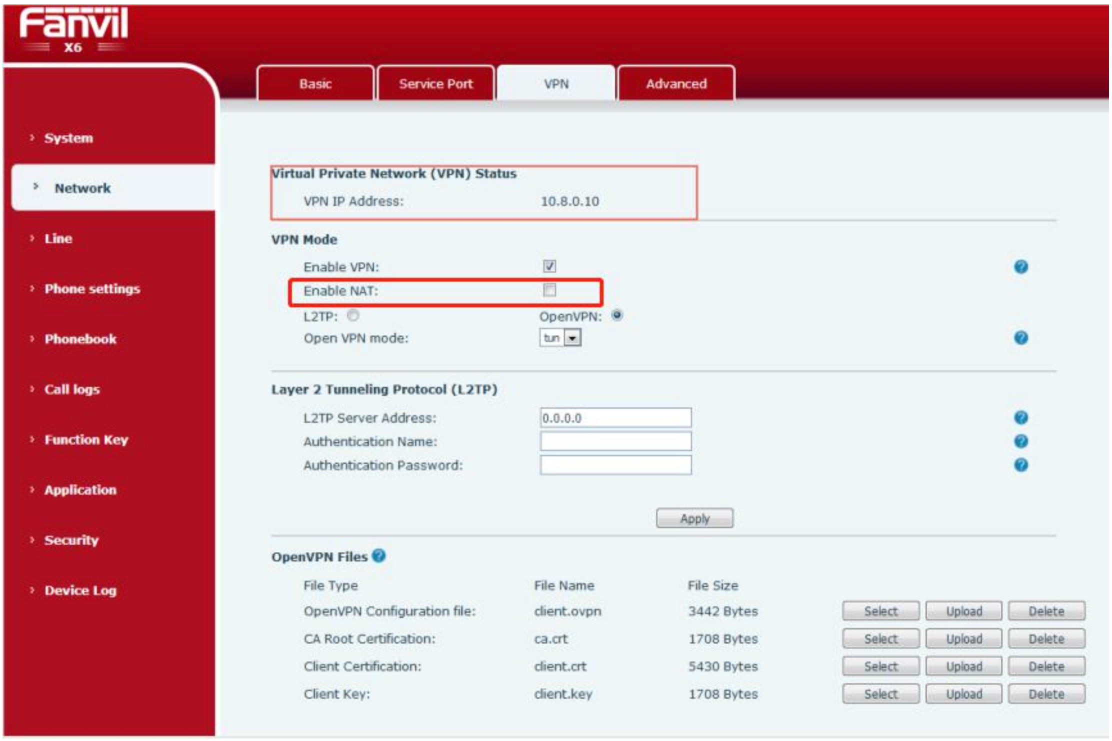
Notes:

1. The X3S / X4 phones do not have the Open VPN mode selection box. The default is tun, which does not support tap mode. The X5S / X6 / X7 / X7C / X210 / X210i phones have the Open VPN mode set to tun by default. You can use the drop-down box to select tap mode.

2. Android phones such as X7A need to import a VPN certificate from the webpage to

install apk on the phone to use openvpn.

3.3 Enable VPN NAT



Virtual Private Network (VPN) Status

VPN IP Address: 10.8.0.10

VPN Mode

Enable VPN: ☑

Enable NAT: □

L2TP: ○ OpenVPN: ●

Open VPN mode: tun

Layer 2 Tunneling Protocol (L2TP)

L2TP Server Address: 0.0.0.0

Authentication Name:

Authentication Password:

Apply

OpenVPN Files

File Type	File Name	File Size			
OpenVPN Configuration file:	client.ovpn	3442 Bytes	Select	Upload	Delete
CA Root Certification:	ca.crt	1708 Bytes	Select	Upload	Delete
Client Certification:	client.crt	5430 Bytes	Select	Upload	Delete
Client Key:	client.key	1708 Bytes	Select	Upload	Delete

application method :

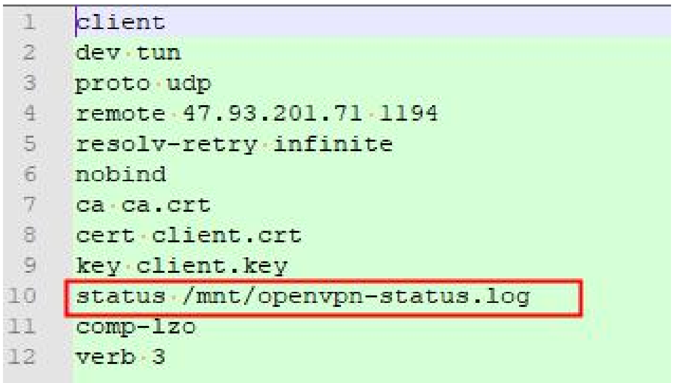
Open **Enable VPN** and **Enable NAT**. The PC (gateway needs to be set to the IP of the phone) connects to the LAN port of the phone. At this time, the PC can access the VPN of the phone.

PC ping10.8.0.10 can ping, ping www.baidu.com can also ping （It's the VPN IP address10.8.0.10)

Notes:

1．Currently supports the models J3G/X3U/X3SG/J1P and X5S/X6/X7/X7C/X210/X210i;X3S/X4 is not currently supported

2．To open the VPN NAT of the J3G/X3U/X3SG/J1P phone, the imported client.ovpn certificate needs to specify the log file path as any path under/MNT /, as shown in the following figure:



```
client
dev tun
proto udp
remote 47.93.201.71 1194
resolv-retry infinite
nobind
ca ca.crt
cert client.crt
key client.key
status /mnt/openvpn-status.log
comp-lzo
verb 3
```