Yealink

Yealink Technical White Paper

Virtual Private Network

Oct. 2013

Contents

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 to create 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 base or carrier protocol, then transmitted between VPN client and 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

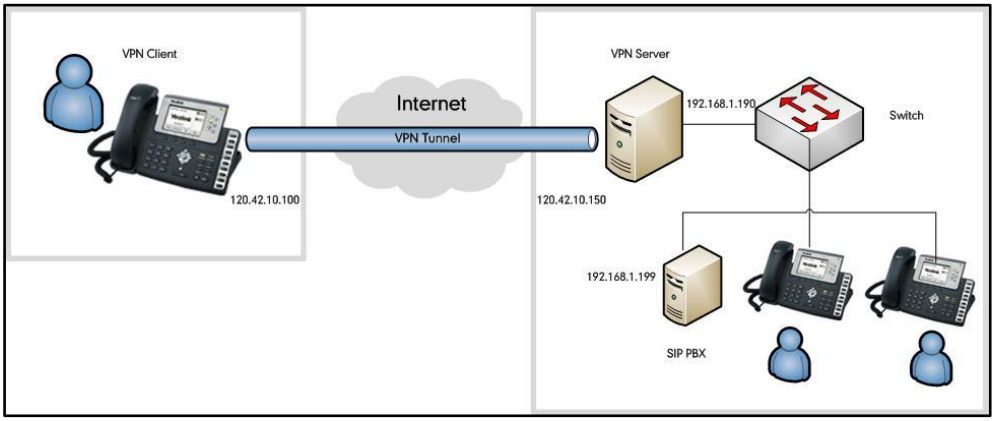
SSL VPN uses SSL protocol, Transport Layer Security (TLS), to provide a secure connection between remote users and internal network resources. It can be used with a standard web browser, and does not require the installation of specialized client software on the end user's device. An SSL VPN offers versatility, 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 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 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 found 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 of 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 120.46.10.100 and destination address 120.46.10.150.
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 source address 192.168.1.199 and destination address 192.168.1.192. The outer VPN packet has source address 120.46.10.150 and destination address 120.46.10.100.
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 with firmware version 61 or later support OpenVPN which is a full-featured SSL VPN software solution. OpenVPN is designed to work with the TUN/TAP virtual networking interface that exists on most platforms (e.g., Linux, Windows). TUN and TAP are virtual network kernel devices. 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 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 the IP phones, the IP phones act as VPN clients and use pre-shared secret keys, certificates, or username/password to authenticate the OpenVPN server.

Note OpenVPN feature is not applicable to the SIP-T19P IP phone.

Installing the OpenVPN Server

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

Before using the OpenVPN feature on the 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 instructions on how to install and configure the OpenVPN server and create the OpenVPN Tar file on Linux and Windows platforms.

Installing and configure the OpenVPN Server on the Linux Platform

The OpenVPN server software is available for free. You can download it for your OS platform at: http://openvpn.net/index.php/open-source/downloads.html. The section provides you instructions on how to install the OpenVPN server (e.g., openvpn-2.1.4.tar.gz) on the Linux platform.

Before the installation, make sure the system meets the following requirements:

- Dual network cards on the system
- Make sure the system kernel has support for the Universal TUN/TAP device driver and the TUN/TAP module is loaded into the kernel. (For more information, contact your system administrator or refer to the network resource)
- Install the required modules (e.g., OpenSSL and LZO. For more information, contact your system administrator or refer to the network resource)

To install the OpenVPN server on the Linux platform:

1. Open up a terminal window.
2. Extract the installation package.

   [root@loacalhost~]# tar zvxf openvpn-2.1.4.tar.gz
3. Enter into the extracting directory.

   [root@loacalhost~]# cd openvpn-2.1.4
4. Enter the following command 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 commond ./configure.

   ./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 configure the OpenVPN server:

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

   [root@localhost ~]# cd 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 interface prompts the following information (if you do 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 certificates for the OpenVPN server.

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

The interface prompts the following information (if you do 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 certificates for the client.

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

The interface prompts the following information (if you do 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 interface prompts the following information:

   ```
   Generating DH parameters, 1024 bit long safe prime, generator 2
   This is going to take a long time
   ```

All the certificate files are generated in the keys directory.

To configure the server's configuration file:

1. Create a new folder (e.g., openvpn) located in the path /etc.

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

2. Create a new folder (e.g., keys) located in the path /etc/openvpn.

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

3. Enter into the installation directory.
4. Copy the certificate files required for the server to the folder (e.g, 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 folder to the folder (e.g,

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.

   The following shows an example of configuring the IP address, protocol and port of the server:

   local 218.107.220.201

   port 1194

   proto udp

   The following shows an example of configuring the VPN mode and network segments for the VPN clients:

   dev tun

   server 10.8.0.0 255.255.255.0

7. Save the change.

According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature and the network connection mode (bridge mode or route mode) between the VPN clients and the Intranet. For more information, contact your network administrator.

To start the OpenVPN service:

1. Enter into the installation directory.
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 the use of certificates to help establish the authenticity of clients connecting to an OpenVPN server. The system generates a file consists of the certificates, secret keys and the configuration file of VPN client. You need to obtain the files: ca.crt, client.crt, client.key and client.conf from the system, and then package these files to tar format.

To configure the client's configuration file:

1. Create a new folder (e.g., client) located in the path /etc/openvpn.

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

2. Enter into the installation directory.
3. Copy the certificate files required for the client to the directory (e.g, /etc/openvpn/keys) created before.

   ```
   [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/client.crt /etc/openvpn/keys/

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

4. Copy the file "client.conf" in the sample-config-files folder to the folder (e.g, client) created above.

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

5. Edit the file "client.conf" and save the change.

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

   [root@localhost openvpn-2.1.4]# vi client.conf

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

   remote 218.107.220.201 1194 udp

   dev tun

   dev-type tun

   The directories vary between different IP phone models:

   /yealink/config/ for SIP-T2xP IP phones

   /phone/config/ for SIP-T3xG IP phones

   /config/ for SIP-T21P, SIP-T4X and VP530 IP phones

   The following shows an example of the certificate files path for SIP-T2xP IP phones:

   ca /yealink/config/openvpn/keys/ca.crt

   cert /yealink/config/openvpn/keys/client.crt

   key /yealink/config/openvpn/keys/client.key

   The following shows an example of the certificates files path for SIP-T4X IP phones:

   ca /config/openvpn/keys/ca.crt

   cert /config/openvpn/keys/client.crt

   key /config/openvpn/keys/client.key

Packaging the Tar File on the Linux Platform

You can package the tar file on the Windows or Linux platform. The following section will guide you with step-by-step instructions on how to package the tar file on the Linux platform.

To package the tar file on the Linux platform:

1. Enter the following command 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 configure the OpenVPN Server on the Windows Platform

The OpenVPN server software is available for free. You can download it for your OS platform at: http://openvpn.net/index.php/open-source/downloads.html. The following will provide you instructions on how to install the OpenVPN server (e.g., openvpn-2.2.2-install.exe) on the Windows platform.

Before the installation, make sure the system meets the following requirement:

- Dual network cards on the system

To install the OpenVPN server on the Windows platform:

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

To configure the OpenVPN server:

1. Enter into the installation directory.
2. Rename the file vars.bat.sample to vars.bat in the easy-rsa folder.
3. Open the file vars.bat 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
4. Rename the file opensl.cnf.sample to openssl.cnf in the easy-rsa folder.
5. Open up a command prompt interface.
6. Enter into the installation directory.

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

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

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

8. Generate a CA certificate.

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

   The interface prompts the following information (if you do 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) []:

   Email Address [admin@yealink.com]:

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

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

   The interface 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

10. Generate certificates for the OpenVPN server.

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

    The interface prompts the following information (if you do 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) []:

Email Address [admin@yealink.com]:

11. Generate certificates for the client.

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

The interface prompts the following information (if you do 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) []:
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 []:yealink
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:'EMB'
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 into the installation directory.
2. Copy the file "server.ovpn" in the sample-config folder to the config folder.
3. Edit the file "server.ovpn" according to your actual network environment.

   The following shows an example of configuring the IP address, protocol and port of the server:

   ```
   local 218.107.220.201
   port 1194
   proto udp
   ```

   The following shows an example of configuring the VPN mode and network segments for the VPN clients:

   ```
   dev tun
   ```

server 10.8.0.0 255.255.255.0

4. Save the change.

According to the actual network environment, configure the network settings of the server, such as the TCP/IP forwarding feature and the network connection mode (bridge mode or route mode) between the VPN clients and the Intranet. For more information, contact your network administrator.

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. The following section will guide you with step-by-step instructions on how to package the tar file using 7-Zip on the Windows platform. 7-Zip is available on http://www.7-zip.org/. For more information on how to package the tar file using GnuWin32, refer to http://gnuwin32.sourceforge.net/packages/gtar.htm.

To configure the client's configuration file:

1. Create a new directory (e.g., openvpn).
2. Copy the file client.ovpn to the openvpn directory.
3. Rename the file client.ovpn to vpn.cnf.
4. Create a new folder (e.g., keys) in the openvpn directory.
5. Copy the client file, ca.crt, client.crt and client.key to the new created folder.
6. Edit the file vpn.cnf.

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

   remote 218.107.220.201 1194 udp

   dev tun

   dev-type tun

   The directories vary between different IP phone models:

   /yealink/config/ for SIP-T2xP IP phones

   /phone/config/ for SIP-T3xG IP phones

   /config/ for SIP-T21P, SIP-T4X and VP530 IP phones

   The following shows an example of the certificates files path for SIP-T2xP IP phones:

   ca /yealink/config/openvpn/keys/ca.crt

   cert /yealink/config/openvpn/keys/client.crt

   key /yealink/config/openvpn/keys/client.key

   The following shows an example of the certificates files path for SIP-T4X IP phones:

   ca /config/openvpn/keys/ca.crt

cert /config/openvpn/keys/client.crt

key /config/openvpn/keys/client.key

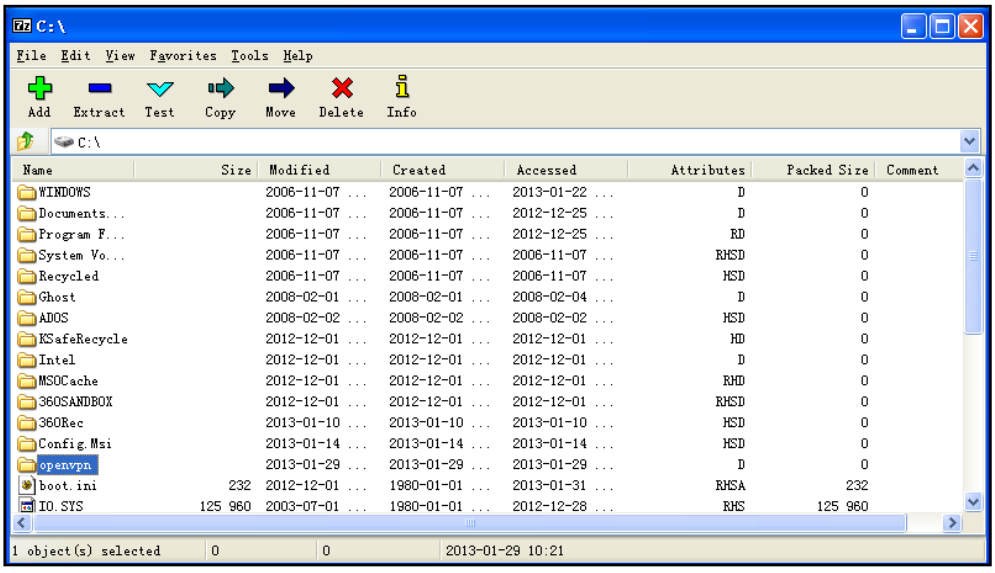
The following figure shows a portion of the vpn.cnf file for SIP-T2xP IP phones:

```
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 /yealink/config/openvpn/keys/ca.crt
cert /yealink/config/openvpn/keys/client.crt
key /yealink/config/openvpn/keys/client.key
```

7. Save the change.

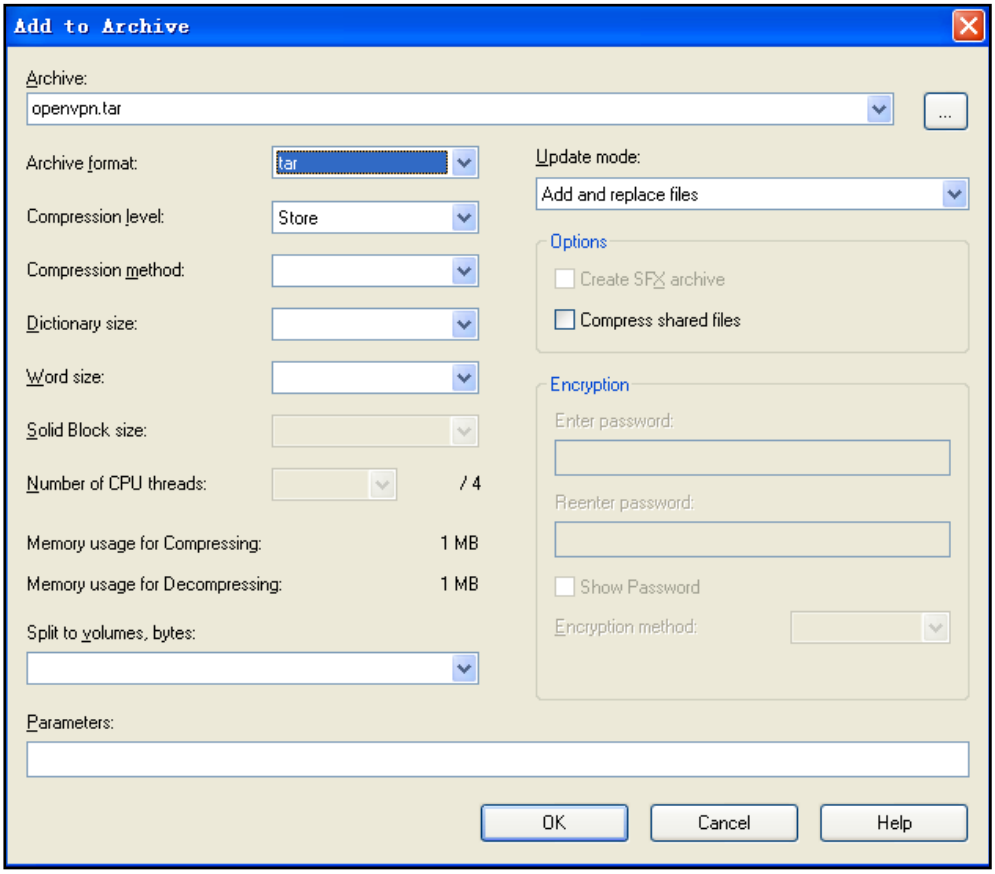
To package a tar file using the tool 7-Zip on the Windows platform:

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

Configuring the OpenVPN Feature on the IP Phones

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

Note The configuration files of VPN client for different phone models may be a little different, please upload the suitable tar file to the IP phone.

To configure the OpenVPN feature using the configuration files:

1. Set the following parameters:

Parameter	Description	Valid Value	Default Value
network.vpn_enable	Enables or disables the VPN feature on the	Boolean	0

Parameter	Description	Valid Value	Default Value
	IP phone. **0**-Disable **1**-Enable		
openvpn.url	Specifies the access URL of the OpenVPN tar file.	URL	Blank

2. Store the configuration files to the root directory of the configuration server.

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

network.vpn_enable = 1

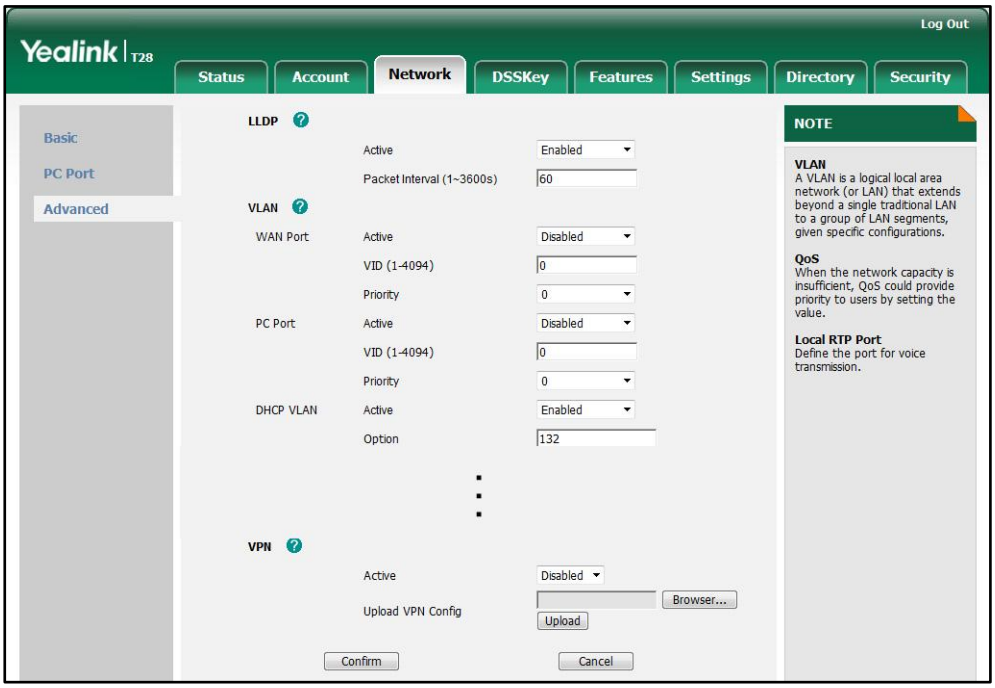
openvpn.url = http://192.168.1.20/openvpn.tar

To configure the OpenVPN feature via web user interface (take T28P as an example):

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 **Enter**.
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. Click **Browse** to locate the OpenVPN tar file from the local system.

6. Click **Upload** to upload the tar file.



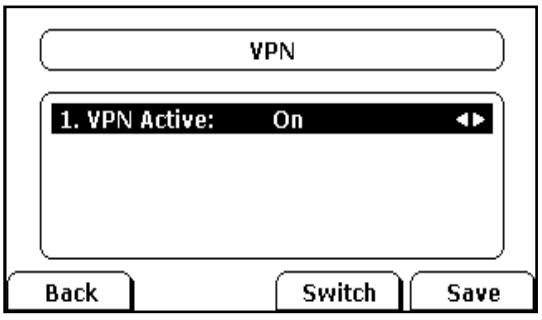
7. Select **Enabled** from the pull-down list of **VPN Active**.
8. Click **Confirm** to accept the change.

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

To configure the OpenVPN feature via phone user interface (take T28P as an example):

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

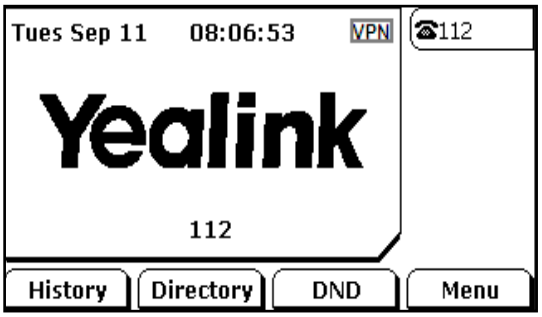
   You should upload the OpenVPN tar file using the configuration file or via the web user interface.



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

   The IP phone reboots automatically to make the settings effective.

After successfully configuring the OpenVPN feature, 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.



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.

Customer Feedback

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