搭建 OpenVPN 服务器

作者：Kerry

日期：2017-06-12

部门：研发

类别：研发培训

产品：IP PHONE

目 录

第一章 服务器安装

1.1 下载 OpenVPN 软件

百度搜索 OpenVPN

打开链接：

欢迎使用中国科学技术大学网络OpenVPN系统

注意：使用VPN首先需要有具有VPN功能的网络通账号。

最新更改：

2013.09.29 增加CMCC移动出口，配置中增加reneg-sec 360000
2015.03.07 更新证书，2015年3月7日前下载过配置文件的，请重新下载下面的文件ca.crt，否则无法连接
2016.01.31 更新为2.3.10客户端，默认以管理员权限运行

1. 什么是VPN，为何要使用OpenVPN

VPN可以让校外的计算机像在校内一样使用，包括使用"网络通"服务，访问文献站点。

我校提供两种VPN服务器，分别是PPTP VPN和OpenVPN。

PPTP VPN不需要安装客户端，但在某些环境下无法连接，为了解决这个问题建设了OpenVPN系统。

2. 什么是OpenVPN

OpenVPN是一个开放源码的基于SSL的VPN系统，比我校使用的PPTP VPN 最大的优势在于仅仅使用UDP协议，支持从NAT设备后的连接。

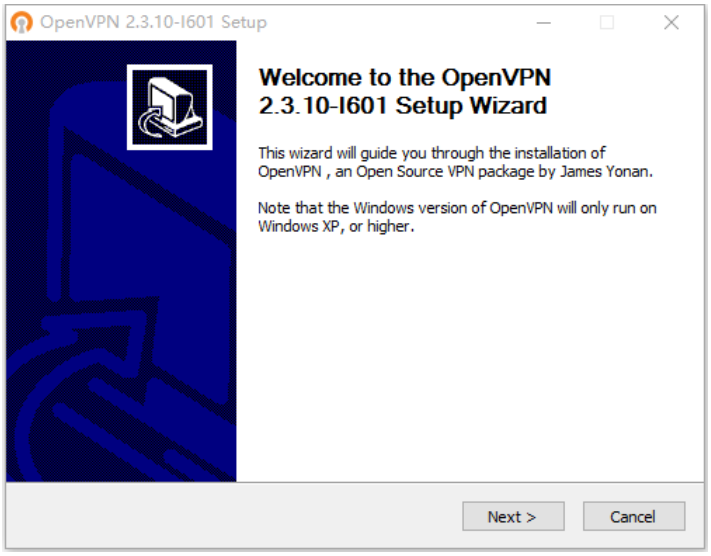
OpenVPN开发站点在 www.openvpn.net。

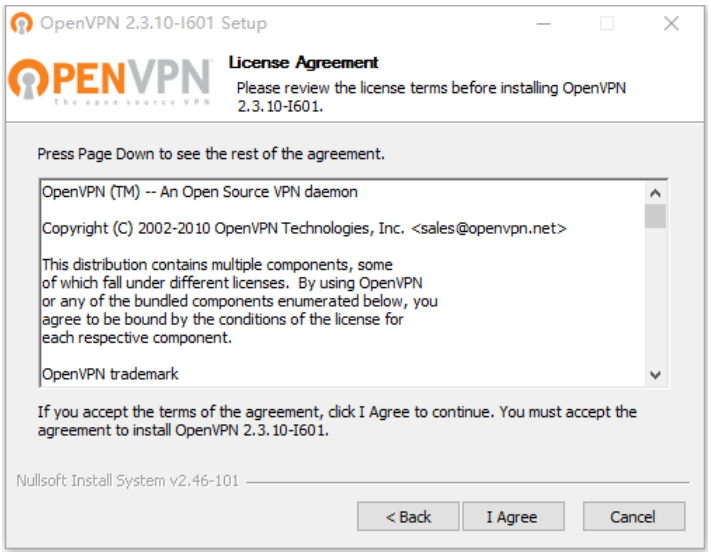
选择版本：openvpn-install-2.3.10-I601-x86_64.exe

操作系统	软件
Installer (32-bit), Windows XP	openvpn-install-2.3.10-I001-i686.exe
Installer (64-bit), Windows XP	openvpn-install-2.3.10-I001-x86_64.exe
Installer (32-bit), Windows Vista and later	openvpn-install-2.3.10-I601-i686.exe
Installer (64-bit), Windows Vista and later	openvpn-install-2.3.10-I601-x86_64.exe

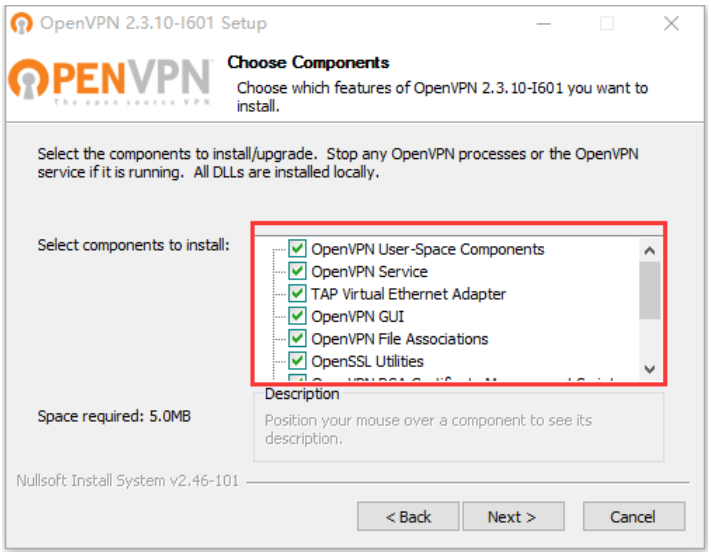
1.2 安装 OpenVPN 软件

运行下载的 exe 文件：

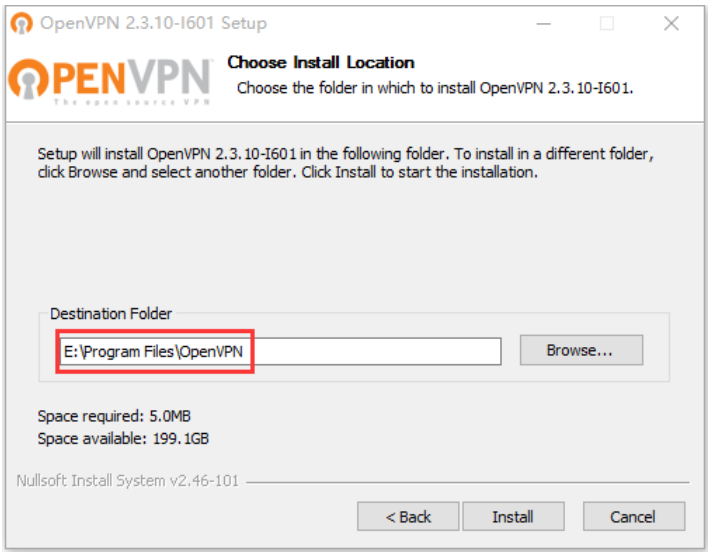




勾选安装组件：



选择安装位置：



第二章 服务器配置

2.1 创建加密证书和私钥

2.1.1 修改 OpenVPN 服务器端的 vars.bat.sample 文件

打开 E:\Program Files\OpenVPN\easy-rsa\vars.bat.sample 文件

```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

set HOME=E:\ProgramFiles\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.
```

变量 HOME 表示 easy-rsa 文件夹的路径

变量 KEY_SIZE 表示生成的私钥大小，一般填写为 1024 或 2048，默认为 1024 位，你可以根据自己的需要进行修改，这里使用默认值。

由于稍后给客户端生成对应加密证书和私钥时，程序会要求我们输入一些注册信息。如果你需要配置多个客户端，并且许多信息都相同(比如国家、省市、

地址、公司名称等)你还可以修改 vars.bat.sample 文件后面的一些相关变量的默认值，这样在稍后生成客户端证书的时候，如果该信息项不输入就会采用默认值。

```
31  set KEY_COUNTRY=CN                国家名称
32  set KEY_PROVINCE=JS               省份名称
33  set KEY_CITY=Nanjing              城市名称
34  set KEY_ORG=OpenVPN               组织机构名称
35  set KEY_EMAIL=kerry@htek.com      邮件地址
```

2.1.2 运行 DOS 命令，初始化执行环境

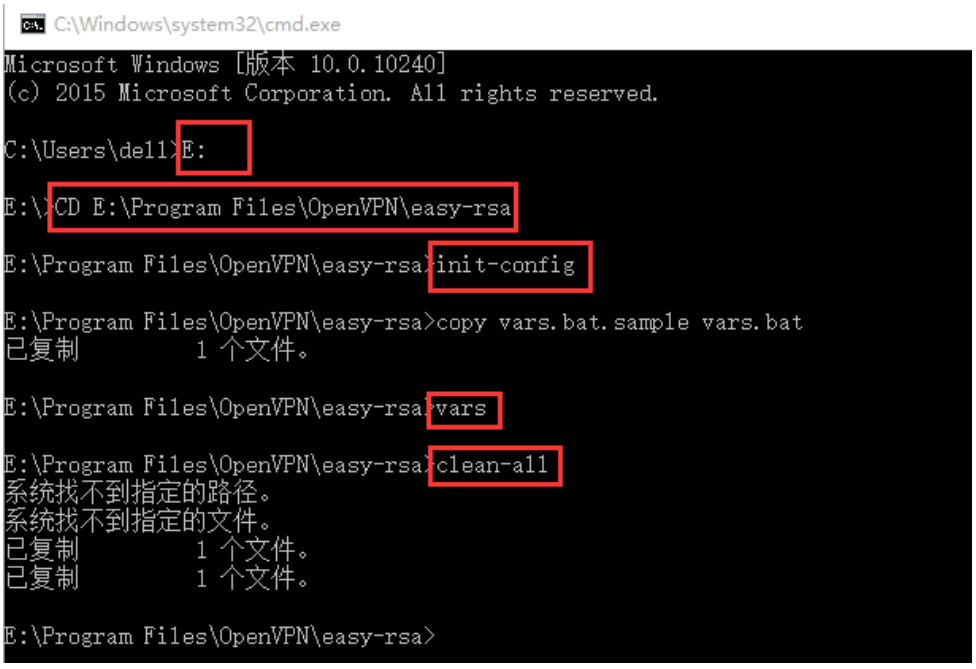
打开 DOS 命令窗口，并进入到 E:\Program Files\OpenVPN\easy-rsa 目录。

然后依次输入并执行以下命令：

1）init-config(初始化配置，将 vars.bat.sample 文件的内容复制到 vars.bat。实际上，你也可以直接双击执行 easy-rsa 目录下的 init-config.bat 文件来代替这一步。)

2）vars(设置相应的局部环境变量，就是我们在 vars.bat.sample 文件中设置的内容)

3）clean-all(相关设置和清理工作)



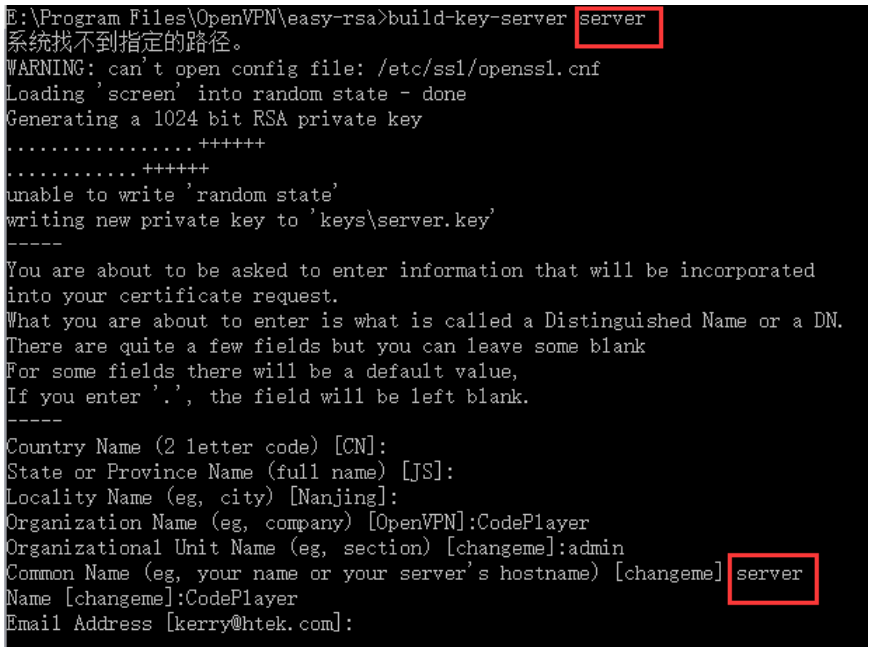
在“已复制”之前出现的两个找不到指定的路径、文件，该错误可以忽略。

2.1.3 创建 CA 根证书：build-ca

如上图所示，在 build-ca 的时候需要输入一些注册信息。在输入信息的时候，如果不输入任何信息，就表示采用默认值(前面[]中的内容就是默认值)；

如果输入，则表示当前信息项留空白。值得注意的是，上图中红色矩形框中的 OpenVPN_CA（需输入）是证书的通用名称(Common Name)，相当于我们常说的账号，也可以自行输入其他名称。

2.1.4 创建服务器端证书：build-key-server server



```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:admin
An optional company name []:CodePlayer
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.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:'JS'
localityName          :PRINTABLE:'Nanjing'
organizationName      :PRINTABLE:'CodePlayer'
organizationalUnitName:PRINTABLE:'admin'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'CodePlayer'
emailAddress          :IA5STRING:'kerry@htek.com'
Certificate is to be certified until Jun 10 08:27:43 2027 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
unable to write 'random state'
```

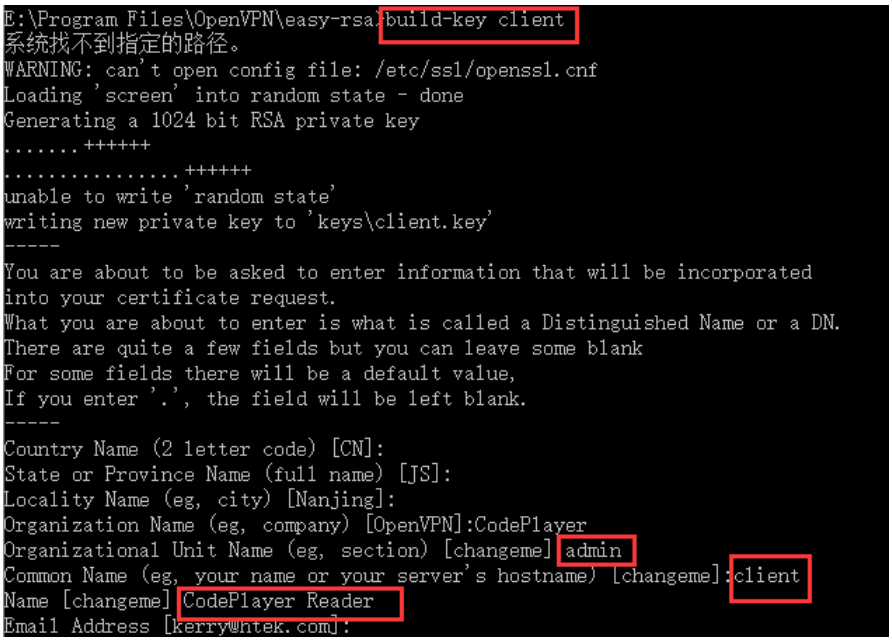
如上图所示，命令中的参数 server 指的是生成的证书文件名称，你可以按照自己的需要进行修改，不过后面的 Common Name 也应保持一致。第二个红色矩形框中是输入的密码，你也可以根据意愿自行输入。最后程序会询问你是否注册并提交证书，两次均输入 y 即可。

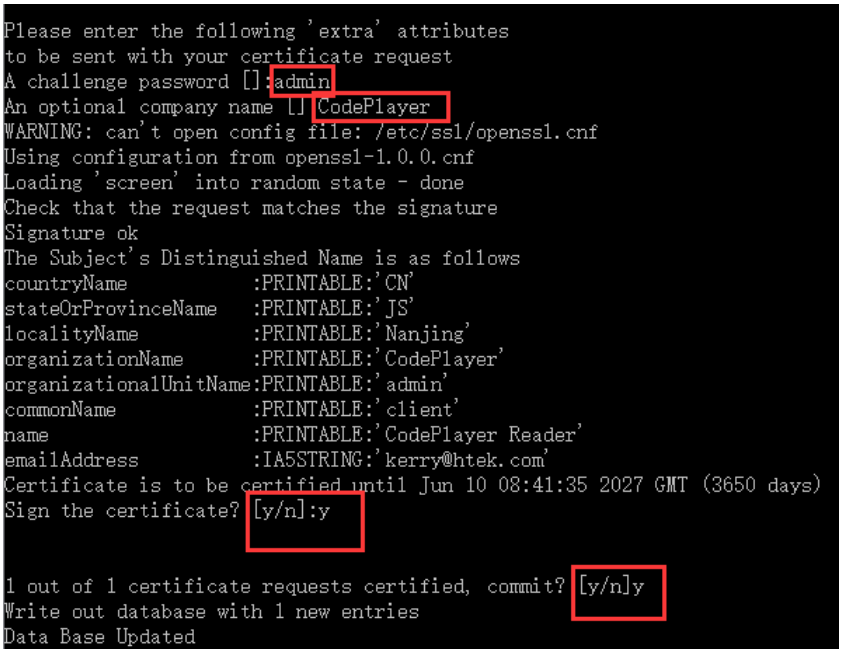
2.1.5 创建迪菲·赫尔曼密钥：build-dh

```
E:\Program Files\OpenVPN\easy-rsa>build-dh
系统找不到指定的路径。
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....+.+.....
.....+.....+.....+..
....+.....
.....+.....+.....
.....+.....
.....
                                                          +
```

迪菲·赫尔曼密钥交换(Diffie－Hellman key exchange，简称「D－H」) 是一种安全协议。它可以让双方在完全没有对方任何预先信息的条件下通过不安全信道创建起一个密钥。这个密钥可以在后续的通讯中作为对称密钥来加密通讯内容。

2.1.6 创建客户端证书：build-key client





如上图所示，命令中的参数 client 表示生成的证书文件名称，你可以按照自己的需要进行修改，不过后面的 Common Name 也应保持一致。第二个红色矩形框中是输入的密码，你也可以根据意愿自行输入。最后程序会询问你是否注册并提交证书，两次均输入 y 即可。

如果你想创建多个不同的客户端证书，只需要重复此步骤即可。切记，Common Name 不要重复，这是 OpenVPN 用来区分不同客户端的关键所在。

2.1.7 生成 ta.key：openvpn --genkey --secret keys/ta.key (可选操作)

```
E:\Program Files\OpenVPN\easy-rsa>openvpn --genkey --secret keys/ta.key

E:\Program Files\OpenVPN\easy-rsa>
```

这一步其实是可选操作，生成的 ta.key 主要用于防御 DoS、UDP 淹没等恶意攻击。命令中的第 3 个参数 keys/ta.key 表示生成的文件路径(含文件名)。

创建完证书后，我们会发现 easy-rsa 目录下多了一个 keys 文件夹。现在我们将 keys 文件夹中对应的文件复制到 OpenVPN 服务器或客户端的安装目录的 config 文件夹下。

服务器端 config 目录需要的文件包括：

ca.crt

ca.key(核心 CA 证书和私钥)

dh1024.pem(如果最初的变量 KEY_SIZE 设为 2048，这里就是 dh2048.pem)

server.crt

server.key(名称 server 根据个人设置可能有所不同)

ta.key(名称也可自行设置，如果不需要防御攻击，可以不创建或复制此文件)

客户端 config 目录需要的文件包括：

ca.crt

client.crt

client.key(名称 client 根据个人设置可能有所不同)

ta.key(如果服务器端具备此文件，客户端也应具备)

非常重要的提醒：以上命令都是在同一个 DOS 窗口中执行的，如果你以后需要打开新窗口来执行命令(比如创建新的客户端证书)：你不需要再执行 init-config 命令，除非你再次改动了 vars.bat.sample 文件；每一次打开新窗口时都需要先执行 vars 命令，后面才能执行其他命令。

2.2 编写对应的配置文件

在 OpenVPN 的安装目录的 sample-config 文件夹中存放有 3 个示例模板文件

server.ovpn 服务器的配置模板

client.ovpn 客户端的配置模板

sample.ovpn 也可用作客户端配置模板，不过配置比较简单，不够全面

现在，我们就复制 server.ovpn 到服务器的 config 目录，client.ovpn 到客户端的 config 目录，并在此基础上进行修改。在 OpenVPN 的配置文件中，前面带「#」或「;」的表示注释内容。

2.2.1 编辑服务器端配置文件

命令解释：

local 192.168.0.157　　#指定监听的本机 IP(因为有些计算机具备多个 IP 地址)，该命令是可选的，也可以不写，默认监听所有 IP 地址。

port 1194　　#指定监听的本机端口号

proto udp　　#指定采用的传输协议，可以选择 tcp 或 udp

dev tun　　#指定创建的通信隧道类型，可选 tun 或 tap

ca ca.crt　　#指定 CA 证书的文件路径

cert server.crt　　#指定服务器端的证书文件路径

key server.key　　#指定服务器端的私钥文件路径

dh dh1024.pem　　#指定迪菲赫尔曼参数的文件路径

server 10.8.0.0 255.255.255.0　　#指定虚拟局域网占用的 IP 地址段和子网掩码，此处配置的服务器自身占用 10.8.0.1。

ifconfig-pool-persist ipp.txt　　#服务器自动给客户端分配 IP 后，客户端下次连接时，仍然采用上次的 IP 地址(第一次分配的 IP 保存在 ipp.txt 中，下一次分配其中保存的 IP)。

tls-auth ta.key 0　　#开启 TLS，使用 ta.key 防御攻击。服务器端的第二个参数值为 0，客户端的为 1。

keepalive 10 120　　#每 10 秒 ping 一次，连接超时时间设为 120 秒。

comp-lzo　　#开启 VPN 连接压缩，如果服务器端开启，客户端也必须开启

client-to-client　　#允许客户端与客户端相连接，默认情况下客户端只能与服务器相连接

persist-key

persist-tun　　#持久化选项可以尽量避免访问在重启时由于用户权限降低而无法访问的某些资源。

status openvpn-status.log　　#指定记录 OpenVPN 状态的日志文件路径

verb 3　　#指定日志文件的记录详细级别，可选 0-9，等级越高日志内容越详细

```
# Which local IP address should OpenVPN
# listen on? (optional)
local 192.168.0.157

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp
```

```
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
```

```
75  # Any X509 key management system can be used.
76  # OpenVPN can also use a PKCS #12 formatted key file
77  # (see "pkcs12" directive in man page).
78  ca ca.crt
79  cert server.crt
80  key server.key  # This file should be kept secret
81
82  # Diffie hellman parameters.
83  # Generate your own with:
84  #   openssl dhparam -out dh2048.pem 2048
85  dh dh1024.pem
```

```
100 # ethernet bridging. See the man page for more info.
101 server 10.8.0.0 255.255.255.0
```

```
208 # server's TUN/TAP interface.
209 client-to-client
```

2.2.2 编辑客户端配置文件

命令解释：

client.ovpn 中所有用到的命令如下：

client　　#指定当前 VPN 是客户端

dev tun　　#必须与服务器端的保持一致

proto udp　　#必须与服务器端的保持一致

remote 192.168.0.157　1194　　#指定连接的远程服务器的实际 IP 地址和端口号

resolv-retry infinite　　#断线自动重新连接，在网络不稳定的情况下(例如：笔记本电脑无线网络)非常有用。

nobind　　#不绑定特定的本地端口号

persist-key

persist-tun

ca ca.crt　　#指定 CA 证书的文件路径

cert client.crt　　#指定当前客户端的证书文件路径

key client.key　　#指定当前客户端的私钥文件路径

ns-cert-type server　　#指定采用服务器校验方式

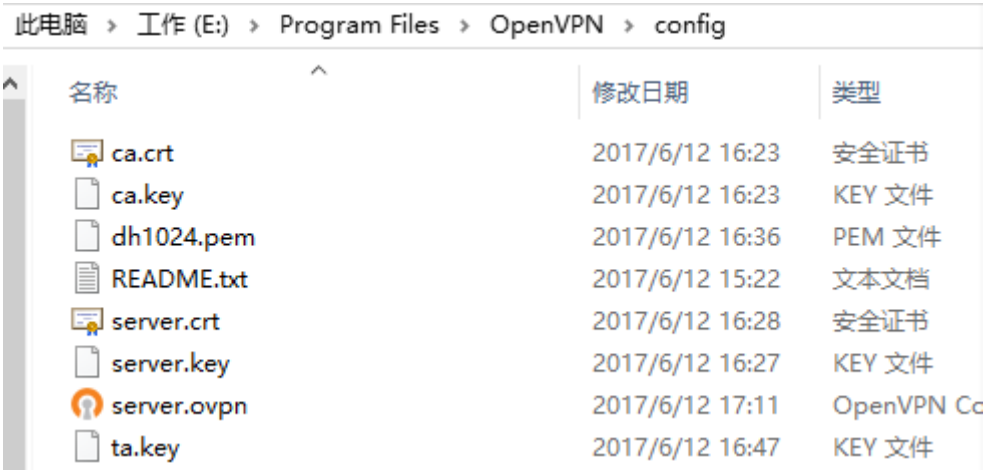
tls-auth ta.key 1　　#如果服务器设置了防御 DoS 等攻击的 ta.key，则必须每个客户端开启；如果未设置，则注释掉这一行；

comp-lzo　　#与服务器保持一致

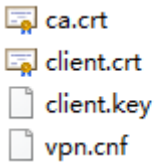
verb 3　　#指定日志文件的记录详细级别，可选 0-9，等级越高日志内容越详细

2.3 config 文件夹所含配置文件

2.3.1 服务器端文件



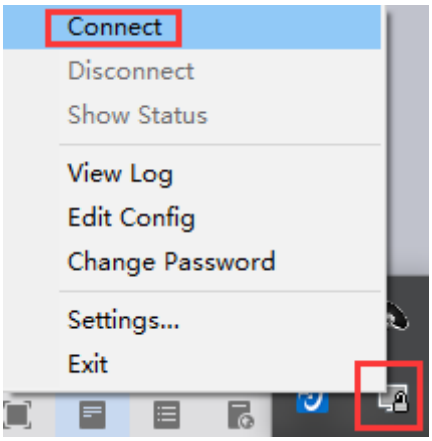
2.3.2 客户端文件

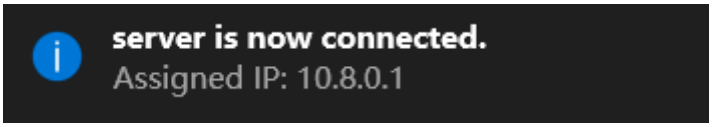


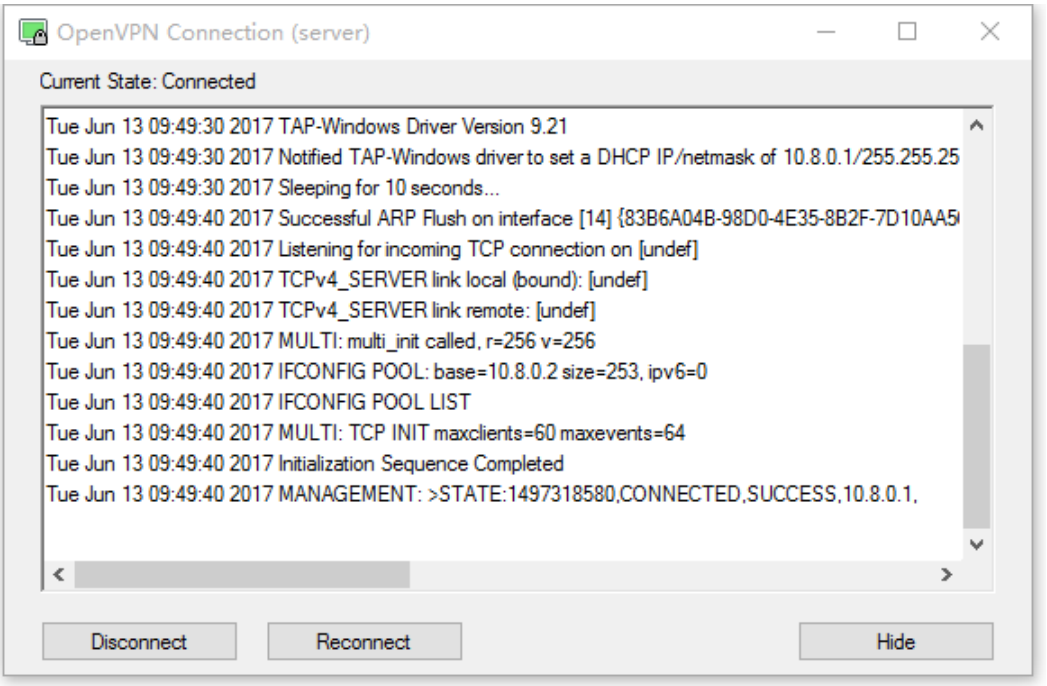
第三章 服务器测试

3.1 OpenVPN 测试

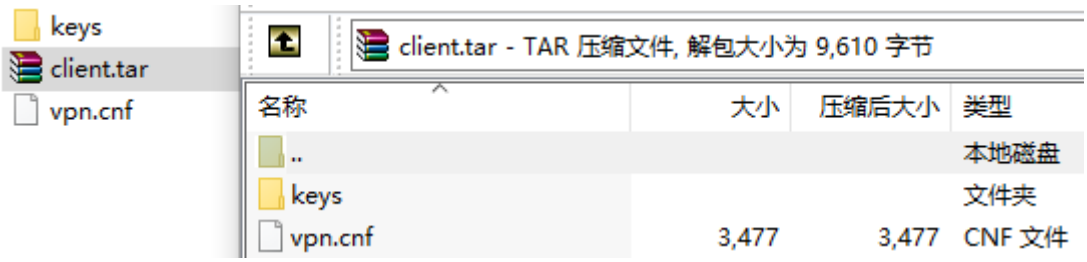
1. 运行服务器端软件，连接服务器：







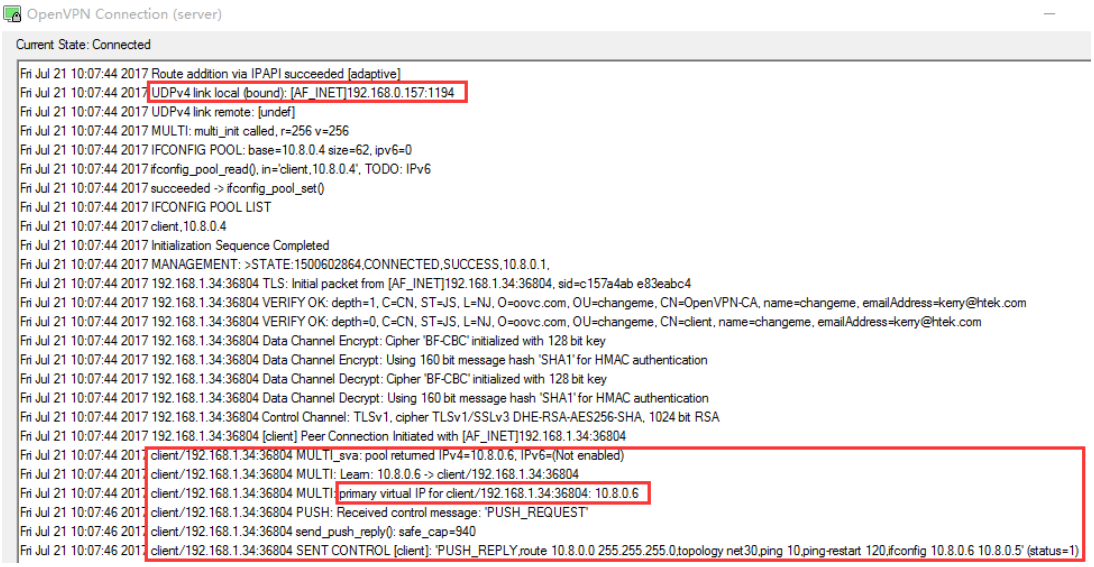
2. 将客户端文件压缩包上传话机网页。



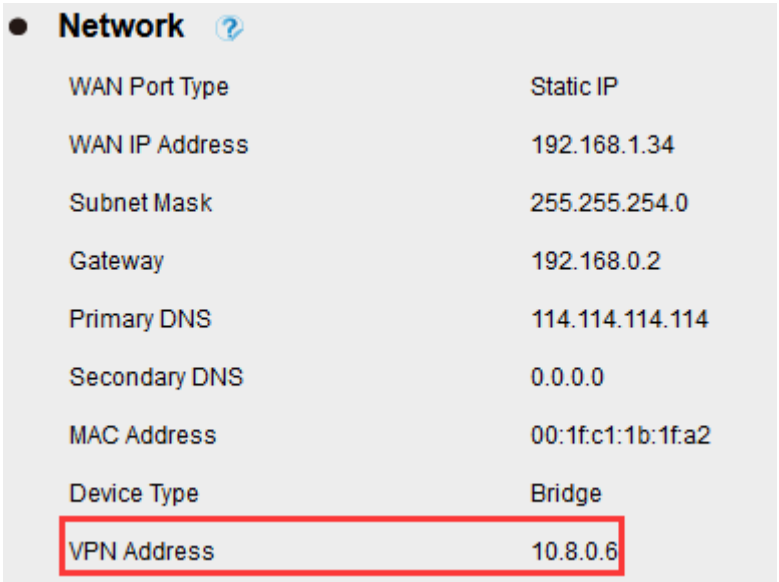
3.2 话机访问测试

执行：Network→Advanced→VPN

重启话机，查看服务器端，显示话机已连接：



查看话机网络状态，取到 VPN 地址：



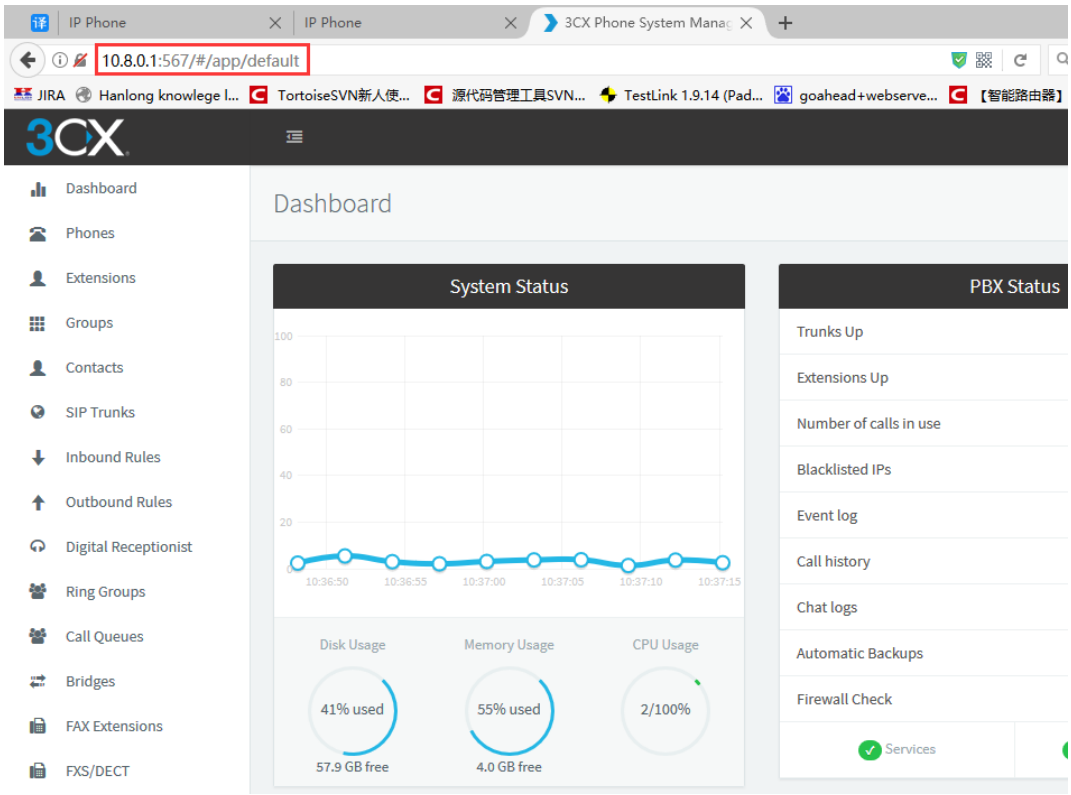
virtual IP for 话机：10.8.0.6

virtual IP for 本机：10.8.0.1

浏览器输入 virtual IP：10.8.0.6，可以访问话机页面：

3.3 通过 VPN Server 访问 3CX Server

浏览器输入本机 virtual IP+配置的 3CX server port 可以访问 3CX server：



参考文献

（无）