关于 VPN

VPN（虚拟专用网络）通过使用公共电信基础设施（如：互联网），为远程办公和旅行用户提供企业核心网络的安全访问。VPN 的优势在于为企业创造安全通信渠道，同时节省开支，提高安全性和提升性能。

VPN 访问有两种类型：远程访问和站点到站点的访问。

VPN 访问的类型

远程访问 VPN，也称为虚拟专用拨号网（VPDN），是指用户到局域网的连接，用于企业内员工需要从不同的远程位置连接到专用网络。

站点到站点 VPN 连接整个网络，具体指的是，站点到站点 VPN 可以用来连接分支机构或远程办公网络到企业总部网络。每个站点都配置一个 VPN 网关（如：路由器、防火墙、VPN 集中器或安全设备）。

VPN 技术

VPN 技术是基于隧道的概念。VPN 隧道包括建立和维护逻辑网络连接（可能包含中间跳点）。在连接中，特定 VPN 协议格式中的数据包被封装在一些其他的基础协议或运营商协议中，然后在 VPN 客户端和服务器之间传输，并最终在接收方解封。

一些计算机网络协议专门用于 VPN 隧道。其中最流行的两种 VPN 隧道协议为 SSL（安全套接字协议）和 IPSec (互联网安全协议)。

SSL VPN

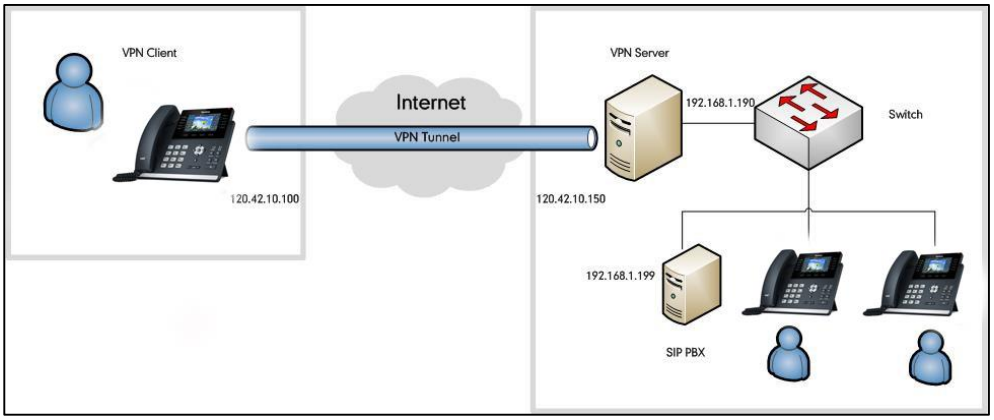
SSL VPN 使用 SSL 协议和传输层安全性协议（TLS）来提供远程用户和内部网络资源之间的安全连接。它可与标准网页浏览器一起使用，并不需要在终端用户设备上安装特定的客户端软件。SSL VPN 提供了通用性、易用性、针对不同设备的用户范围的粒度控制和从多个位置访问资源的优势。

IPSec VPN

IPSec VPN 使用标准的 IPSec 机制在公网上建立 VPN 连接。IPSec 是用于网络通信的网络或数据包层面安全的协议框架。建立连接前，IPSec VPN 需要在客户设备上安装 IPSec 客户端软件。IPSec 可以满足大多数安全目标：身份验证、整合性和保密性。

VPN 隧道使用示例

一位职员拥有一部 IP 话机（其公网 IP 地址为 120.42.10.100），并想连接到企业网络内的 SIP 服务器。该 SIP 服务器带有一个内网 IP 地址（192.168.1.199），且无法被公开访问。在访问该服务器之前，IP 话机需要通过一个同时具有公网 IP 地址（120.42.10.100）和内网 IP 地址（192.168.1.190）的 VPN 服务器。IP 话机和 SIP 服务器之间的所有数据将需要保密，因而需要使用安全的 VPN。



下列步骤介绍了 VPN 客户端-服务器交互原理：

1. VPN 客户端通过外部网络接口连接 VPN 服务器。
2. VPN 服务器从 VPN 服务器子网分配一个 IP 地址给 VPN 客户端。例如，客户端获得一个内网 IP 地址 192.168.1.192，并创建一个虚拟网络接口，通过该接口发送加密的数据包给隧道对端的终端。
3. 当 VPN 客户端想要与 SIP 服务器通信，它准备了一个地址为 192.168.1.199 的数据包并将其加密和封装到一个外部 VPN 数据包中。然后该数据包被发送到公网上 IP 地址为 120.42.10.150 的 VPN 服务器。内部数据包被加密，因而如果有人想从网络上截获该数据包，他们无法从中获取到任何信息。内部加密的数据包带有来源地址 192.168.1.192 和目的地址 192.168.1.199。外部数据包带有来源地址 120.42.10.100 和目的地址 120.42.10.150。
4. 当数据包从网络上访问 VPN 服务器，VPN 服务器将内部数据包解封、解密，发现目的地址为 192.168.1.199，并将其发送给目标 SIP 服务器（192.168.1.199）。
5. 一段时间后，VPN 服务器收到来自 192.168.1.199 的应答包，该应答包用于 192.168.1.192。VPN 服务器查阅其路由表并知道其数据包用于必须通过 VPN 的远程设备（IP 话机）。
6. VPN 服务器加密该应答包，并将其封装到 VPN 数据包中，通过网络发送出去。内部加密

数据包带有来源地址 192.168.1.199 和目的地址 192.168.1.192。外部 VPN 数据包带有来源地址 120.42.10.150 和目的地址 120.42.10.100。

7. VPN 客户端接收并解封数据包，将其解密并传递给上一层。

Yealink IP 话机兼容 VPN

Yealink IP 话机支持 OpenVPN 功能。OpenVPN 是远程访问 VPN，用于搭配大多数平台（如：Linux，Windows）上的 TUN/TAP 虚拟网络接口使用。TAP 模拟以太网设备并搭配第二层数据包（如：帧）进行操作。TUN 模拟网络层设备并搭配第三层数据包（如：IP 数据包）进行操作。

OpenVPN 作为客户端-服务器应用程序运行。在 IP 话机上启用 OpenVPN 功能后，IP 话机作为 VPN 客户端使用预先共享的密钥、证书或用户名/密码来验证 OpenVPN 服务器。

安装 OpenVPN 服务器

OpenVPN 服务器是一组用来简化 VPN 远程访问解决方案快速部署的安装和配置工具。它支持 Linux、Windows、MAC 平台上使用。

在 IP 话机上使用 OpenVPN 功能之前，你必须确保 OpenVPN 服务器已准备就绪。否则，你需要安装和配置 OpenVPN 服务器。本章节介绍如何安装和配置 OpenVPN 服务器和在 Linux 和 Windows 平台上创建 OpenVPN TAR 文件。

Linux 平台

安装和配置 OpenVPN 服务器

OpenVPN 服务器是免费提供的。本章节介绍如何在 Linux 平台（如：Centos 5.8 和内核: 2.6.18-308.el5-i686）安装 OpenVPN 服务器（如：openvpn-2.1.4.tar.gz）。

在安装前，确保硬件和系统满足以下条件：

- 双网卡。
- 系统内核支持 Universal TUN/TAP 设备驱动程序（内核 2.6.0 以上）且将 TUN/TAP 模块加载到内核中。
- 安装所需的 “OpenSSL and LZO” 模块。

检查 TUN/TAP 模块是否已加载到内核中：

1. 打开终端窗口。
2. 输入下列命令。
   [root@localhost~]# cat /dev/net/tun

- 如果返回的信息为“cat: /dev/net/tun: File descriptor in bad state”，意味着 TUN/TAP 模块已经添加到内核中。

- 如果返回的信息为“cat: /dev/net/tun: No such device”，你需要执行下列命令来加载 TUN/TAP 模块。
  [root@localhost~]# cd /usr/src/kernels/2.6.18-308.el5-i686/
  [root@localhost 2.6.18-308.el5-i686]# make menuconfig

  在弹出的配置页面，选择 **Device Drivers->Network device support->Universal TUN/TAP device driver support** 并设置 **Universal TUN/TAP device driver support** 为 **M**。

你可以在线下载 OpenSSL 模块，下载链接为：http://www.openssl.org/。以下操作以“openssl-1.0.0e.tar.gz”为例。下载并保存到根目录中。

安装 OpenSSL 模块：

1. 打开终端窗口。
2. 提取安装包到 /etc 目录。
   [root@localhost~]# cd /etc/
   [root@localhost etc]# tar zvxf /openssl-1.0.0e.tar.gz
3. 进入提取目录。
   [root@localhost etc]# cd openssl-1.0.0e
4. 输入下列命令来安装安装包。
   [root@localhost openssl-1.0.0e]# ./config
   [root@localhost openssl-1.0.0e]# make
   [root@localhost openssl-1.0.0e]# make install

你可以在线下载 LZO 模块，下载链接为：http://www.oberhumer.com/opensource/lzo/download/。以下操作以“lzo-2.02.tar.gz”为例。下载并保存到根目录中。

安装 LZO 模块：

1. 打开终端窗口。
2. 提取安装包到 /etc 目录。
   [root@localhost~]# cd /etc/
   [root@localhost etc]# tar zvxf /lzo-2.02.tar.gz
3. 进入提取目录。
   [root@localhost etc]# cd lzo-2.02
4. 输入下列命令来安装安装包。
   [root@localhost lzo-2.02]# ./configure
   [root@localhost lzo-2.02]# make
   [root@localhost lzo-2.02]# make install

你可以在线下载 OpenVPN 软件，下载链接为：
http://openvpn.net/index.php/open-source/downloads.html。下载并保存到根目录中。

安装 OpenVPN 服务器：

1. 打开终端窗口。
2. 提取安装包到 /etc 目录。
   [root@localhost~]# cd /etc/
   [root@localhost etc]# tar zvxf /openvpn-2.1.4.tar.gz
3. 进入提取目录。
   [root@localhost etc]# cd openvpn-2.1.4
4. 输入下列命令来安装安装包。
   [root@localhost openvpn-2.1.4]# ./configure
   [root@localhost openvpn-2.1.4]# make
   [root@localhost openvpn-2.1.4]# make install

   如果没有找到头文件（header）和库文件（library files），你需要使用下列命令来代替上述的“./configure”命令。

   ./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. 添加 OpenVPN 服务。
   [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

为 OpenVPN 服务器和 IP 话机生成证书文件：

1. 进入用于生成证书文件的目录（不同版本间可能会不同）。
   [root@localhost ~]# cd /etc/openvpn-2.1.4/easy-rsa/2.0
2. 输入下列命令。
   [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. 生成 CA 证书。
   [root@localhost 2.0]# ./clean-all
   [root@localhost easy-rsa]# ./build-ca

   页面提示下列信息（如果你不想更改默认设置，按 **ENTER** 键，输入所需值，再次按 **ENTER** 键）：

   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. 为 OpenVPN 服务器生成证书。
[root@localhost 2.0]# ./build-key-server server

页面提示下列信息（如果你不想更改默认设置，按 **ENTER** 键，输入所需值，再次按 **ENTER** 键）：

Generating a 1024 bit RSA private key
.....++++++
...++++++
writing the 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. 为客户端生成证书。

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

   页面提示下列信息（如果你不想更改默认设置，按 **ENTER** 键，输入所需值，再次按 **ENTER** 键）：

```
Generating a 1024 bit RSA private key
.....................................................++++++
....++++++
writing the 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. 为服务器生成 dh1024.pem 文件。

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

页面提示下列信息：

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

如果页面提示“./build-dh: line 7: dhparam: command not found”，你需要编辑文件“build-dh” in the /etc/openvpn-2.1.4/easy-rsa/2.0 directory. Set “$OPENSSL” 为“openssl”并保存该文件。

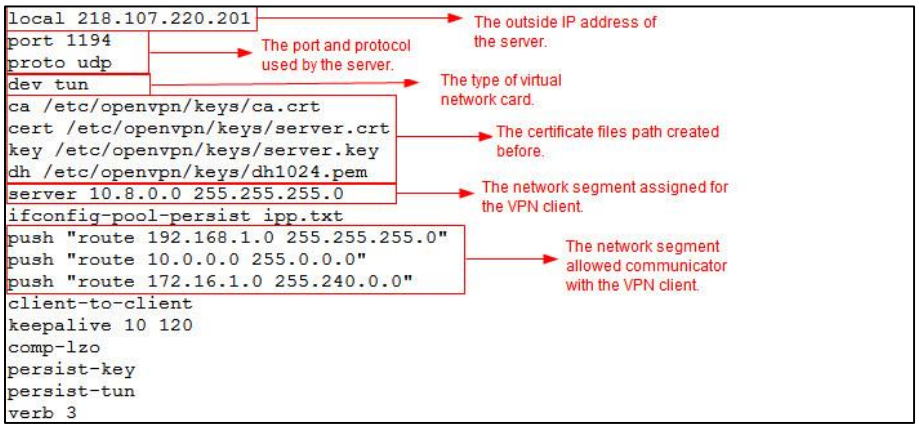
所有证书文件都生成在目录“/openvpn-2.1.4/easy-rsa/2.0/keys”下。

配置服务器的配置文件：

1. 在路径 /etc 下创建新目录“openvpn”。
   [root@localhost ~]# mkdir /etc/openvpn
2. 在路径 /etc/openvpn 下创建新目录 ”keys”。
   [root@localhost ~]# mkdir /etc/openvpn/keys
3. 进入 OpenVPN 服务器安装目录。
   [root@localhost ~]# cd /etc/openvpn-2.1.4
4. 为上述创建的目录 ”keys” 复制所需的证书文件。
   [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. 复制 sample-config-files 目录下的“server.conf”文件到上述创建的目录“openvpn”。
   [root@localhost openvpn-2.1.4]# cp sample-config-files/server.conf /etc/openvpn
6. 根据你的实际网络环境编辑“server.conf”文件，并保存更改。
   [root@localhost ~]# vi /etc/openvpn/server.conf

   按“**I**”键进入 Insert Mode，修改所需参数，按“**Esc**”键返回 Command Mode 并输入“**wq!**”。

   示例如下：



根据实际网络环境，配置服务器的网络设置，如 TCP/IP 转发功能和在 VPN 客户端和内部网之间的路由条目。更多信息请联系你的网络管理员。

启用 TCP/IP 转发：

1. 打开终端窗口。
2. 编辑 /etc 目录下的“sysctl.conf”文件，并保存更改。
   [root@localhost ~]# vi /etc/sysctl.conf

   按“**I**”键进入 Insert Mode，设置“**net.ipv4.ip_forward**”值为 1，按“**Esc**”键返回 Command Mode 并输入“**wq!**”。

启用 OpenVPN 服务：

1. 进入 OpenVPN 服务器的安装目录。
   [root@localhost ~]# cd /etc/openvpn-2.1.4
2. 启用 OpenVPN 服务。
   [root@localhost openvpn-2.1.4]# service openvpn start

为 VPN 客户端创建 OpenVPN TAR 文件

OpenVPN 需要使用证书来帮助创建连接到 OpenVPN 服务器的客户端认证。你需要从系统中获取文件：ca.crt，client.crt，client.key 和 vpn.cnf，并打包这些文件为 TAR 格式。

配置客户端配置文件：

1. 在路径 /etc/openvpn 下创建新目录 ”client”。
   [root@localhost ~]# mkdir /etc/openvpn/client
2. 在路径 /etc/openvpn/client 下创建新目录 ”keys”。
   [root@localhost ~]# mkdir /etc/openvpn/client/keys
3. 进入 OpenVPN 服务器安装目录。
   [root@localhost ~]# cd /etc/openvpn-2.1.4
4. 为客户端复制所需证书文件到之前创建的“/etc/openvpn/client/keys”目录。
   [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. 复制 sample-config-files 目录下的“client.conf”文件到上述创建的“client”目录，并重命名该文件为 vpn.cnf。
   [root@localhost openvpn-2.1.4]# cp sample-config-files/client.conf /etc/openvpn/client/vpn.cnf
6. 编辑“vpn.cnf”文件并保存更改。
   [root@localhost openvpn-2.1.4]# cd /etc/openvpn/client
   [root@localhost client]# vi vpn.cnf

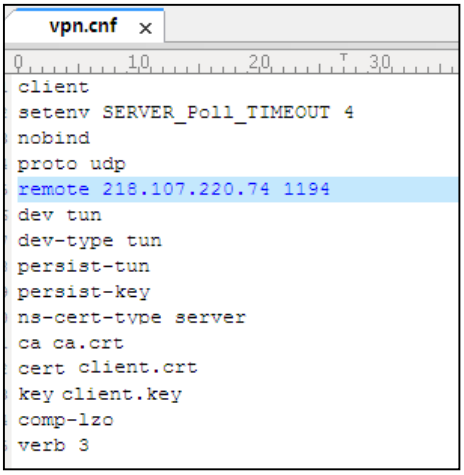
   按“**I**”键进入 Insert Mode，修改所需参数，按“**Esc**”键返回 Command Mode 并输入“**wq!**”。

   下列参数需要配置为与服务器的参数一致。
   remote 218.107.220.201 1194 udp
   dev tun
   dev-type tun

   以下定义了为 Yealink IP 话机配置 OpenVPN 证书和密钥：

```
ca ca.crt
cert client.crt
key client.key
```

下图显示 vpn.cnf 文件的一部分作为示例：



在 Linux 平台上打包 TAR 文件：

1. 输入下列命令来打包 TAR 文件。
   [root@localhost ~]# cd /etc/openvpn/client
   [root@localhost client]# tar -cvpf openvpn.tar *

   openvpn.tar 文件在 client 目录下生成。

Windows 平台

安装和配置 OpenVPN 服务器

OpenVPN 服务器是免费提供的。你可以为你的 Windows 平台在线下载 OpenVPN 服务器。

本章节介绍如何在 Windows XP 平台安装 OpenVPN 服务器（如：openvpn-2.1.1-install.exe）。

在安装前，确保硬件和系统满足以下条件：

- 双网卡。
- 系统内核支持 TUN/TAP 模块。

在 Windows XP 平台安装 OpenVPN 服务器：

1. 在本地系统双击安装文件。
2. 根据提示完成安装。

   默认安装目录为 C:\Program Files\OpenVPN\。

为 Open VPN 服务器和 IP 话机生成证明文件：

1. 进入 OpenVPN 服务器的安装目录。
2. 打开 easy-rsa 文件夹的 vars.bat 文件，并编辑下列参数：
   set KEY_COUNTRY=US
   set KEY_PROVINCE=CA

set KEY_CITY=SanFrancisco
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@host.domain

以下为配置参数示例：
set KEY_COUNTRY=CN
set KEY_PROVINCE=FJ
set KEY_CITY=XM
set KEY_ORG=Yealink
set KEY_EMAIL=admin@yealink.com

3. 点击 **Start**->**Run**。
4. 在弹出的对话框中输入 **cmd**，点击 **OK** 打开指令提示页面。
5. 进入 OpenVPN 服务器安装目录下的 easy-rsa 目录。
   C:\Documents and Settings\Administrator>cd \Program Files\OpenVPN\easy-rsa
6. 输入下列指令。
   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. 生成 CA 证书。
   C:\Program Files\OpenVPN\easy-rsa>build-ca.bat

   页面提示下列信息（如果你不想更改默认设置，按 **ENTER** 键，输入所需值，再次按 **ENTER** 键）：

   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. 为服务器生成 dh1024.pem 文件。
   C:\Program Files\OpenVPN\easy-rsa>build-dh.bat

   页面提示下列信息：

   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. 为 Open VPN 服务器生成证书。

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

页面提示下列信息（如果你不想更改默认设置，按 **ENTER** 键，输入所需值，再次按 **ENTER** 键）：

```
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. 为客户端生成证书。

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

页面提示下列信息（如果你不想更改默认设置，按 **ENTER** 键，输入所需值，再次按 **ENTER** 键）：

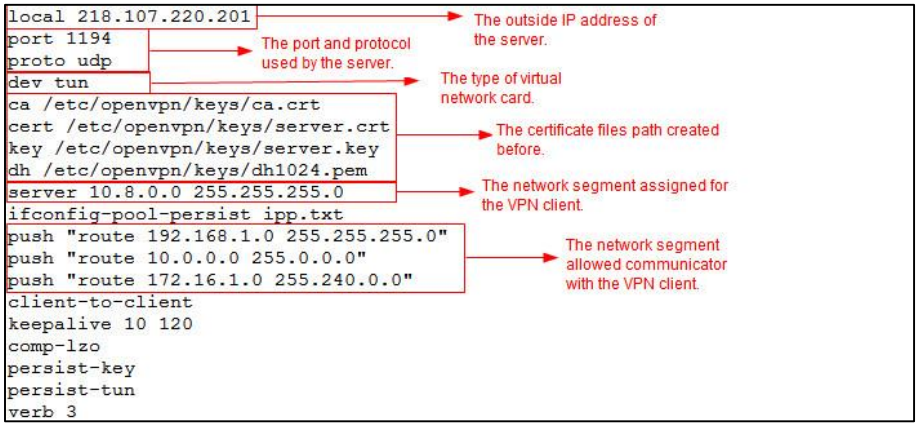
```
Loading 'screen' into random state - done
```

```
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
```

配置服务器配置文件：

1. 进入 Open VPN 服务器安装目录。
2. 在目录中创建新文件夹 “serverconfig”。
3. 复制 sample-config 文件夹中 “server.ovpn” 文件到上述创建的 serverconfig 文件夹。
4. 根据你的实际网络环境编辑 “server.ovpn” 文件并保存更改。

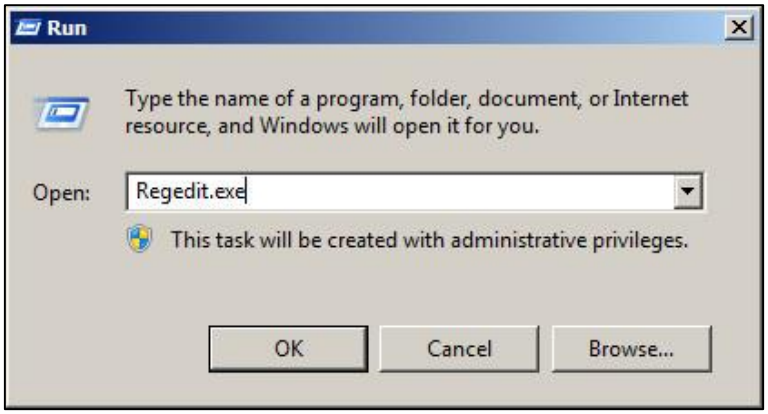
示例如下：



根据实际网络环境，配置服务器的网络设置，如 TCP/IP 转发功能、网络连接共享功能和在 VPN 客户端和内部网之间的路由条目。更多信息请联系你的网络管理员。

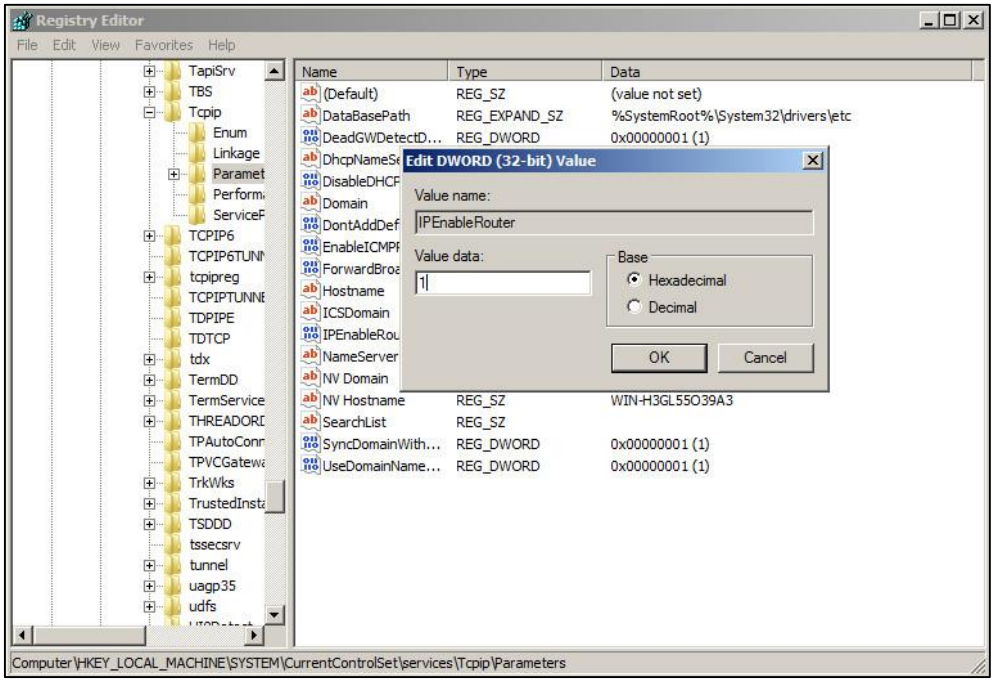
启用 TCP/IP 转发：

1. 点击 **Start->Run**。
2. 在弹出的对话框中输入 **Regedit.exe** 并点击 **OK**。



3. 点击 **HKEY_LOCAL_MACHINE->SYSTEM->CurrentControlSet->Services->Tcpip->Parameters**。

4. 设置 “**IPEnableRouter**” 值为 1。



启用内部网卡网络连接共享:

1. 打开网络连接。
2. 右键单击内部网卡局域网，选择 **Properties**。
3. 在 **Advanced** 选项卡，选中 **Allow other network users to connect through this computer's Internet connection** 复选框。
4. 在 **Home networking connection** 下拉框选择服务器虚拟网卡。
5. 点击 **OK** 保存更改。

为 VPN 客户端创建 OpenVPN Tar 文件

你可以使用工具 7-Zip 或 GnuWin32 在 Windows 平台打包 TAR 文件。你可以在线下载工具 7-Zip，下载地址为：http://www.7-zip.org/；或在线下载工具 GnuWin32，下载地址为：http://gnuwin32.sourceforge.net/packages/gtar.htm。

本章节介绍如何在 Windows XP 平台使用工具 7-Zip 打包 TAR 文件。

配置客户端配置文件：

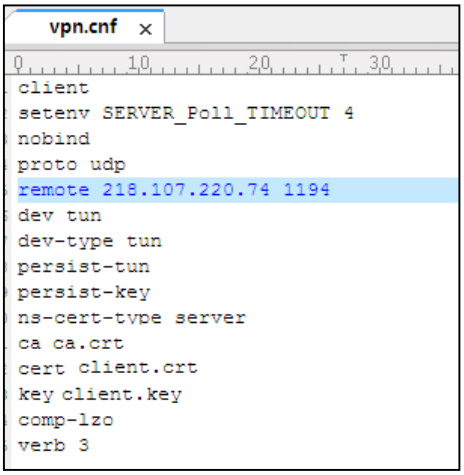
1. 在目录 C:/ 创建新文件 “openvpn”。
2. 复制 sample-config 文件夹中 client.ovpn 文件到 openvpn 文件夹。
3. 重命名 client.ovpn 文件为 vpn.cnf。
4. 在 openvpn 文件夹创建新文件夹 “keys”。
5. 复制 ca.crt、client.crt 和 client.key 文件到上述创建的 keys 文件夹。

6. 编辑文件 vpn.cnf。

   下列参数需要配置为与服务器的参数一致。
   remote 218.107.220.201 1194 udp
   dev tun
   dev-type tun

   以下为 Yealink IP 话机定义 OpenVPN 证书和密钥：
   ca ca.crt
   cert client.crt
   key client.key

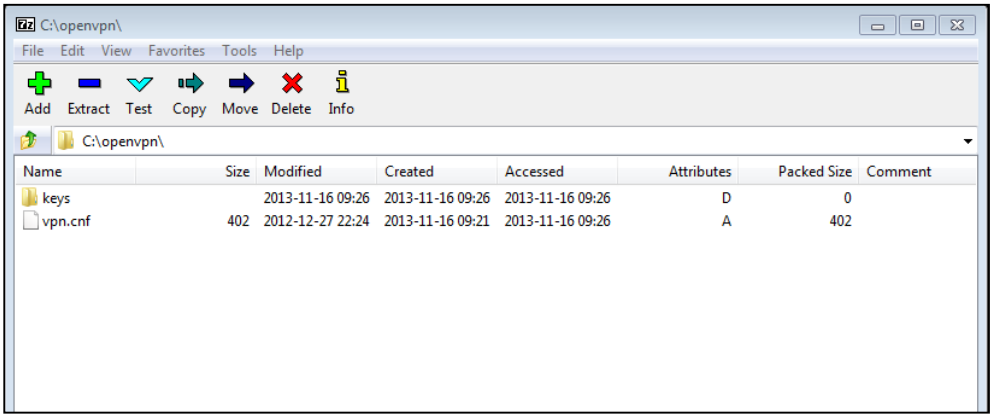
   下图显示 vpn.cnf 文件的一部分作为示例：



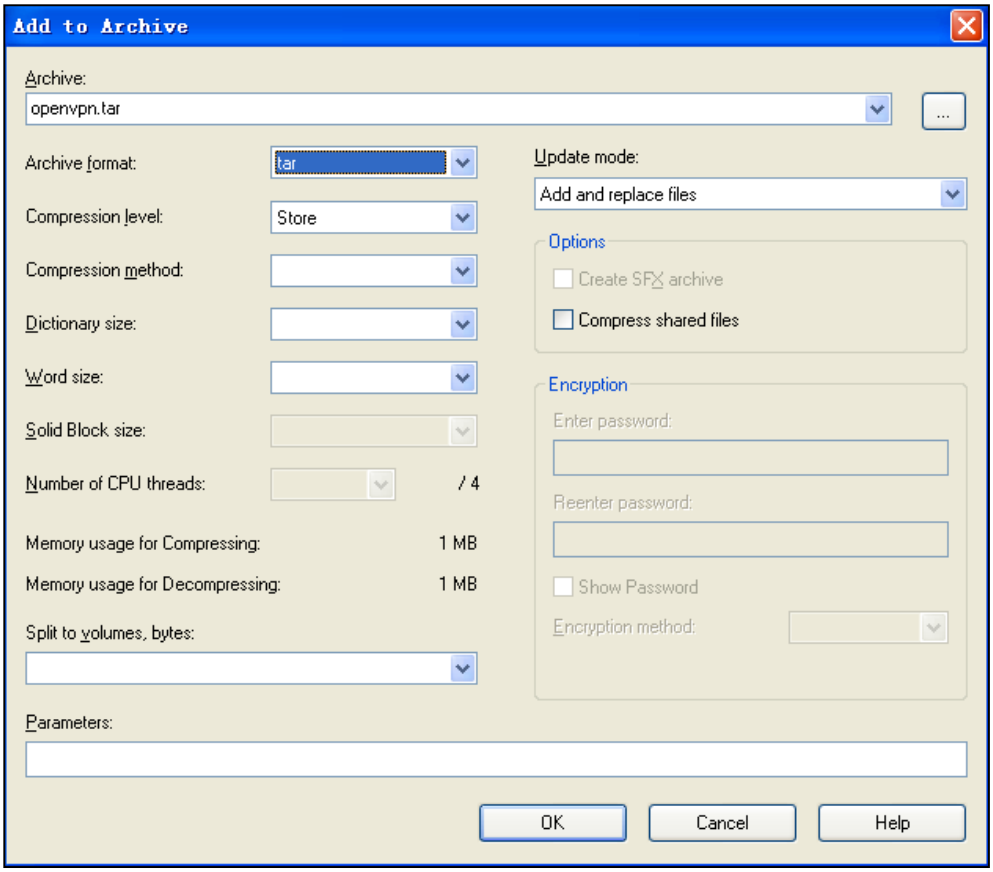
7. 保存更改。

在 Windows 平台使用工具 7-Zip 打包 TAR 文件：

1. 在本地系统下载和安装 7-Zip。
2. 启动 7-Zip 文件管理器应用程序。
3. 从本地系统找到 openvpn 文件夹。



4. 点击 **Add**。
5. 在 **Archive format** 下拉框中选择 **tar**。



6. 点击 **OK**。

   openvpn.tar 文件在 C:/openvpn 目录下生成。

在 IP 话机上配置 OpenVPN 功能

IP 话机默认禁用 OpenVPN 功能。你可以使用配置文件、在网页端用户页面或话机端用户页面启用 OpenVPN 功能。要使用 OpenVPN 功能，你还需要上传 OpenVPN TAR 文件到 IP 话机。本章节介绍的配置操作适用于运行固件为 V85 及之后版本的 IP 话机。

使用配置文件配置 OpenVPN 功能

过程

1. 在配置文件（如：static.cfg）中添加/编辑 OpenVPN 参数。

   下列表格介绍 OpenVPN 参数：

参数	允许值	默认值
static.network.vpn_enable	**0 或 1**	**0**
描述：		

参数	允许值	默认值
启用或禁用 IP 话机的 VPN 功能。 **0**-禁用 **1**-启用 **网页端用户页面**： Network->Advanced->VPN->Active **话机端用户页面**： Menu->Settings->Advanced Settings (默认密码：admin) ->Network->VPN->VPN Active		
static.network.vpn.mode	**0 或 1**	**1**
描述： 配置 VPN 类型。 **0**-L2TP **1**-OpenVPN		
static.openvpn.url	**511 字符以内的 URL**	**空白**
描述： 指定 OpenVPN TAR 文件的访问 URL。 **网页端用户页面：** Network->Advanced->VPN->Upload VPN Config		

以下显示配置文件中配置 OpenVPN 功能示例：

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

2. 在引导文件（如：y000000000000.boot）中引用配置文件。

   例如：

   include:config “http://10.2.1.158/static.cfg”

3. 上传引导文件和配置文件到配置服务器的根目录。
4. 触发 IP 话机执行自动配置更新。

   更多关于自动配置的信息，请参阅 Yealink 技术支持上最新的自动配置指南。

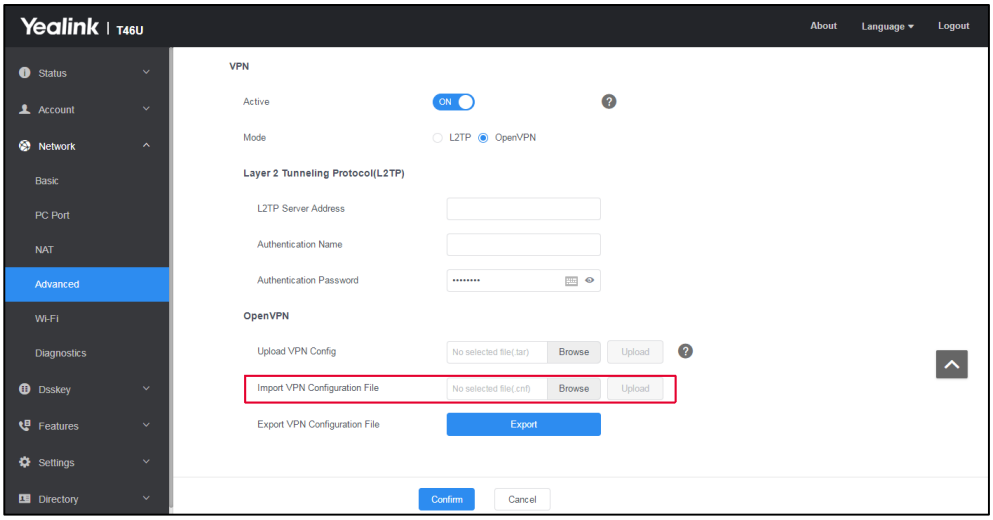
在网页端用户页面配置 OpenVPN 功能

过程

1. 按 **OK** 键，在话机空闲时获取 IP 地址。

2. 在电脑网页浏览器的地址栏输入 IP 地址（如：http://192.168.0.10 or 192.168.0.10），按 **Enter** 键。
3. 在登录页面输入用户名和密码。

   默认用户名为 admin（区分大小写），默认密码为 admin（区分大小写）。
4. 点击 **Network->Advanced**。
5. 打开 VPN 功能。
6. 在 **Mode** 区域选择 **OpenVPN**。
7. 在 **OpenVPN** 区域，点击 **Browse** 从本地系统定位 OpenVPN TAR 文件，点击 **Upload** 上传该文件。



8. 点击 **Confirm** 保存更改。

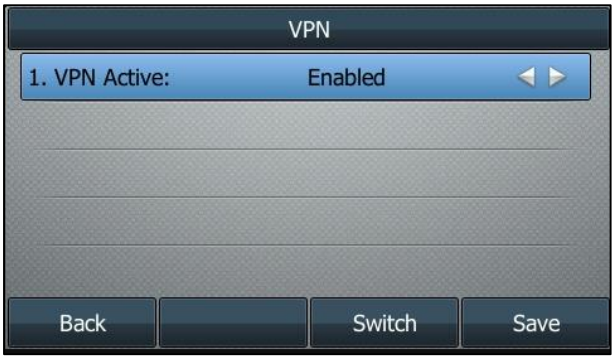
   网页端用户页面提示是否重启话机。
9. 点击 **OK**。

在话机端用户页面启用 OpenVPN 功能

过程

1. 按 **Menu->Advanced** (默认密码：admin) **->Network->VPN**。
2. 在 **VPN Active** 区域选择 **Enabled**。

   你必须提前使用配置文件或在网页端用户页面上传 OpenVPN TAR 文件。



3. 保存更改。

   话机自动重启使配置生效。

注 在话机端用户页面，你只能启用或禁用 OpenVPN 功能。

OpenVPN 功能成功配置后，话机液晶屏显示 VPN 图标。在家或办公室外，话机都能访问企业内部网络资源。

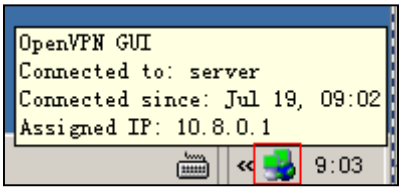
故障排除

为什么话机连接 OpenVPN 服务器失败?

按顺序进行下列操作：

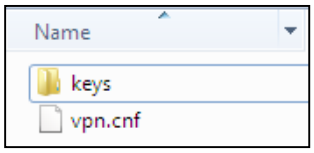
- 确保 OpenVPN 服务器已启动并运行。

  如果 OpenVPN 服务器正常运行，当你将鼠标指针放在 VPN 图标上时将出现一个分配给 OpenVPN 服务器的虚拟 IP 地址。系统托盘通知区的 VPN 图标显示如下：



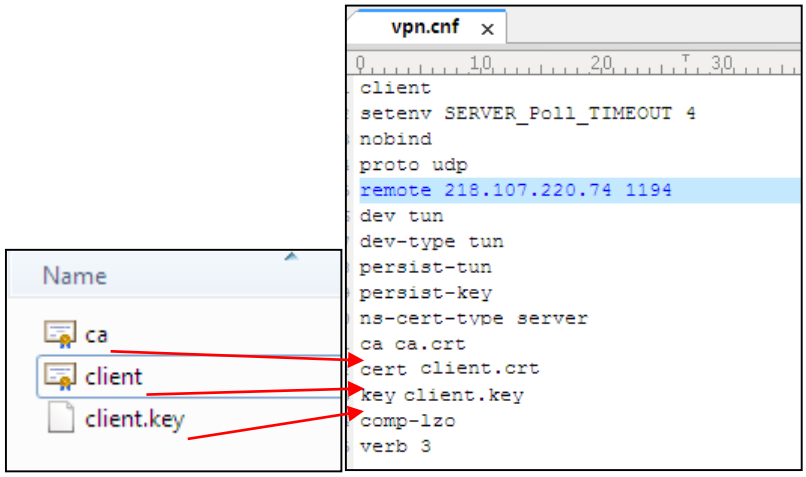
- 确保上传到 IP 话机的 OpenVPN TAR 文件创建正确。

  提取 TAR 文件并确保证书文件夹命名为“keys”，客户端配置文件命名为“vpn.cnf”，如下所示：

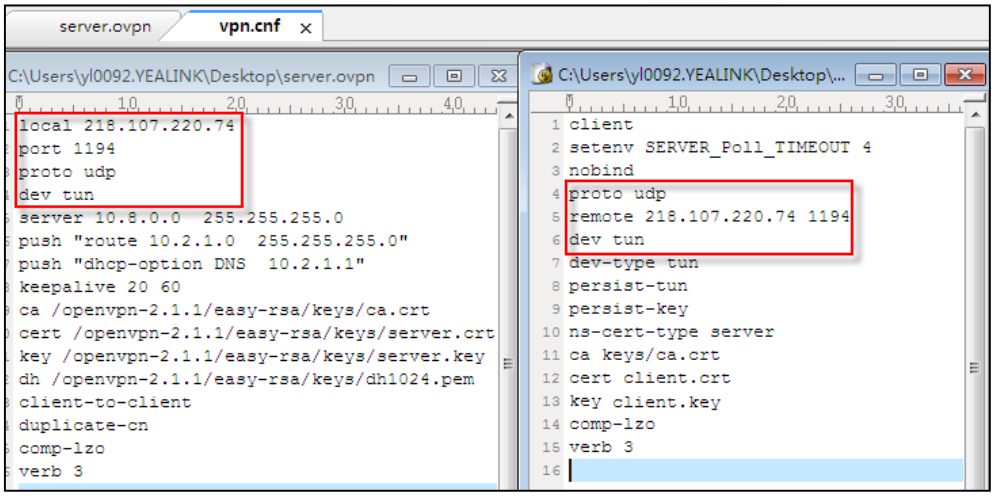


- 确保客户端证书的文件名和客户端配置文件中定义的密钥正确。

  输入目录“keys”检查客户端证书的文件名和密钥。



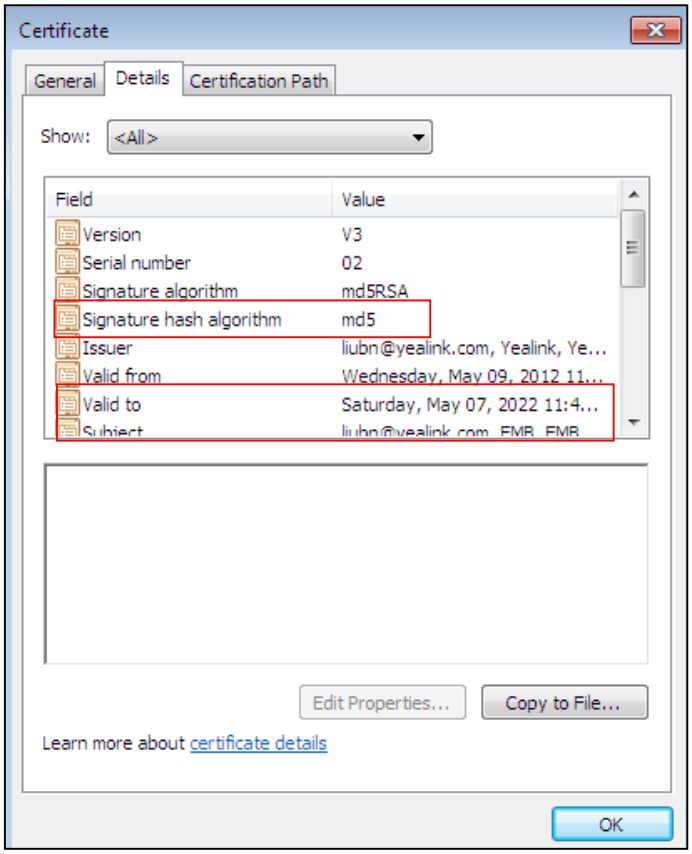
- 确保服务器配置文件和客户端配置文件的下列配置完全匹配。



- 确保话机的时间和日期在证书的有效期内。
- 检查话机是否支持客户端证书签名算法。

  IP 话机支持 MD5 和 SHA 1 签名算法。

  双击客户端证书文件检查证书的有效期和签名算法。



如何更改证书的签名算法?

如果话机不支持客户端证书的签名算法，你需要更改签名算法并再次生成客户端文件。

进行如下操作：

1. 找到 OpenVPN 安装路径下 easy-rsa 文件夹中的 openssl.cnf 文件。

   文件名和存储路径可能根据你的安装环境而不同。

2. 配置 “default_md” 参数值为 md5 或 sha1，如下所示：

   default_md = md5 或 default_md = sha1

3. 根据安装 OpenVPN 服务器章节的步骤介绍，再次生成客户端证书。

为什么话机在成功连接到 OpenVPN 服务器后注册 SIP 服务器失败?

按顺序进行下列操作：

- 确保 OpenVPN 服务器带双网卡。
- 确保 OpenVPN 服务器和 SIP 服务器通过 Ping 命令正常连接。

- 确保 Windows 平台上的 OpenVPN 服务器启用 Internet Connection Sharing 和 TCP/IP 转发。
- 确保在服务器配置文件中分配给话机访问 SIP 服务器网络段的权限。

  例如，SIP 服务器的 IP 地址为 192.168.3.6，服务器配置文件必须包含配置 **push "route 192.168.3.0 255.255.255.0"**。

为什么话机上配置 SIP 服务器域名时，话机注册失败？

按顺序进行下列操作：

- 确保已将 DNS 服务器的 IP 地址添加到服务器配置文件。

  例如，DNS 服务器的 IP 地址为 192.1682.3.10，服务器配置文件必须包含配置 **push "dhcp-option DNS 192.1682.3.10"**。
- 确保 DNS 服务器和话机正常连接。

为什么通话时没有声音？

进行下列操作：

1. 确保已将 **client-to-client** 配置添加到服务器配置文件。
2. 重启 OpenVPN 服务器。

为什么音质很差？

进行下列操作：

- 网络拥塞、RTP 丢包或延迟可能会导致呼叫质量差。在这种情况下，你需要联系你的网络管理员。
- 确保在客户端配置文件中设置适当的日志级别。

  Yealink 建议你设置日志级别为 3（客户端配置文件中的 “verb 3”）。如果日志级别设置过高，话机将会频繁记录话机事件。这可能导致话机性能问题。

术语解释

IPSec – 一种协议包，用于通过验证和加密通信会话的每个数据包来保护 IP 通信。

TLS/SSL – 在 Internet 上提供通信安全的加密协议。TLS 和 SSL 在应用层（Application Layer）为传输层（Transport Layer）加密网络连接段，使用不对称加密保证密钥交换，对称加密保证机密性，信息验证码保证信息完整性。

TAR – 文件格式（以归档比特流的形式）和用于处理这些文件的程序的名称。

预共享密钥 – 在需要使用之前，双方之间使用某种安全通道来共享的共享密钥。

7-Zip – 一个免费和开源的文件归档器。它使用 7z 归档格式操作，但是可以读写一些其他的归档格式。

GnuWin32 – 以可运行计算机程序、补丁和源代码形式为各种 GNU 和开源工具与软件提供本地端口，其中大多数修改为在 32 位的 Windows 平台运行。

配置文件示例

以下为配置文件示例，具体介绍如何配置服务器和客户端配置文件。不同的网络环境配置可能有所不同。

服务器配置文件

```
local 218.107.220.74        #VPN 服务器外网 IP 地址
port 1194                   #VPN 服务器端口
proto udp                   #VPN 服务器传输协议（udp 或 tcp）
dev tun                     #虚拟网络接口（tun 或 tap）
server 10.8.0.0   255.255.255.0          #分配给 VPN 客户端的虚拟 IP 段
push "route 10.2.1.0   255.255.255.0"    #允许 VPN 客户端访问的内网段
push "dhcp-option DNS   10.2.1.1"        #分配给 VPN 客户端的 DNS 服务器
                                          IP 地址
keepalive 20 60      #每 20 秒 Ping 一次 VPN 服务器。如果 60 秒内 Ping 没有成
                     功，重新连接 VPN 服务器。
ca /openvpn-2.1.1/easy-rsa/keys/ca.crt              #CA 证书
cert /openvpn-2.1.1/easy-rsa/keys/server.crt        #服务器证书
key /openvpn-2.1.1/easy-rsa/keys/server.key         #服务器私钥
dh /openvpn-2.1.1/easy-rsa/keys/dh1024.pem
client-to-client     #允许连接的 VPN 客户端直接通信，而不是通过 VPN 服务器
                     转发数据。
duplicate-cn         #允许 VPN 客户端使用相同证书连接 VPN 服务器。
comp-lzo             #启用数据压缩
verb 3               #日志级别
```

客户端配置文件

```
client
setenv SERVER_Poll_TIMEOUT 4
nobind
proto udp                          #VPN 服务器传输协议（udp 或 tcp）
remote 218.107.220.74 1194         #VPN 服务器外网 IP 地址和端口
dev tun                            #虚拟网络接口（tun 或 tap）
dev-type tun
persist-tun
persist-key
ns-cert-type server
ca ca.crt                          #CA 证书
cert client.crt                    #客户端证书
key client.key                     #客户端私钥
verb 3                             #日志级别
comp-lzo
verb 3
```

客户反馈

我们正在努力提高文档质量，感谢您的反馈。请将您的意见和建议发送邮件至 DocsFeedback@yealink.com。