About VPN

VPN (Virtual Private Network) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users with secure access to a central organizational network. VPN gives the organization the advantage of creating secure channels of communication, while at the same time reducing costs, improving security and increasing performance.

There are two types of VPN access: remote-access and site-to-site.

Types of VPN Access

Remote-access VPN, also called a virtual private dial-up network (VPDN), is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.

Site-to-site VPN connects entire networks to each other, that means, site-to-site VPN can be used to connect a branch or remote office network to a company headquarters network. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator or security appliance.

VPN Technology

VPN technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other bases or carrier protocols, then transmitted between the VPN client and the server, and finally de-encapsulated on the receiving side.

Several computer network protocols have been implemented specifically for use with VPN tunnels. The most two popular VPN tunneling protocols are: SSL (Security Socket Layer) and IPSec (Internet Protocol Security). VPN can be classified by the protocols used to tunnel the traffic.

SSL VPN

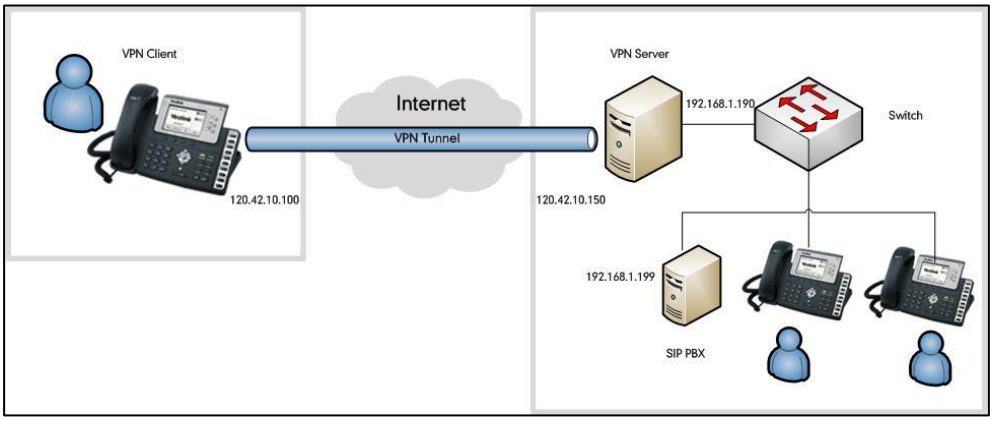
SSL VPN uses SSL protocol and Transport Layer Security (TLS) protocol to provide a secure connection between remote users and internal network resources. It can be used with a standard web browser, and does not require the installation of specialized client software on the end user's device. An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of devices, accessing resources from many locations.

IPSec VPN

An IPSec VPN uses the standard IPSec mechanism to establish a VPN connection over the public Internet. IPSec is a framework for a set of protocols for security at the network or packet processing layer of network communication. IPSec VPN requires installation of the IPSec client software on a client device before a connection can be established. IPSec can meet most security goals: authentication, integrity and confidentiality.

Example Use of a VPN Tunnel

An employee has an IP phone with a public IP address 120.42.10.100 that wishes to connect to the SIP server inside a company network. The SIP server has an internal IP address 192.168.1.199 and is not reachable publicly. Before reaching this server, the IP phone needs to go through a VPN server that has a public IP address 120.42.10.150 and an internal address 192.168.1.190. All data between the IP phone and the SIP server will need to be kept confidential, hence a secure VPN is used.



The following steps illustrate the principles of a VPN client-server interaction:

1. The VPN client connects to a VPN server via an external network interface.
2. The VPN server assigns an IP address to the VPN client from the VPN server's subnet. The client gets an internal IP address 192.168.1.192, for example, and creates a virtual network interface through which it will send encrypted packets to the other tunnel endpoint (the device at the other end of the tunnel).
3. When the VPN client wishes to communicate with the SIP server, it prepares a packet addressed to 192.168.1.199, encrypts it and encapsulates it in an outer VPN packet. This packet is then sent to the VPN server at IP address 120.42.10.150 over the public Internet. The inner packet is encrypted so that even if someone intercepts the packet over the Internet, they cannot get any information from it. The inner encrypted packet has source address 192.168.1.192 and destination address 192.168.1.199. The outer packet has source address 120.42.10.100 and destination address 120.42.10.150.
4. When the packet reaches the VPN server from the Internet, the VPN server de-encapsulates the inner packet, decrypts it, finds the destination address to be 192.168.1.199, and forwards it to the intended SIP server at 192.168.1.199.

5. After some time, the VPN server receives a reply packet from 192.168.1.199, intended for 192.168.1.192. The VPN server consults its routing table, and knows this packet is intended for a remote device (IP phone) that must go through VPN.
6. The VPN server encrypts this reply packet, encapsulates it in a VPN packet and sends it out over the Internet. The inner encrypted packet has a source address 192.168.1.199 and a destination address 192.168.1.192. The outer VPN packet has a source address 120.42.10.150 and a destination address 120.42.10.100.
7. The VPN client receives and de-encapsulates the packet, decrypts the inner packet and passes it to the appropriate software at upper layers.

Yealink IP Phones Compatible with VPN

Yealink IP phones support OpenVPN feature. OpenVPN is a remote-access VPN and is designed to work with the TUN/TAP virtual networking interface that exists on most platforms (e.g., Linux, Windows). TAP simulates an Ethernet device and operates with layer 2 packets such as frames. TUN simulates a network layer device and operates with layer 3 packets such as IP packets. Packets sent by an operating system via a TUN/TAP device are delivered to a user-space program that attaches itself to the device. A user-space program may also pass packets into a TUN/TAP device.

OpenVPN operates as a client-server application. After enabling the OpenVPN feature on IP phones, the IP phones act as VPN clients and use pre-shared secret keys, certificates, or user name/password to authenticate the OpenVPN server.

Installing the OpenVPN Server

OpenVPN server is a set of installation and configuration tools that simplifies the rapid deployment of a VPN remote access solution. It's supported on Linux, Windows, and MAC platforms.

Before using the OpenVPN feature on IP phones, you must make sure the OpenVPN server is prepared properly, otherwise you need to install and configure the OpenVPN server. This chapter provides you on how to install and configure the OpenVPN server and create the OpenVPN TAR file on Linux and Windows platforms.

Installing and Configuring the OpenVPN Server on the Linux Platform

The OpenVPN server software is available for free. This section provides you information on how to install the OpenVPN server (e.g., openvpn-2.1.4.tar.gz) on the Linux platform (e.g., Centos 5.8 and kernel: 2.6.18-308.el5-i686).

Before the installation, make sure the hardware and system meet the following requirements:

- Dual network cards.
- The system kernel supports the Universal TUN/TAP device driver (kernel 2.6.0 above) and the TUN/TAP module is loaded into the kernel.
- Install the required modules "OpenSSL and LZO".

To check if the TUN/TAP module is loaded into the kernel:

1. Open a terminal window.
2. Enter the following command.

   [root@localhost~]# cat /dev/net/tun

   - If the return information is "cat: /dev/net/tun: File descriptor in bad state", it means that the TUN/TAP module has been loaded into the kernel.
   - If the return information is "cat: /dev/net/tun: No such device", you need to execute the following commands to load the TUN/TAP module.

     [root@localhost~]# cd /usr/src/kernels/2.6.18-308.el5-i686/

     [root@localhost 2.6.18-308.el5-i686]# make menuconfig

     In the pop-up configuration screen, select **Device Drivers**->**Network device support**->**Universal TUN/TAP device driver support** and set **Universal TUN/TAP device driver support** to **M**.

You can download the OpenSSL module online: http://www.openssl.org/. The following takes "openssl-1.0.0e.tar.gz" as an example. Download and store it in the root directory.

To install the OpenSSL module:

1. Open a terminal window.
2. Extract the installation package to the /etc directory.

   [root@localhost~]# cd /etc/

   [root@localhost etc]# tar zvxf /openssl-1.0.0e.tar.gz
3. Enter into the extracted directory.

   [root@localhost etc]# cd openssl-1.0.0e
4. Enter the following commands to install the package.

   [root@localhost openssl-1.0.0e]# ./config

   [root@localhost openssl-1.0.0e]# make

   [root@localhost openssl-1.0.0e]# make install

You can download the LZO module online: http://www.oberhumer.com/opensource/lzo/download/. The following takes "lzo-2.02.tar.gz" as an example. Download and store it in the root directory.

To install the LZO module:

1. Open a terminal window.

2. Extract the installation package to the /etc directory.

   [root@localhost~]# cd /etc/

   [root@localhost etc]# tar zvxf /lzo-2.02.tar.gz

3. Enter into the extracted directory.

   [root@localhost etc]# cd lzo-2.02

4. Enter the following commands to install the package.

   [root@localhost lzo-2.02]# ./configure

   [root@localhost lzo-2.02]# make

   [root@localhost lzo-2.02]# make install

You can download the OpenVPN software online: http://openvpn.net/index.php/open-source/downloads.html. Download and store it in the root directory.

To install the OpenVPN server:

1. Open a terminal window.
2. Extract the installation package to the /etc directory

   [root@localhost~]# cd /etc/

   [root@localhost etc]# tar zvxf /openvpn-2.1.4.tar.gz

3. Enter into the extracted directory.

   [root@localhost etc]# cd openvpn-2.1.4

4. Enter the following commands to install the package.

   [root@localhost openvpn-2.1.4]# ./configure

   [root@localhost openvpn-2.1.4]# make

   [root@localhost openvpn-2.1.4]# make install

   If the header and library files are not found, you should use the following command instead of the command "./configure" mentioned above.

   ./configure-prefix=/usr/local --with-lzo-headers=/usr/local/include --with-lzo-lib=/usr/local/lib --with-ssl-headers=/usr/local/include/openssl --with-ssl-lib=/usr/local/lib

5. Add the OpenVPN service.

   [root@localhost openvpn-2.1.4]# cp -p sample-scripts/openvpn.init /etc/init.d/openvpn

   [root@localhost openvpn-2.1.4]# chkconfig --add openvpn

To generate certificate files for the OpenVPN server and IP phones:

1. Enter into the directory used to generate the certificate files (may vary between different versions).

   [root@localhost ~]# cd /etc/openvpn-2.1.4/easy-rsa/2.0

2. Enter the following commands.

   [root@localhost 2.0]# export D=`pwd`

```
[root@localhost 2.0]# export KEY_CONFIG=$D/openssl.cnf
[root@localhost 2.0]# export KEY_DIR=$D/keys
[root@localhost 2.0]# export KEY_SIZE=1024
[root@localhost 2.0]# export KEY_COUNTRY=CN
[root@localhost 2.0]# export KEY_PROVINCE=FJ
[root@localhost 2.0]# export KEY_CITY=XM
[root@localhost 2.0]# export KEY_ORG="yealink.com"
[root@localhost 2.0]# export KEY_EMAIL="admin@yealink.com"
```

3. Generate a CA certificate.

```
[root@localhost 2.0]# ./clean-all
[root@localhost easy-rsa]# ./build-ca
```

The screen prompts the following information (if you don't want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
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) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [yealink.com]:
Organizational Unit Name (eg, section) []:yealink.com
Common Name (eg, your name or your server's hostname) [yealink.com CA]:server
Name []:
Email Address [admin@yealink.com]:
```

4. Generate a certificate for the OpenVPN server.

```
[root@localhost 2.0]# ./build-key-server server
```

The screen prompts the following information (if you don't want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

```
Generating a 1024 bit RSA private key
.....++++++
...++++++
writing new private key to '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) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [yealink.com]:
Organizational Unit Name (eg, section) []:yealink.com
Common Name (eg, your name or your server's hostname) [server]:server
Name []:
Email Address [admin@yealink.com]:yealink.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abcd1234
An optional company name []:yealink.com
Using configuration from /root/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:'CN'
stateOrProvinceName       :PRINTABLE:'FJ'
localityName              :PRINTABLE:'XM'
organizationName          :PRINTABLE:'yealink.com'
organizationalUnitName:PRINTABLE:'yealink.com'
commonName                :PRINTABLE:'server'
emailAddress              :IA5STRING:'yealink.com'
Certificate is to be certified until May 18 11:53:36 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

5. Generate a certificate for the client.

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

The screen prompts the following information (if you don't want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

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) [CN]:

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

Locality Name (eg, city) [XM]:

Organization Name (eg, company) [yealink.com]:

Organizational Unit Name (eg, section) []:yealink.com

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

Name []:

Email Address [admin@yealink.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:abcd1234

An optional company name []:yealink.com

Using configuration from /root/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:'CN'

stateOrProvinceName :PRINTABLE:'FJ'

localityName :PRINTABLE:'XM'

organizationName :PRINTABLE:'yealink.com'

organizationalUnitName:PRINTABLE:'yealink.com'

commonName :PRINTABLE:'server'

emailAddress :IA5STRING:'admin@yealink.com'

Certificate is to be certified until May 18 11:57:27 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

6. Generate a dh1024.pem file for the server.

   [root@localhost 2.0]# ./build-dh

   The screen prompts the following information:

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

   This is going to take a long time

   If the screen prompts "./build-dh: line 7: dhparam: command not found", you need to edit the file "build-dh" in the /etc/openvpn-2.1.4/easy-rsa/2.0 directory. Set "$OPENSSL" to "openssl" and save the file.

All the certificate files are generated in the directory "/openvpn-2.1.4/easy-rsa/2.0/keys".

To configure the server's configuration file:

1. Create a new directory "openvpn" located in the path /etc.

   [root@localhost ~]# mkdir /etc/openvpn

2. Create a new directory "keys" located in the path /etc/openvpn.

   [root@localhost ~]# mkdir /etc/openvpn/keys

3. Enter into the installation directory of the OpenVPN server.

   [root@localhost ~]# cd /etc/openvpn-2.1.4

4. Copy the certificate files required for the server to the directory "keys" created above.

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/ca.crt /etc/openvpn/keys/

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/dh1024.pem /etc/openvpn/keys/

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/server.crt /etc/openvpn/keys/

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/server.key /etc/openvpn/keys/

5. Copy the file "server.conf" in the sample-config-files directory to the directory "openvpn" created above.

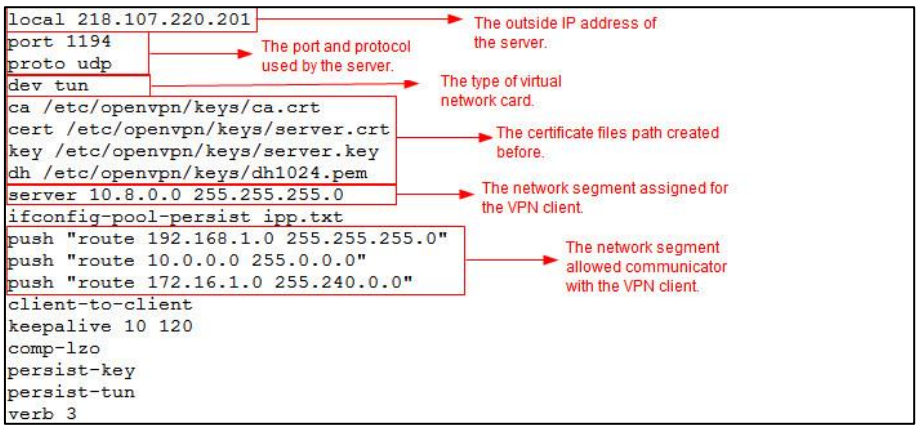
   [root@localhost openvpn-2.1.4]# cp sample-config-files/server.conf /etc/openvpn

6. Edit the file "server.conf" according to your actual network environment and save the change.

   [root@localhost ~]# vi /etc/openvpn/server.conf

Press the "I" key to enter into the Insert Mode and modify the desired parameters, and then press the "Esc" key to return to the Command Mode and enter "wq!".

The following shows an example:



According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature and routing entries between the VPN clients and the Intranet. For more information, contact your network administrator.

To enable the TCP/IP forwarding:

1. Open a terminal window.
2. Edit the file "sysctl.conf" in the /etc directory and save the change.

   [root@localhost ~]# vi /etc/sysctl.conf

   Press the "I" key to enter into the Insert Mode and Set "**net.ipv4.ip_forward**" to 1, and then press the "Esc" key to return to the Command Mode and enter "wq!".

To start the OpenVPN service:

1. Enter into the installation directory of the OpenVPN server.

   [root@localhost ~]# cd /etc/openvpn-2.1.4
2. Start the OpenVPN service.

   [root@localhost openvpn-2.1.4]# service openvpn start

Creating the OpenVPN TAR File for the VPN Client on the Linux Platform

OpenVPN requires using certificates to help establish the authenticity of clients connecting to an OpenVPN server. You need to obtain the files: ca.crt, client.crt, client.key and vpn.cnf from the system, and then package these files to TAR format.

To configure the client's configuration file:

1. Create a new directory "client" located in the path /etc/openvpn.

[root@localhost ~]# mkdir /etc/openvpn/client

2. Create a new directory "keys" located in the path /etc/openvpn/client.

   [root@localhost ~]# mkdir /etc/openvpn/client/keys

3. Enter into the installation directory of the OpenVPN server.

   [root@localhost ~]# cd /etc/openvpn-2.1.4

4. Copy the certificate files required for the client to the directory "/etc/openvpn/client/keys" created before.

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/ca.crt /etc/openvpn/client/keys/

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/client.crt /etc/openvpn/client/keys/

   [root@localhost openvpn-2.1.4]# cp easy-rsa/2.0/keys/client.key /etc/openvpn/client/keys/

5. Copy the file "client.conf" in the sample-config-files directory to the directory "client" created above and rename it to vpn.cnf.

   [root@localhost openvpn-2.1.4]# cp sample-config-files/client.conf /etc/openvpn/client/vpn.cnf

6. Edit the file "vpn.cnf" and save the change.

   [root@localhost openvpn-2.1.4]# cd /etc/openvpn/client

   [root@localhost client]# vi vpn.cnf

   Press the "I" key to enter into the Insert Mode and modify the desired parameters, and then press the "Esc" key to return to the Command Mode and enter "wq!".

   The following parameters should be configured as the same as that of the server.

   remote 218.107.220.201 1194 udp

   dev tun

   dev-type tun

   The following defines the unified directories of the OpenVPN certificates and key for Yealink IP phones:

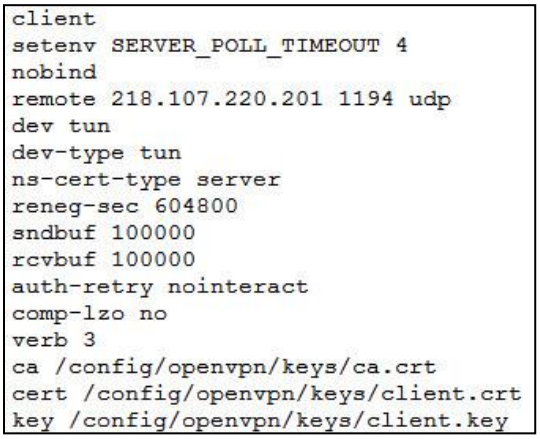
   ca /config/openvpn/keys/ca.crt

   cert /config/openvpn/keys/client.crt

   key /config/openvpn/keys/client.key

   The unified directories of the certificates and key listed above are supported by SIP-T57W, SIP-T54W, SIP-T53W, SIP-T53, VP59, SIP-T58A, SIP VP-T49G, SIP-T4X, CP860, CP920, CP960, CP930W-Base, W52P, W56P, W60P, W53P, SIP-T29G, SIP-T27G, SIP-T23P/G, SIP-T21(P) E2 IP phones.

The following figure shows a portion of the vpn.cnf file for reference:



```
client
setenv SERVER_POLL_TIMEOUT 4
nobind
remote 218.107.220.201 1194 udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 604800
sndbuf 100000
rcvbuf 100000
auth-retry nointeract
comp-lzo no
verb 3
ca /config/openvpn/keys/ca.crt
cert /config/openvpn/keys/client.crt
key /config/openvpn/keys/client.key
```

To package the TAR file on the Linux platform:

1. Enter the following commands to package the TAR file.

   [root@localhost ~]# cd /etc/openvpn/client

   [root@localhost client]# tar -cvpf openvpn.tar *

   An openvpn.tar file is generated in the client directory.

Installing and Configuring the OpenVPN Server on the Windows Platform

The OpenVPN server software is available for free. You can download it for your Windows platform online.

This section provides you on how to install the OpenVPN server (e.g., openvpn-2.1.1-install.exe) on the Windows XP platform.

Before the installation, make sure the hardware and system meet the following requirements:

- Dual network cards.
- The system kernel supports the TUN/TAP module.

To install the OpenVPN server on the Windows XP platform:

1. Double click the installation file on the local system.
2. Follow the prompts to finish the installation.

   The default installation directory is C:\Program Files\OpenVPN\.

To generate certificate files for the OpenVPN server and IP phones:

1. Enter into the installation directory of the OpenVPN server.
2. Open the file vars.bat in the easy-rsa folder and edit the following parameters:

   set KEY_COUNTRY=US

set KEY_PROVINCE=CA

set KEY_CITY=SanFrancisco

set KEY_ORG=OpenVPN

set KEY_EMAIL=mail@host.domain

The following shows an example of configuring these parameters:

set KEY_COUNTRY=CN

set KEY_PROVINCE=FJ

set KEY_CITY=XM

set KEY_ORG=Yealink

set KEY_EMAIL=admin@yealink.com

3. Click **Start**->**Run**.
4. Enter **cmd** in the pop-up dialogue box and click **OK** to open a command prompt screen.
5. Enter into the directory easy-rsa located in the installation directory of the OpenVPN server.

   C:\Documents and Settings\Administrator>cd \Program Files\OpenVPN\easy-rsa
6. Enter the following commands.

   C:\Program Files\OpenVPN\easy-rsa>init-config.bat

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

   C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
7. Generate a CA certificate.

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

   The screen prompts the following information (if you don't want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

   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) [FJ]:

Locality Name (eg, city) [XM]:

Organization Name (eg, company) [Yealink]:

Organizational Unit Name (eg, section) []:

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

Email Address [admin@yealink.com]:

8. Generate a dh1024.pem file for the server.

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

The screen prompts the following information:

Loading 'screen' into random state - done

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

This is going to take a long time

9. Generate a certificate for the OpenVPN server.

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

The screen prompts the following information (if you don't want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

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) [CN]:

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

Locality Name (eg, city) [XM]:

Organization Name (eg, company) [Yealink]:

Organizational Unit Name (eg, section) []:

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

Email Address [admin@yealink.com]:

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

A challenge password []:serverpwd

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:'Yealink'

organizationalUnitName:PRINTABLE:'EMB'

commonName :PRINTABLE:'Server'

emailAddress :IA5STRING:'admin@yealink.com'

Certificate is to be certified until Jan 20 13:10:22 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

10. Generate a certificate for the client.

C:\Program Files\OpenVPN\easy-rsa>build-key.bat client

The screen prompts the following information (if you don't want to change the default settings, press the ENTER key, else enter the desired value and then press the ENTER key):

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.

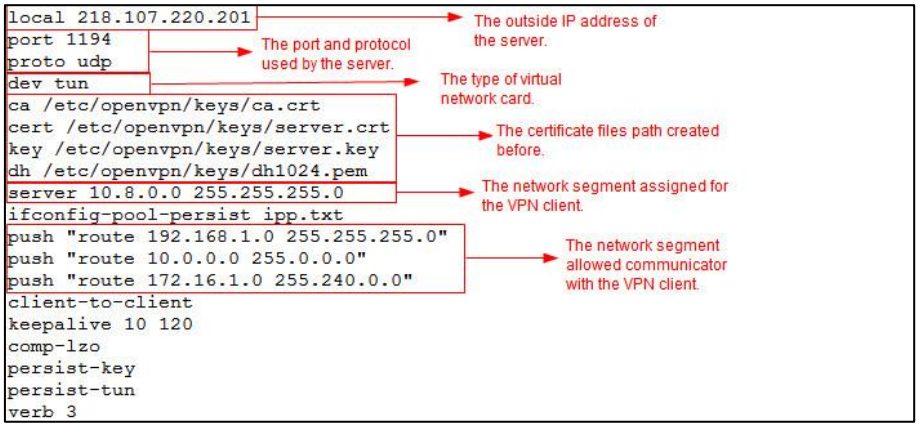
Country Name (2 letter code) [CN]:

```
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [XM]:
Organization Name (eg, company) [Yealink]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: Client
Email Address [admin@yealink.com]:
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:clientpwd
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:'Yealink'
organizationalUnitName:PRINTABLE:'EMB'
commonName                  :PRINTABLE:'Client'
emailAddress                :IA5STRING:'admin@yealink.com'
Certificate is to be certified until Jan 20 13:10:22 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
```

To configure the server's configuration file:

1. Enter the installation directory of the OpenVPN server.
2. Create a new folder "serverconfig" in the directory.
3. Copy the file "server.ovpn" in the sample-config folder to the serverconfig folder created above.
4. Edit the file "server.ovpn" according to your actual network environment and save the change.

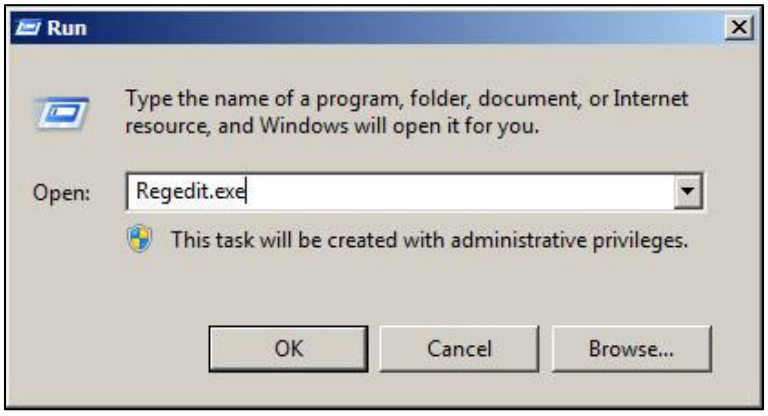
The following shows an example:



According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature, Internet connection sharing feature and routing entries between the VPN clients and the Intranet. For more information, contact your network administrator.

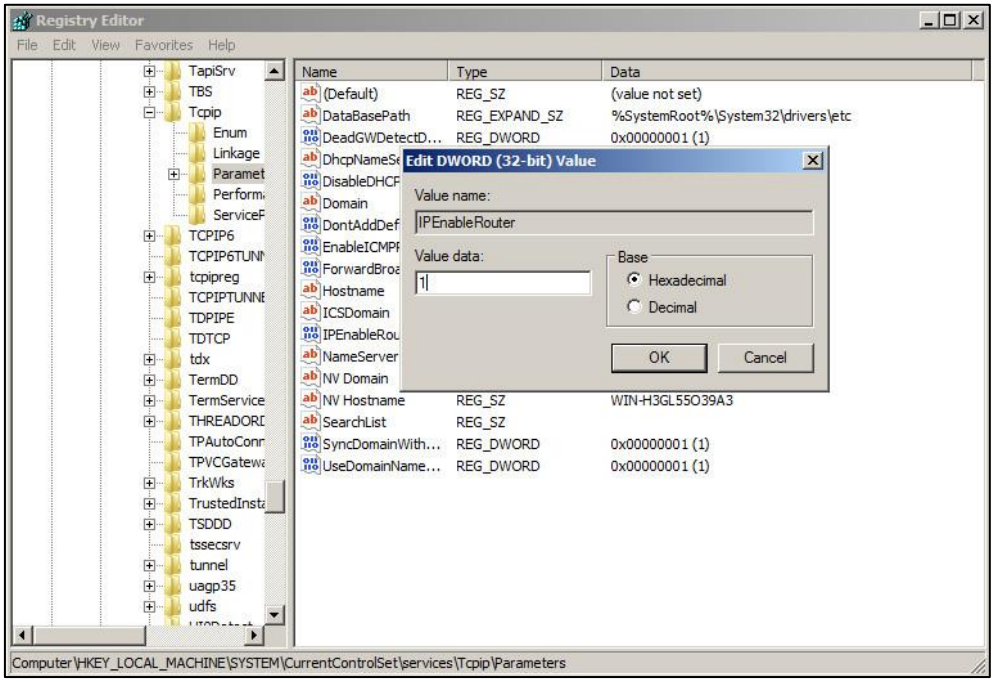
To enable the TCP/IP forwarding:

1. Click **Start**->**Run**.
2. Enter **Regedit.exe** in the pop-up dialogue box and click **OK**.



3. Click on **HKEY_LOCAL_MACHINE**->**SYSTEM**->**CurrentControlSet**->**Services**->**Tcpip**->**Parameters**.

4. Set "**IPEnableRouter**" to 1.



To enable Internet connection sharing for inside network card:

1. Open network connections.
2. Right click the local area network for the inside network card and select **Properties**.
3. On the **Advanced** tab, check the **Allow other network users to connect through this computer's Internet connection** check box.
4. Select the virtual network card of the server from the pull-down list of **Home networking connection**.
5. Click **OK** to save the change.

Creating the OpenVPN Tar File for the VPN Client on the Windows Platform

You can package the TAR file on the Windows platform using the tool 7-Zip or GnuWin32. You can download 7-Zip online: http://www.7-zip.org/ and GnuWin32 online: http://gnuwin32.sourceforge.net/packages/gtar.htm.

This section provides you on how to package the TAR file using 7-Zip on the Windows XP platform.

To configure the client's configuration file:

1. Create a new folder "openvpn" in the directory C:/.
2. Copy the file client.ovpn in the sample-config folder to the openvpn folder.
3. Rename the file client.ovpn to vpn.cnf.

4. Create a new folder "keys" in the openvpn folder.
5. Copy ca.crt, client.crt and client.key files to the keys folder created above.
6. Edit the file vpn.cnf.

   The following parameters should be configured as the same as that of the server.

   remote 218.107.220.201 1194 udp

   dev tun

   dev-type tun

   The following defines the unified directories of the OpenVPN certificates and key for Yealink IP phones:

   ca /config/openvpn/keys/ca.crt

   cert /config/openvpn/keys/client.crt

   key /config/openvpn/keys/client.key

   The unified directories of the certificates and key listed above are supported by SIP-T57W, SIP-T54W, SIP-T53W, SIP-T53, VP59, SIP-T58A, SIP VP-T49G, SIP-T4X, CP860, CP920, CP960, CP930W-Base, W52P, W56P, W60P, W53P, SIP-T29G, SIP-T27G, SIP-T23P/G, SIP-T21(P) E2 and SIP-T19(P) E2 IP phones.

   The following figure shows a portion of the vpn.cnf file for reference:

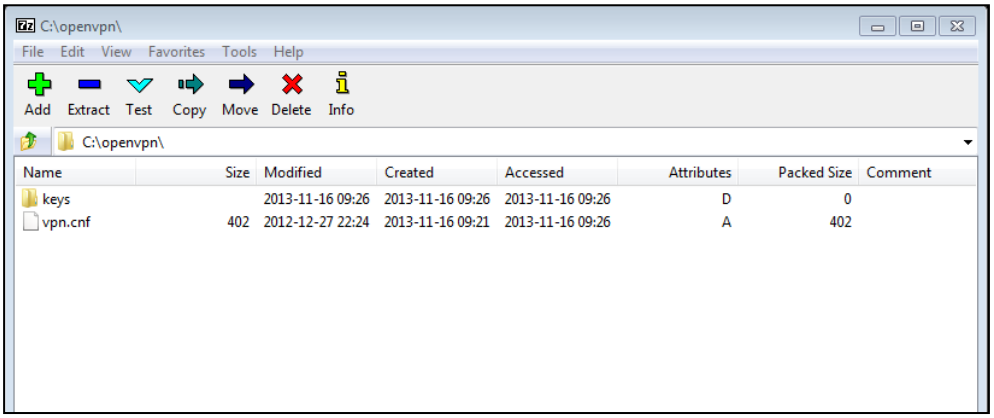
```
client
setenv SERVER_POLL_TIMEOUT 4
nobind
remote 218.107.220.201 1194 udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 604800
sndbuf 100000
rcvbuf 100000
auth-retry nointeract
comp-lzo no
verb 3
ca /config/openvpn/keys/ca.crt
cert /config/openvpn/keys/client.crt
key /config/openvpn/keys/client.key
```

7. Save the change.

To package a TAR file using the tool 7-Zip on the Windows platform:

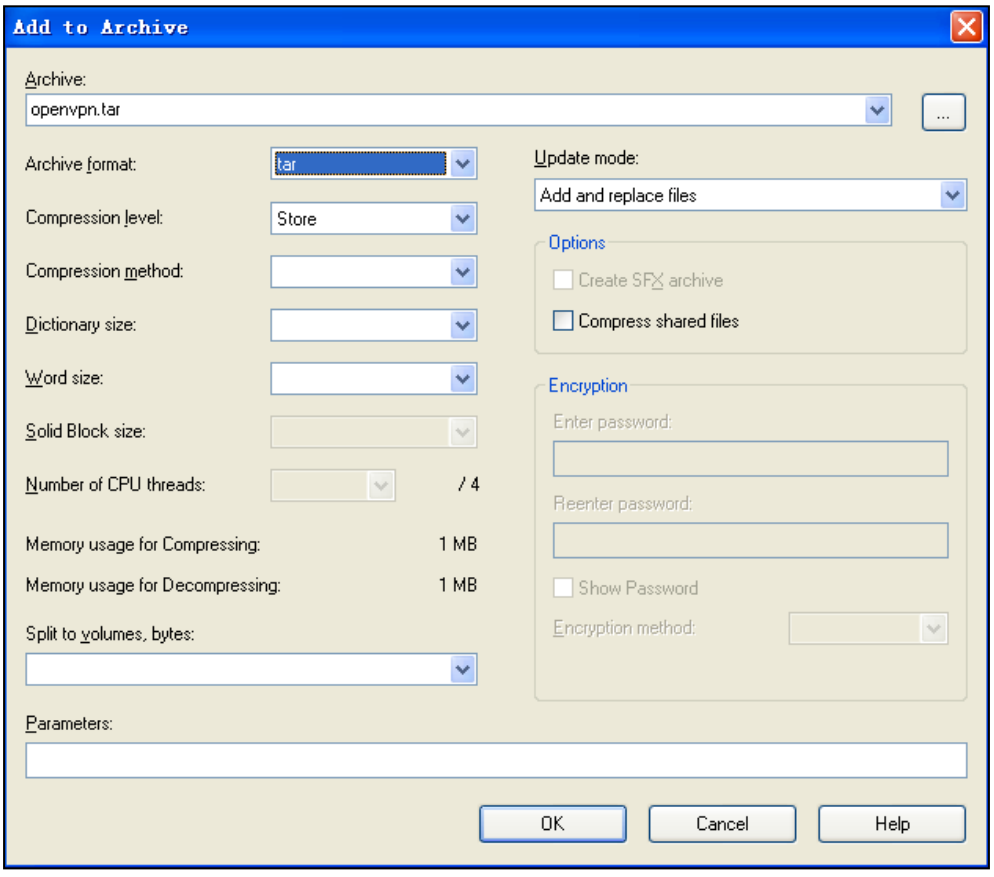
1. Download and install 7-Zip on the local system.
2. Start the 7-Zip file manager application.

3. Locate the openvpn folder from the local system.



4. Click the **Add** button.

5. Select **tar** from the pull-down list of **Archive format**.



6. Click the **OK** button.

   An openvpn.tar file is generated in the directory C:/openvpn.

Configuring OpenVPN Feature on IP Phones

OpenVPN feature is disabled on IP phones by default. You can enable the OpenVPN feature

using configuration files, via web user interface or phone user interface. To use the OpenVPN feature, you also need to upload the OpenVPN TAR file to the IP phones.

The configurations described in this section apply to the following IP phones:

- SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and CP860 IP phones running firmware version 71 or later
- W52P IP DECT phones running firmware version 30 or later
- SIP-T58A, SIP VP-T49G, SIP-T40P, SIP-T29G, SIP-T23P/G, SIP-T21(P) E2, CP960 and W56P IP phones running firmware version 80 or later
- SIP-T48S, SIP-T46S, SIP-T42S, SIP-T41S, SIP-T40G, SIP-T27G, SIP-T19(P) E2, CP920 and W60P IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later
- SIP-T57W, SIP-T54W, SIP-T53W and SIP-T53 IP phones running firmware version 84 or later

Note For Yealink IP phones running firmware version not listed above, configuration files of VPN client for different phone models may be a little different. Please upload the proper TAR files to IP phones.

The following IP phones use the new auto provisioning mechanism:

- SIP-T58A/CP960 IP phones running firmware version 80 or later
- SIP-T48G/T48S/T46G/T46S/T42G/T42S/T41P/T41S/T40P/T40G/T29G/T27G/T23P/T23G/T21(P) E2/T19(P) E2, CP860, CP920, W60P, W52P and W56P IP phones running firmware version 81 or later
- VP59, W53P and CP930W-Base IP phones running firmware version 83 or later
- SIP-T57W/T54W/T53W/T53 IP phones running firmware version 84 or later

Other IP phones or the IP phones listed above running old firmware version use the old auto provisioning mechanism.

For Old Auto Provisioning Mechanism

The followings take the SIP-T23G IP phone running firmware version 80 as examples.

To configure the OpenVPN feature using configuration files:

1. Add/Edit OpenVPN parameters in the configuration file (e.g., y000000000044.cfg).

The following table lists the OpenVPN parameters:

Parameters	Permitted Values	Default
network.vpn_enable	**0 or 1**	**0**
Description: Enables or disables the VPN feature on the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Network->Advanced->VPN->Active **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->VPN->VPN Active		
openvpn.url	**URL within 511 characters**	**Blank**
Description: Specifies the access URL of the OpenVPN TAR file. **Web User Interface:** Network->Advanced->VPN->Upload VPN Config **Phone User Interface:** None		

The following shows an example of configuring the OpenVPN feature in configuration files:

network.vpn_enable = 1

openvpn.url = http://192.168.1.20/openvpn.tar

2. Upload configuration files to the root directory on the provisioning server and trigger IP phones to perform an auto provisioning for configuration update.

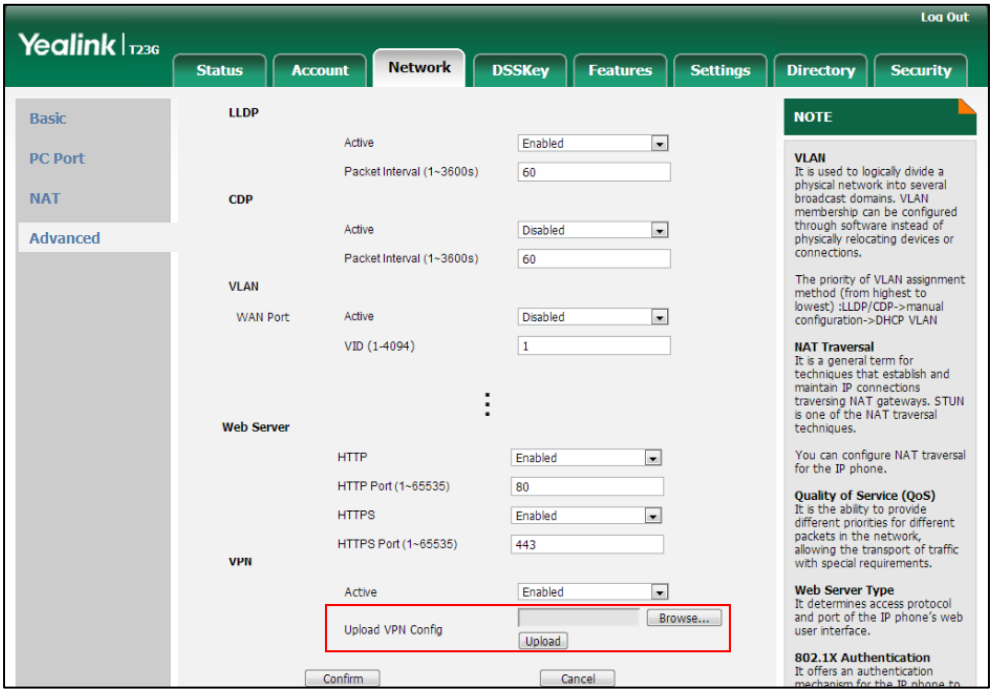
   For more information on auto provisioning, refer to *Yealink_SIP-T2 Series_T19(P) E2_T4 Series_CP860_IP_Phones_Auto_Provisioning_Guide_V80*.

To configure the OpenVPN feature via web user interface:

1. Press the **OK** key on the phone when it is idle to obtain the IP address.
2. Enter the IP address (e.g., http://192.168.0.10 or 192.168.0.10) in the address bar of web browser on your PC and then press the **Enter** key.
3. Enter the user name and password in the login page.

   The default login user name is admin (case-sensitive) and the password is admin (case-sensitive).

4. Click on **Network**->**Advanced**.
5. In the **VPN** block, click **Browse** to locate the OpenVPN TAR file from the local system and then click **Upload** to upload it.



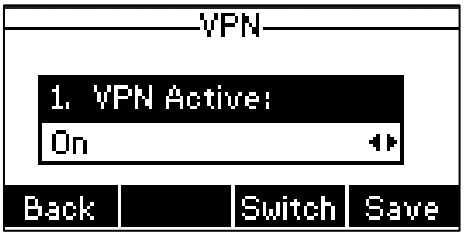
6. In the **VPN** block, select **Enabled** from the pull-down list of **Active**.
7. Click **Confirm** to save the change.

   The web user interface prompts the warning "Some settings you changed take effect when you restart your machine! Do you want to reboot now?".
8. Click **OK** to reboot the IP phone.

To enable the OpenVPN feature via phone user interface (not applicable to W56P):

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**VPN**.
2. Press ◄ or ►, or the **Switch** soft key to select **On** from the **VPN Active** field.

   You must upload the OpenVPN TAR file using configuration files or via web user interface in advance.

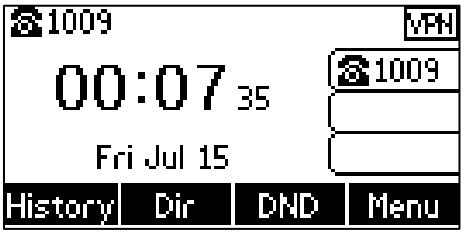


3. Press the **Save** soft key to save the change.

The IP phone reboots automatically to make the settings take effect.

Note On the phone user interface, you can only enable or disable OpenVPN feature.

After the OpenVPN feature is configured successfully, the phone LCD screen displays the VPN icon. The IP phone can access the resources in the company's intranet from home or outside the office.



For New Auto Provisioning Mechanism

The followings take the SIP-T23G IP phone running firmware version 81 as examples.

To configure the OpenVPN feature using configuration files:

1. Add/Edit OpenVPN parameters in the configuration file (e.g., static.cfg).

The following table lists the OpenVPN parameters:

Parameters	Permitted Values	Default
static.network.vpn_enable	**0 or 1**	**0**
Description: Enables or disables the VPN feature on the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Network->Advanced->VPN->Active **Phone User Interface:** Menu->Settings->Advanced Settings (default password: admin) ->Network->VPN->VPN Active		
static.openvpn.url	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Specifies the access URL of the OpenVPN TAR file. **Web User Interface:** Network->Advanced->VPN->Upload VPN Config **Phone User Interface:** None		

The following shows an example of configuring the OpenVPN feature in the configuration file:

```
static.network.vpn_enable = 1
static.openvpn.url = http://192.168.1.20/openvpn.tar
```

2. Reference the configuration file in the boot file (e.g., y000000000000.boot).

   Example:

   include:config "http://10.2.1.158/static.cfg"

3. Upload the boot file and configuration file to the root directory of the provisioning server.
4. Trigger IP phones to perform an auto provisioning for configuration update.

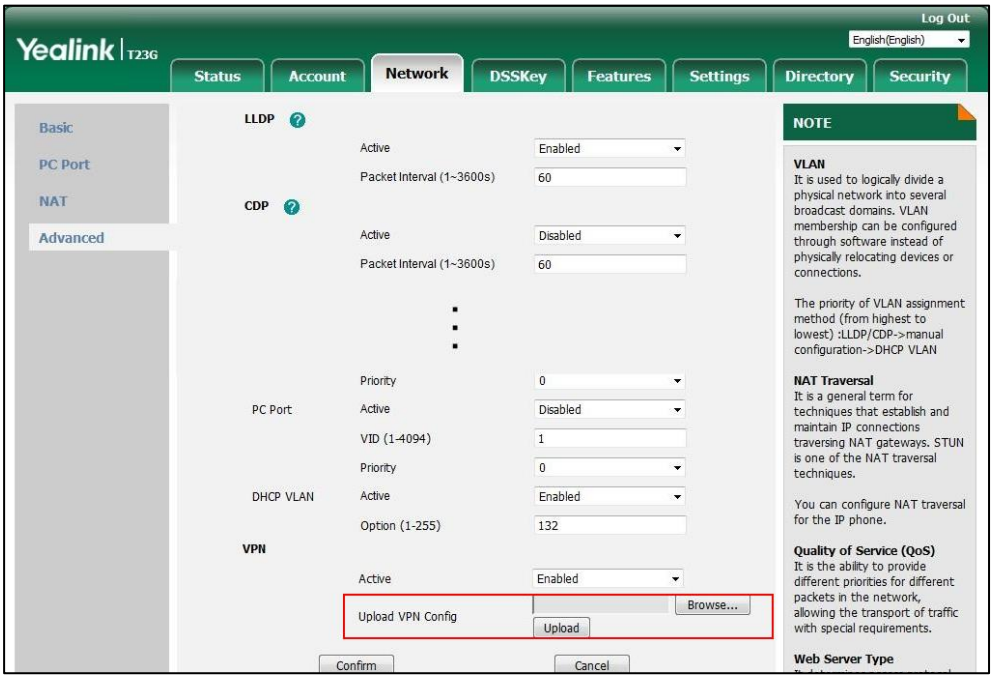
   For more information on auto provisioning, refer to the latest Auto Provisioning Guide on Yealink Technical Support.

To configure the OpenVPN feature via web user interface:

1. Press the **OK** key on the phone when it is idle to obtain the IP address.
2. Enter the IP address (e.g., http://192.168.0.10 or 192.168.0.10) in the address bar of web browser on your PC and then press the **Enter** key.
3. Enter the user name and password in the login page.

   The default login user name is admin (case-sensitive) and the password is admin (case-sensitive).
4. Click on **Network**->**Advanced**.

5. In the **VPN** block, click **Browse** to locate the OpenVPN TAR file from the local system and then click **Upload** to upload it.



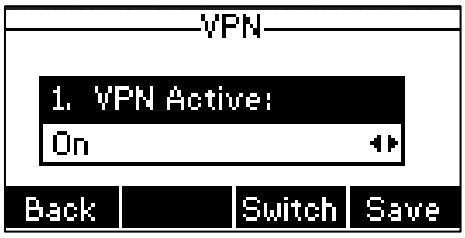
6. In the **VPN** block, select **Enabled** from the pull-down list of **Active**.
7. Click **Confirm** to save the change.

   The web user interface prompts the warning "Some settings you changed take effect when you restart your machine! Do you want to reboot now?".
8. Click **OK** to reboot the IP phone.

To enable the OpenVPN feature via phone user interface:

1. Press **Menu**->**Settings**->**Advanced Settings** (default password: admin) ->**Network**->**VPN**.
2. Press ◄ or ►, or the **Switch** soft key to select **On** from the **VPN Active** field.

   You must upload the OpenVPN TAR file using configuration files or via web user interface in advance.

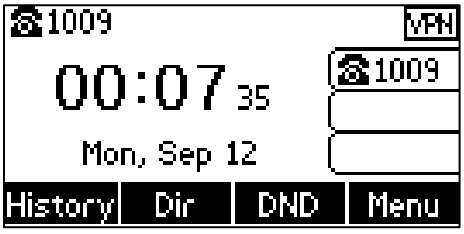


3. Press the **Save** soft key to save the change.

   The IP phone reboots automatically to make the settings take effect.

Note On the phone user interface, you can only enable or disable OpenVPN feature.

After the OpenVPN feature is configured successfully, the phone LCD screen displays the VPN icon. The IP phone can access the resources in the company's intranet from home or outside the office.



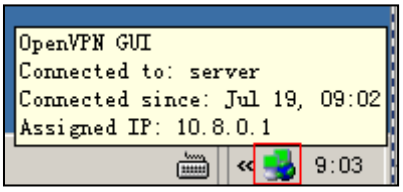
Troubleshooting

Why does the phone fail to connect to the OpenVPN server?

Do the following in sequence:

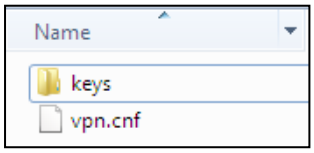
- Ensure that the OpenVPN server is up and running.

  If the OpenVPN server is running properly, a virtual IP address assigning to the OpenVPN server will appear when you hover your mouse pointer over the VPN icon. The VPN icon in the notification area of the system tray is shown as below:



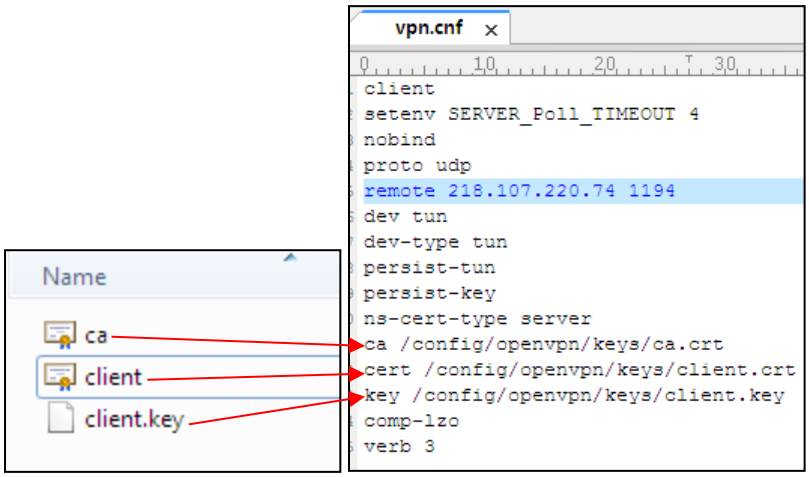
- Ensure that the OpenVPN TAR file uploaded to the IP phone is correctly created.

  Extract the TAR file and ensure that the certificate folder is named as "keys" and the client configuration file is named as "vpn.cnf", as shown below:

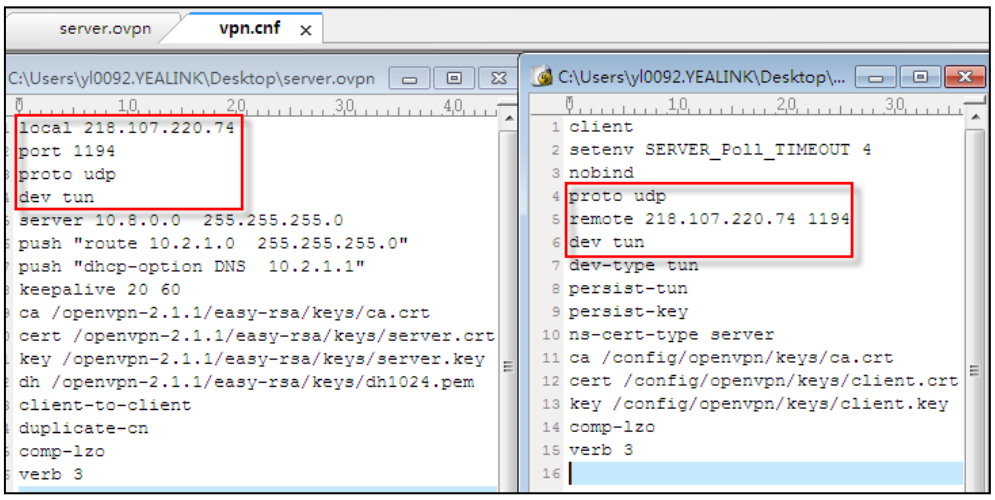


- Ensure that the file names and directories of the client certificates and key defined in the client configuration file are correct.

Enter the "keys" directory to check the file names of client certificates and key.



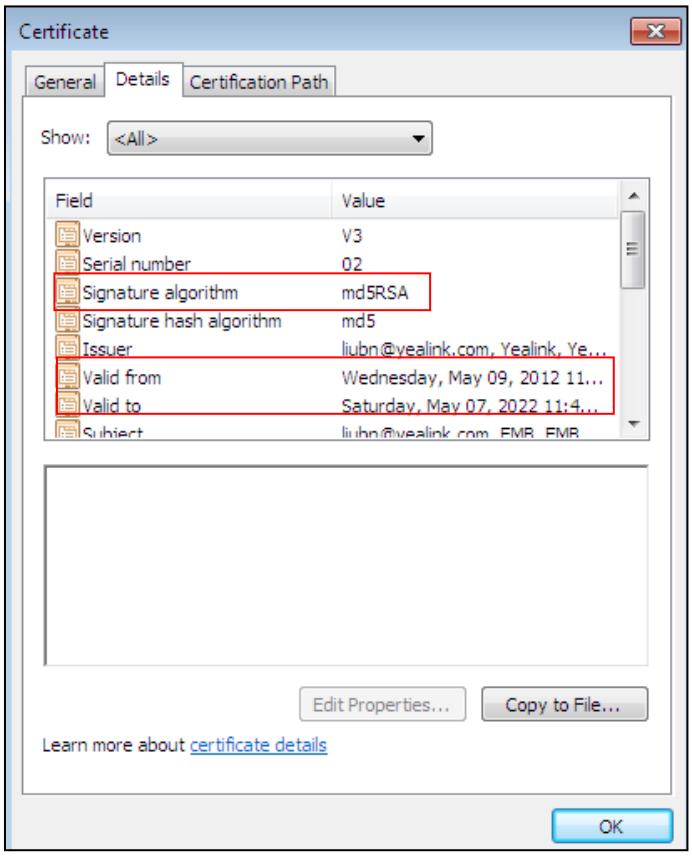
- Ensure that the following configurations in the server configuration file and client configuration file are exactly matched.



- Ensure that the time and date on the phone is within the validity time of the certificate.
- Check if the signature algorithm of the client certificate is supported by the phone.

  IP phones support MD5 and SHA 1 signature algorithms.

Double click the client certificate file to check the validity time and signature algorithm of the certificate.



How to change the signature algorithm of the certificate?

If the signature algorithm of the client certificate is not supported by IP phones, you need to change the signature algorithm, and then re-generate the client certificate.

Do the following:

1. Find the openssl.cnf file located in the folder easy-rsa of the OpenVPN installation path.

   The file name and storage path may vary in your installation environment.
2. Configure the value of the parameter "default_md" to be md5 or sha1, as shown below:

   default_md = md5 or default_md = sha1
3. Re-generate a client certificate following the steps introduced in the section Installing the OpenVPN Server on page 3.

Why does the phone fail to register to the SIP server after successfully connecting to the OpenVPN server?

Do the following in sequence:

- Ensure that the OpenVPN server has dual network cards.
- Ensure that the connection between the OpenVPN server and the SIP server is working correctly by the Ping command.
- Ensure that Internet Connection Sharing and TCP/IP forwarding are enabled on the OpenVPN server on the Windows platform.
- Ensure that access permission of SIP server network segment has been assigned to the phone in the server configuration file.

  For example, the IP address of the SIP server is 192.168.3.6, the server configuration file must contain the configuration **push "route 192.168.3.0 255.255.255.0"**.

Why does the phone fail to register when the domain name of the SIP server is configured on the IP phone?

Do the following in sequence:

- Ensure that the IP address of the DNS server has been added to the server configuration file.

  For example, the IP address of the DNS server is 192.1682.3.10, the server configuration file must contain the configuration **push "dhcp-option DNS 192.1682.3.10"**.
- Ensure that the connection between the DNS server and the phone is working correctly.

Why there is no sound during a call?

Do the following:

1. Ensure that the configuration **client-to-client** has been added to the server configuration file.
2. Reboot the OpenVPN server.

Why the voice quality is poor?

Do the following:

- Network congestion, RTP packet loss or delay may result in poor call quality. In this case, you need to contact your network administrator.

- Ensure that an appropriate log level is set in the client configuration file.

  Yealink recommends you to set the log level to 3 ("verb 3" in the client configuration file). If the log level is set too high, the phone will log phone events frequently. This may cause phone performance issue.

Glossary

IPSec – a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a communication session.

TLS/SSL – cryptographic protocols that provide communication security over the Internet. TLS and SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

TAR - a file format (in the form of a type of archive bit stream) and the name of a program used to handle such files.

Pre - shared Key -a shared secret which was previously shared between the two parties using some secure channel before it needs to be used.

7-Zip - a free and open source file archiver. It operates with the 7z archive format, but can read and write several other archive formats.

GnuWin32 - provides native ports in the form of runnable computer programs, patches, and source code for various GNU and open source tools and software, much of it modified to run on the 32-bit Windows platform.

Example Configuration Files

The following lists example configuration files detailing how to configure the server and client configuration files. Configurations may vary between different network environments.

Server Configuration File

```
local 218.107.220.74       #Outside IP address of the VPN server
port 1194                  #Port of the VPN server
proto udp                  #Transport protocol (udp or tcp) of the VPN server
dev tun                    #Virtual network interface (tun or tap)
server 10.8.0.0    255.255.255.0       #Virtual IP segment assigned to VPN clients
push "route 10.2.1.0    255.255.255.0"    # Inside network segment allowed to #be
                                          accessed by VPN clients
push "dhcp-option DNS    10.2.1.1"          #IP address of the DNS server #assigned
                                            to the VPN clients.
keepalive 20 60     #Ping the VPN server every 20 seconds. If the ping is not
                     #successfully within 60 seconds, reconnect the VPN server.
```

Client Configuration File

```
client
setenv SERVER_Poll_TIMEOUT 4
nobind
proto udp                          #Transport protocol (udp or tcp) of the VPN server
remote 218.107.220.74 1194         #Outside IP address and port of the VPN server
dev tun                            #Virtual network interface (tun or tap)
dev-type tun
persist-tun
persist-key
ns-cert-type server
ca /config/openvpn/keys/ca.crt           #CA certificate
cert /config/openvpn/keys/client.crt     #Client certificate
key /config/openvpn/keys/client.key      #Private key of the client
verb 3                                   #Log level
```

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.