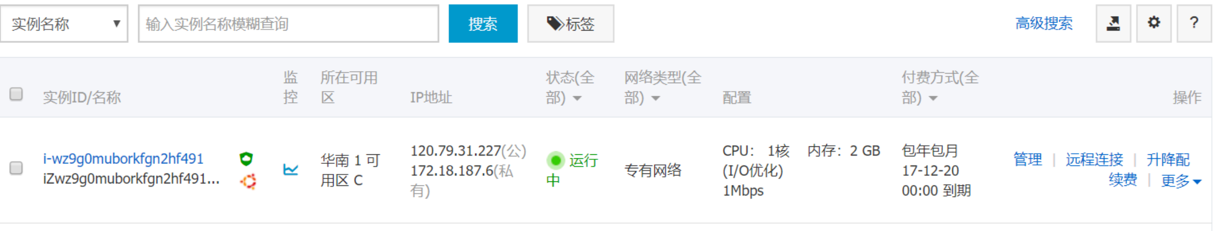
用OpenVPN搭建VPN

15331191 廖颖泓

本文建立VPN过程参考了Digital Ocean 提供的在Ubuntu上使用OpenVPN建立VPN教程：https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04#prerequisites，截图均来自亲自操作。

一、准备服务器

为了完成本次作业，我在阿里云上租了一台云服务器，使得搭建的VPN可以连接到云服务器上，服务器的公网IP是120.79.31.227。



□	实例ID/名称	监控	所在可用区	IP地址	状态(全部) ▾	网络类型(全部) ▾	配置	付费方式(全部) ▾	操作

□	i-wz9g0muborkfgn2hf491
	iZwz9g0muborkfgn2hf491...
			华南 1 可用区 C	120.79.31.227(公)
				172.18.187.6(私有)
					● 运行中	专有网络	CPU： 1核 内存： 2 GB
							(I/O优化)
							1Mbps
								包年包月
								17-12-20 00:00 到期
									管理 | 远程连接 | 升降配
									续费 | 更多 ▾

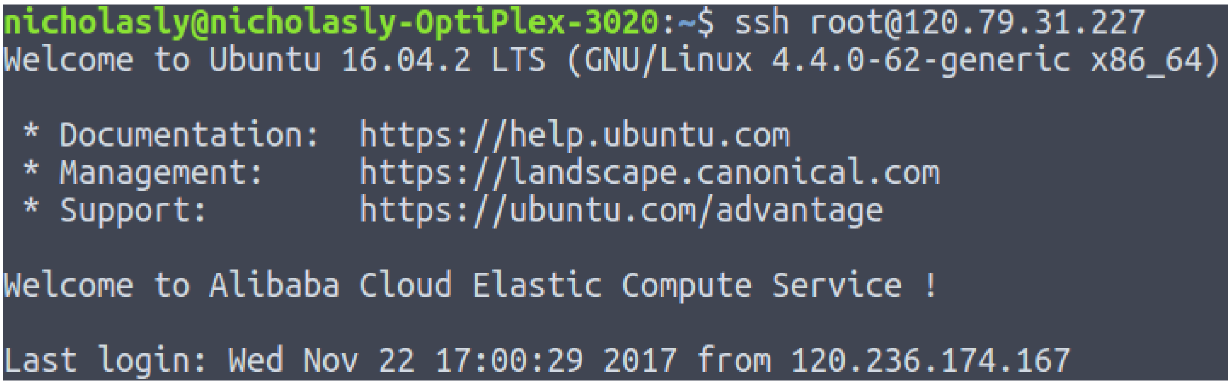
二、在服务器上安装OpenVPN和Easy-RSA

在Ubuntu系统上用SSH以root的身份登录服务器：

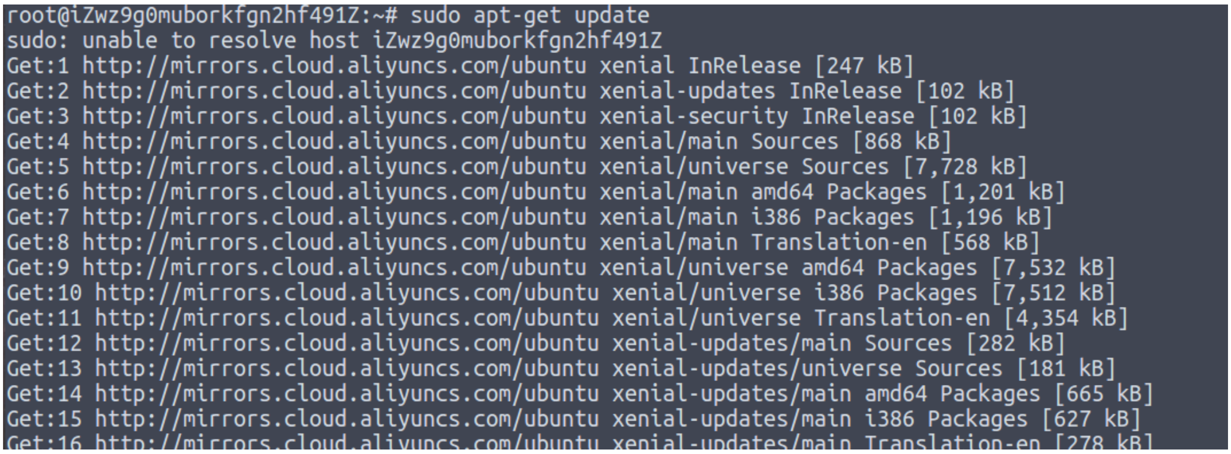
```
$ ssh root@120.79.31.227
```

然后输入命令安装OpenVPN和Easy-RSA：

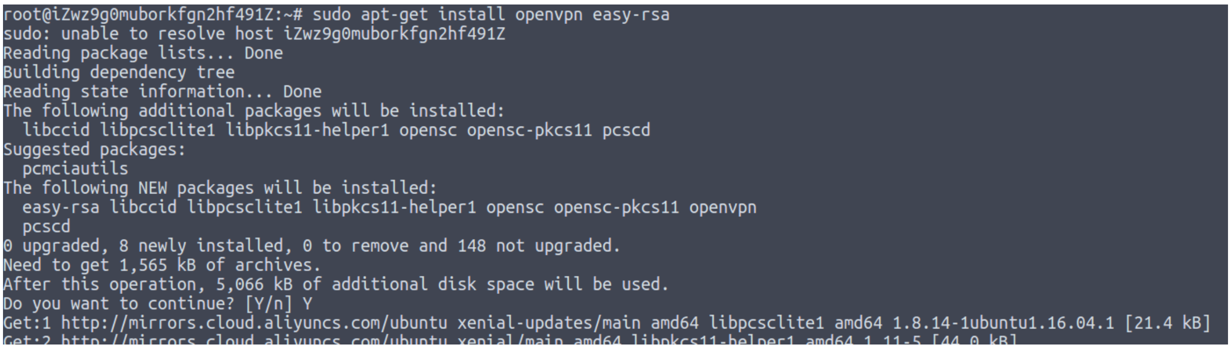
```
$ sudo apt-get update
$ sudo apt-get install openvpn easy-rsa
```



```
nicholasly@nicholasly-OptiPlex-3020:~$ ssh root@120.79.31.227
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Wed Nov 22 17:00:29 2017 from 120.236.174.167
```



```
root@iZwz9g0muborkfgn2hf491Z:~# sudo apt-get update
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Get:1 http://mirrors.cloud.aliyuncs.com/ubuntu xenial InRelease [247 kB]
Get:2 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates InRelease [102 kB]
Get:3 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-security InRelease [102 kB]
Get:4 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/main Sources [868 kB]
Get:5 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/universe Sources [7,728 kB]
Get:6 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/main amd64 Packages [1,201 kB]
Get:7 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/main i386 Packages [1,196 kB]
Get:8 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/main Translation-en [568 kB]
Get:9 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
Get:10 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/universe i386 Packages [7,512 kB]
Get:11 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/universe Translation-en [4,354 kB]
Get:12 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates/main Sources [282 kB]
Get:13 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates/universe Sources [181 kB]
Get:14 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates/main amd64 Packages [665 kB]
Get:15 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates/main i386 Packages [627 kB]
Get:16 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates/main Translation-en [278 kB]
```



```
root@iZwz9g0muborkfgn2hf491Z:~# sudo apt-get install openvpn easy-rsa
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libccid libpcsclite1 libpkcs11-helper1 opensc opensc-pkcs11 pcscd
Suggested packages:
  pcmciautils
The following NEW packages will be installed:
  easy-rsa libccid libpcsclite1 libpkcs11-helper1 opensc opensc-pkcs11 openvpn
  pcscd
0 upgraded, 8 newly installed, 0 to remove and 148 not upgraded.
Need to get 1,565 kB of archives.
After this operation, 5,066 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://mirrors.cloud.aliyuncs.com/ubuntu xenial-updates/main amd64 libpcsclite1 amd64 1.8.14-1ubuntu1.16.04.1 [21.4 kB]
Get:2 http://mirrors.cloud.aliyuncs.com/ubuntu xenial/main amd64 libpkcs11-helper1 amd64 1.11-5 [44.0 kB]
```

三、建立CA目录和设置CA量

OpenVPN是一个基于TLS/SSL的VPN，采用非对称加密方式，需要建立一个公钥基础设施(PKI)，包括为OpenVPN服务器创建一个证书(公钥)和一个私钥、为每个OpenVPN客户端创建证书和私钥、建立一个证书颁发机构(CA)并创建证书和私钥。这里的私钥用来给OpenVPN服务器和客户端的证书签名。

首先，我们先建立一个CA目录`~/openvpn-ca`：

```
$ make-cadir ~/openvpn-ca
$ cd ~/openvpn-ca
```

然后我们还要设置CA变量，修改文件`~/openvpn-ca/vars`，其中包括主证书和密钥的信息，如：

```
...
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"
...
```

这里我的设置是：

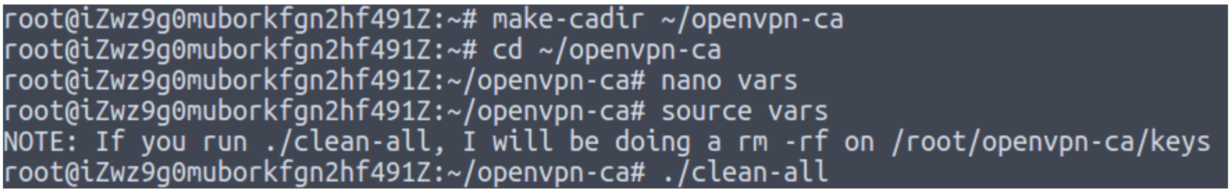
```
...
export KEY_COUNTRY="CN"
export KEY_PROVINCE="GD"
export KEY_CITY="Shenzhen"
export KEY_ORG="Aliyun"
export KEY_EMAIL="382112699@qq.com"
export KEY_OU="MyOrganizationalUnit"
...
```

另外我还设置了密钥的名字：

```
export KEY_NAME="server"
```

然后我们为了让变量生效，并防止有旧证书的影响，输入以下命令

```
$ source vars
$ ./clean-all
```

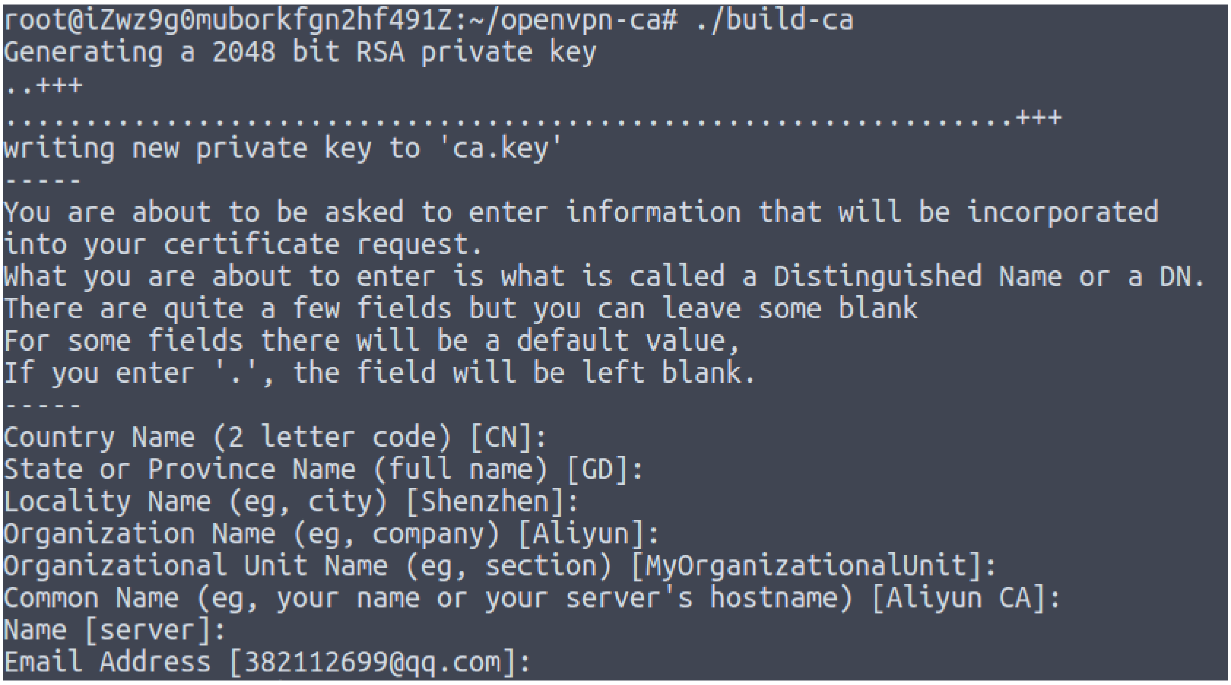


```
root@iZwz9g0muborkfgn2hf491Z:~# make-cadir ~/openvpn-ca
root@iZwz9g0muborkfgn2hf491Z:~# cd ~/openvpn-ca
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# nano vars
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /root/openvpn-ca/keys
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# ./clean-all
```

四、建立CA

输入以下命令建立CA：

```
$ ./build-ca
```



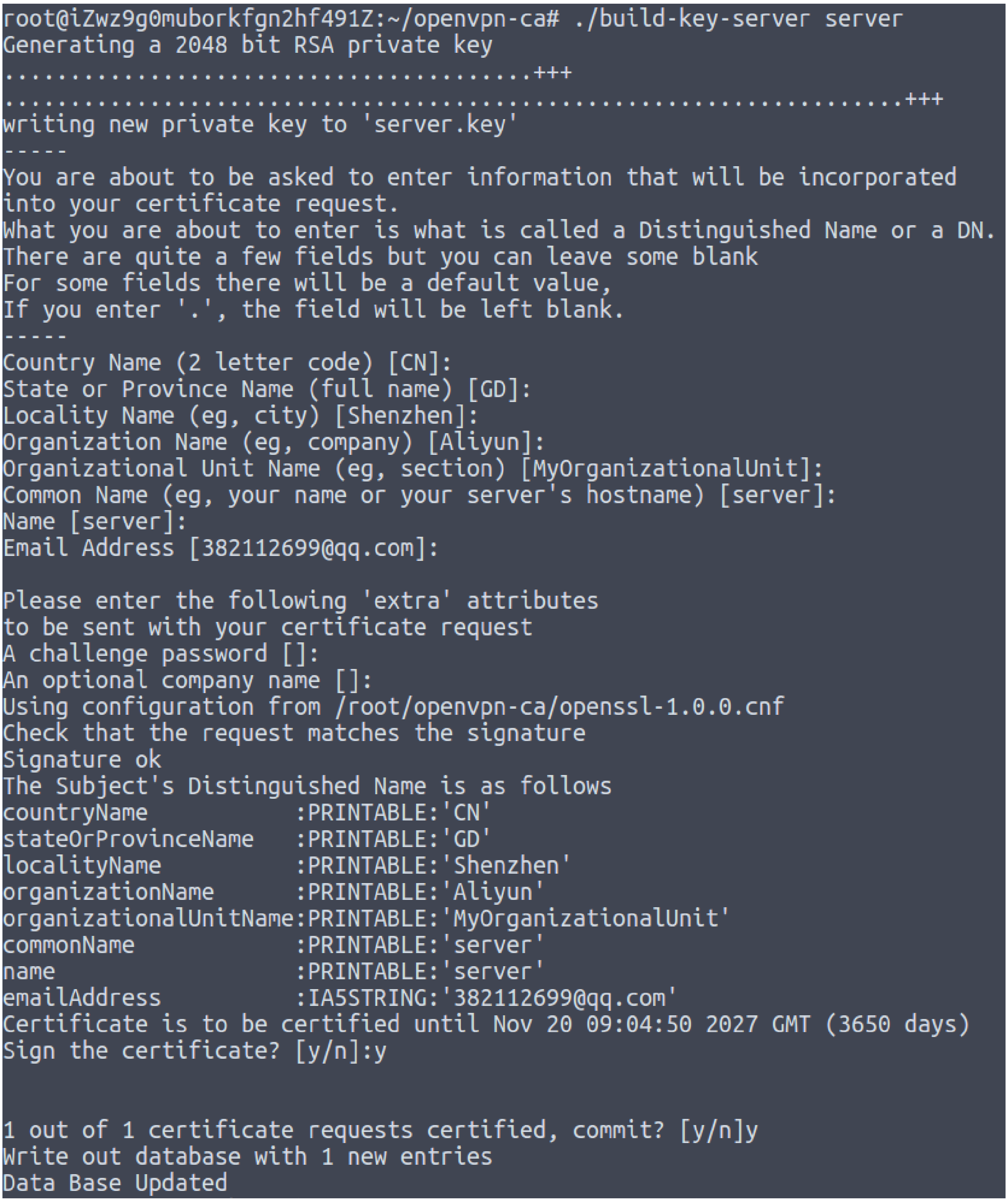
```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# ./build-ca
Generating a 2048 bit RSA private key
..+++
...............................................................+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate 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) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [Aliyun]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [Aliyun CA]:
Name [server]:
Email Address [382112699@qq.com]:
```

上面的信息不断按Enter选择了默认设置的信息。

五、创建服务器证书、密钥和加密文件

输入以下命令创建服务器证书、密钥和加密文件：

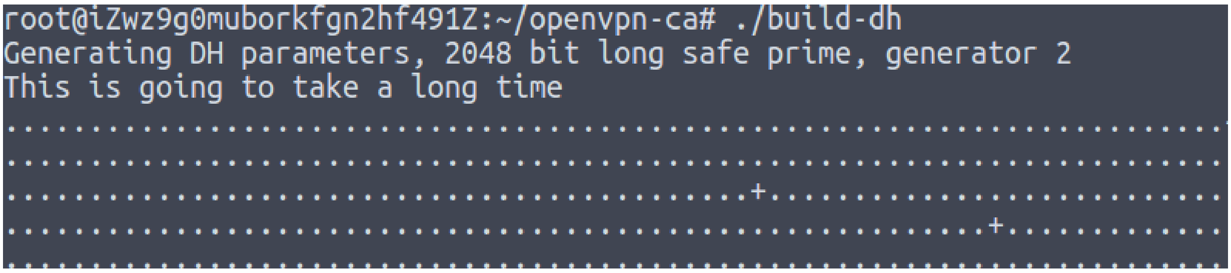
```
$ ./build-key-server server
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# ./build-key-server server
Generating a 2048 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) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [Aliyun]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [server]:
Name [server]:
Email Address [382112699@qq.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /root/openvpn-ca/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Shenzhen'
organizationName      :PRINTABLE:'Aliyun'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'server'
emailAddress          :IA5STRING:'382112699@qq.com'
Certificate is to be certified until Nov 20 09:04:50 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
```

然后我们输入以下命令生成Diffie-Hellman参数：

```
$ ./build-dh
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
........................................................................
........................................................................
............................................+...........................
..........................................................+.............
........................................................................
```

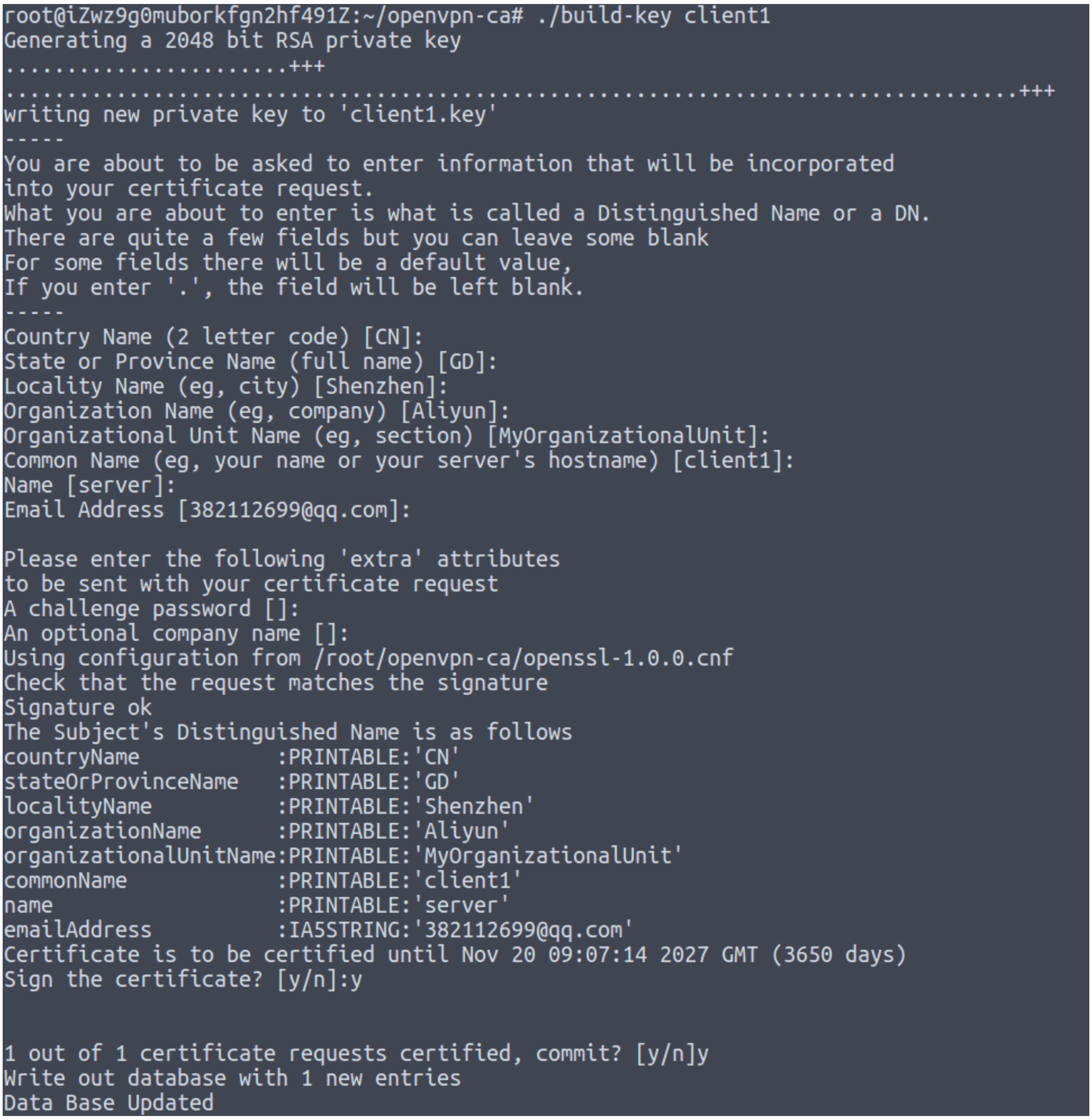
然后我们输入命令生成HMAC签名来增强服务器TLS完整性验证能力：

```
$ openvpn --genkey --secret keys/ta.key
```

六、生成客户端证书和密钥对

输入以下命令生成客户端证书和密钥对，客户端名称为client1：

```
$ ./build-key client1
```

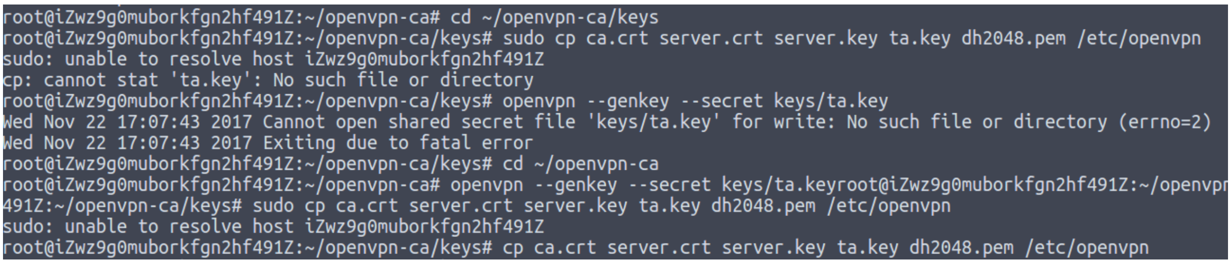


```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# ./build-key client1
Generating a 2048 bit RSA private key
.......................+++
..................................................................................+++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information 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) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [Aliyun]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [client1]:
Name [server]:
Email Address [382112699@qq.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /root/openvpn-ca/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Shenzhen'
organizationName      :PRINTABLE:'Aliyun'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'client1'
name                  :PRINTABLE:'server'
emailAddress          :IA5STRING:'382112699@qq.com'
Certificate is to be certified until Nov 20 09:07:14 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
```

七、配置OpenVPN服务端

首先我们需要把CA目录`~/openvpn-ca/keys`下的证书和密钥复制到OenVPN的目录`~/etc/openvpn/`下：

```
  $ sudo cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# cd ~/openvpn-ca/keys
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
cp: cannot stat 'ta.key': No such file or directory
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# openvpn --genkey --secret keys/ta.key
Wed Nov 22 17:07:43 2017 Cannot open shared secret file 'keys/ta.key' for write: No such file or directory (errno=2)
Wed Nov 22 17:07:43 2017 Exiting due to fatal error
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# cd ~/openvpn-ca
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca# openvpn --genkey --secret keys/ta.keyroot@iZwz9g0muborkfgn2hf491Z:~/openvpr
491Z:~/openvpn-ca/keys# sudo cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
```

我们再修改服务器的配置文件：

```
$ sudo nano /etc/openvpn/server.conf
```

修改包括：
1、

```
tls-auth ta.key 0 # This file is secret
```

修改成：

```
tls-auth ta.key 0 # This file is secret
key-direction 0
```

2、

```
;cipher AES-128-CBC
```

修改成：

```
cipher AES-128-CBC
auth SHA256
```

3、

```
;push "redirect-gateway def1 bypass-dhcp"
```

修改成：

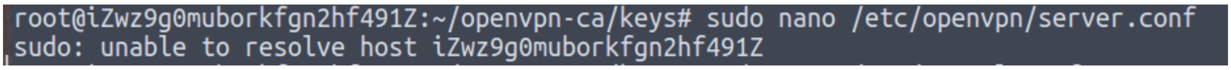
```
push "redirect-gateway def1 bypass-dhcp"
```

4、

```
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"
```

修改成：

```
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/openvpn/server.conf
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
```

八、调整服务端配置

首先我们修改`~/etc/sysctl.conf`文件允许IP转发：

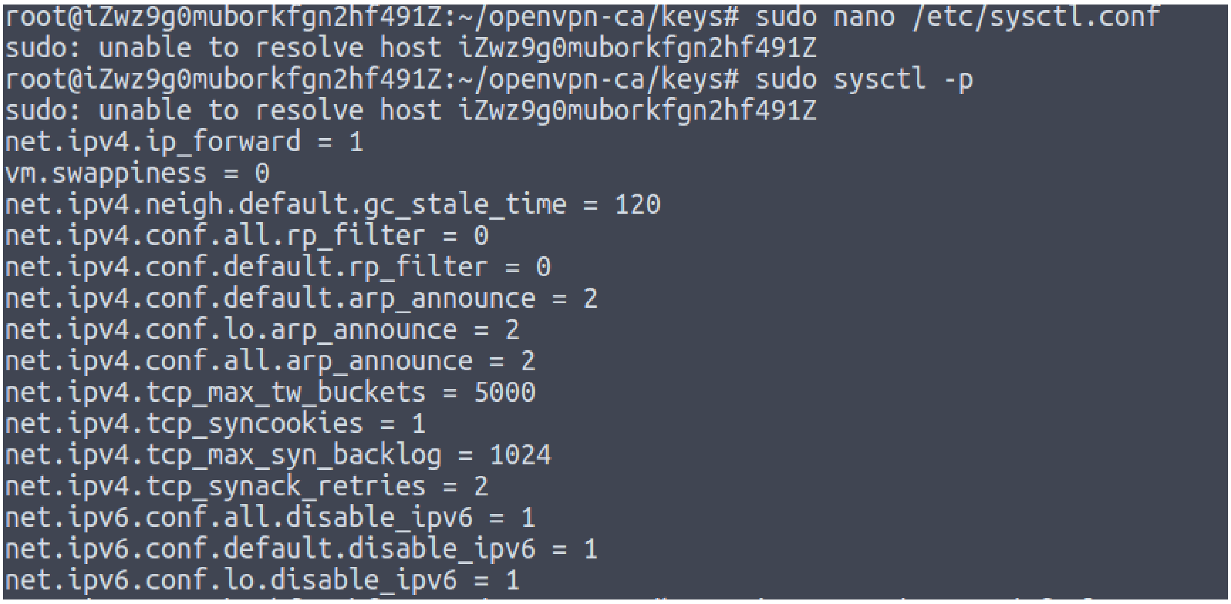
```
$ sudo nano /etc/sysctl.conf
```

修改将以下内容前面的#去掉：

```
# net.ipv4.ip_forward=1
net.ipv4.ip_forward=1
```

然后输入命令让修改生效：

```
$ sudo sysctl -p
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/sysctl.conf
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo sysctl -p
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
net.ipv4.ip_forward = 1
vm.swappiness = 0
net.ipv4.neigh.default.gc_stale_time = 120
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.arp_announce = 2
net.ipv4.conf.lo.arp_announce = 2
net.ipv4.conf.all.arp_announce = 2
net.ipv4.tcp_max_tw_buckets = 5000
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 1024
net.ipv4.tcp_synack_retries = 2
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

接着我们修改防火墙规则：

```
$ sudo nano /etc/ufw/before.rules
```

1、将虚拟网卡加入规则中:

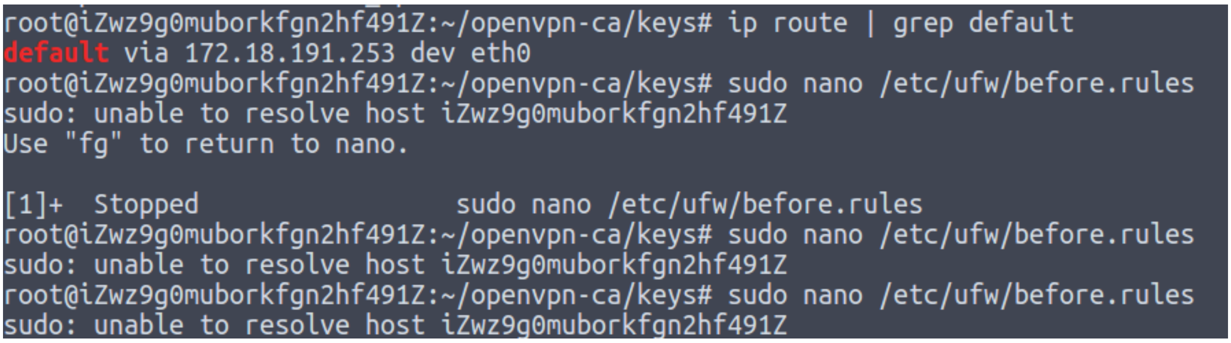
```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# START OPENVPN RULES
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]
# Allow traffic from OpenVPN client to wlp11s0 (change to the interface you discovered!)
-A POSTROUTING -s 10.8.0.0/8 -o wlp11s0 -j MASQUERADE
COMMIT
# END OPENVPN RULES

# Don't delete these required lines, otherwise there will be errors
*filter
. . .
```

我的虚拟网卡为eth0，只需要将wlp11s0换成eth0

```
$ sudo nano /etc/default/ufw
```

2、允许转发协议

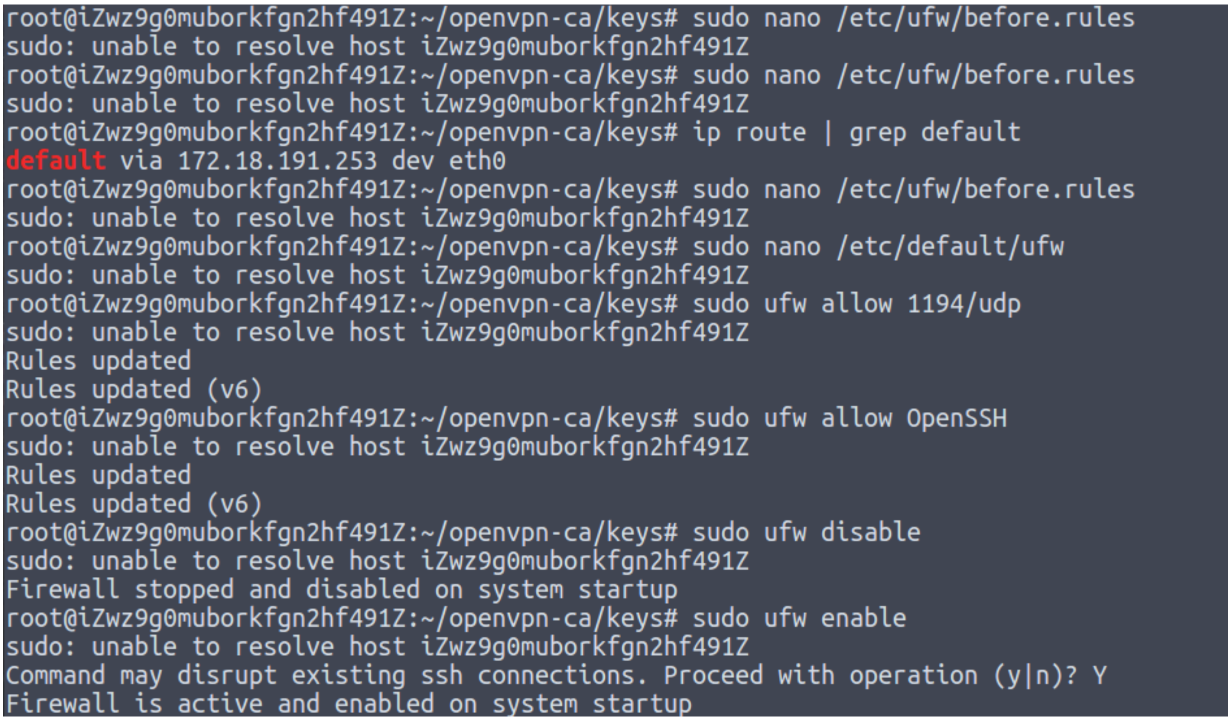
```
DEFAULT_FORWARD_POLICY="ACCEPT"
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# ip route | grep default
default via 172.18.191.253 dev eth0
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/ufw/before.rules
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Use "fg" to return to nano.

[1]+  Stopped                 sudo nano /etc/ufw/before.rules
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/ufw/before.rules
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/ufw/before.rules
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
```

3、打开OpenVPNd端口允许修改，包括打开1191端口和OpenSSH以及重新打开防火墙

```
$ sudo ufw allow 1194/udp
$ sudo ufw allow OpenSSH
$ sudo ufw disable
$ sudo ufw enable
```

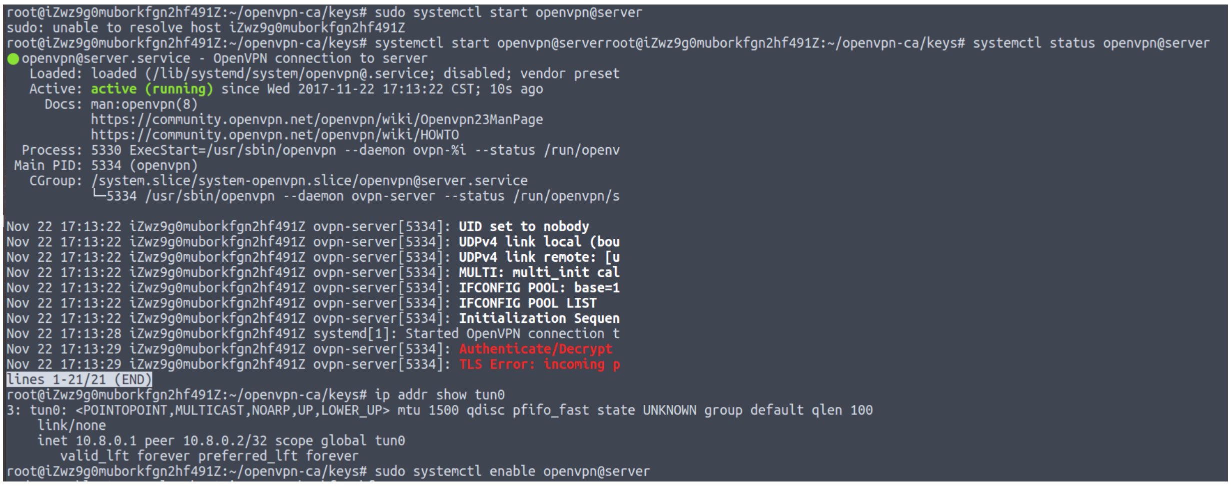


```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/ufw/before.rules
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/ufw/before.rules
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# ip route | grep default
default via 172.18.191.253 dev eth0
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/ufw/before.rules
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo nano /etc/default/ufw
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo ufw allow 1194/udp
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Rules updated
Rules updated (v6)
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo ufw allow OpenSSH
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Rules updated
Rules updated (v6)
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo ufw disable
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Firewall stopped and disabled on system startup
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo ufw enable
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Command may disrupt existing ssh connections. Proceed with operation (y|n)? Y
Firewall is active and enabled on system startup
```

九、打开并启动OpenVPN服务端

输入命令打开OpenVPN服务端并确认状态：

```
$ sudo systemctl start openvpn@server
$ sudo systemctl status openvpn@server
```



```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo systemctl start openvpn@server
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# systemctl start openvpn@serverroot@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset
   Active: active (running) since Wed 2017-11-22 17:13:22 CST; 10s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
  Process: 5330 ExecStart=/usr/sbin/openvpn --daemon ovpn-%i --status /run/openv
 Main PID: 5334 (openvpn)
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─5334 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/s

Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: UID set to nobody
Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: UDPv4 link local (bou
Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: UDPv4 link remote: [u
Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: MULTI: multi_init cal
Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: IFCONFIG POOL: base=1
Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: IFCONFIG POOL LIST
Nov 22 17:13:22 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: Initialization Sequen
Nov 22 17:13:28 iZwz9g0muborkfgn2hf491Z systemd[1]: Started OpenVPN connection t
Nov 22 17:13:29 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: Authenticate/Decrypt
Nov 22 17:13:29 iZwz9g0muborkfgn2hf491Z ovpn-server[5334]: TLS Error: incoming p
lines 1-21/21 (END)
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# ip addr show tun0
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
       valid_lft forever preferred_lft forever
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo systemctl enable openvpn@server
```

我们可以看到服务端已经开始运行。

十、创建客户端配置框架

1、建立客户端目录结构并降低权限：

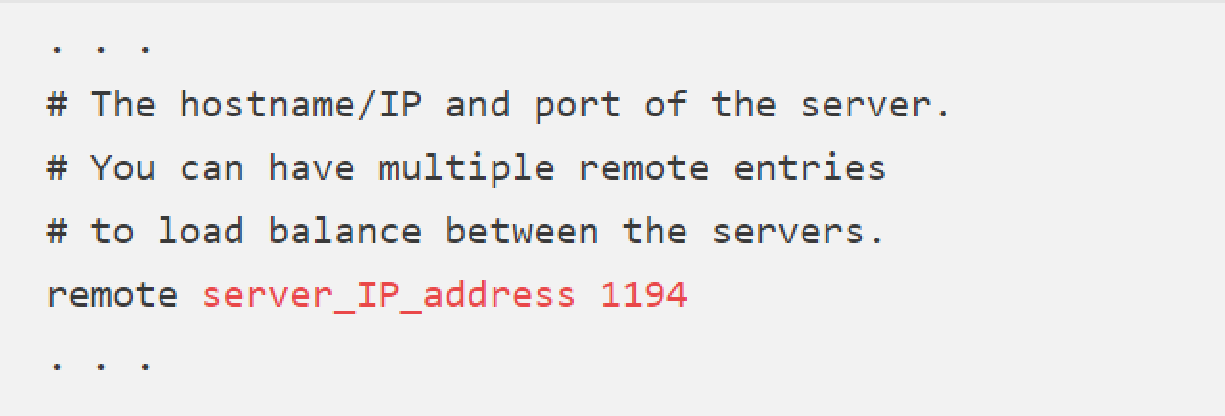
```
    $ mkdir -p ~/client-configs/files
    $ chmod 700 ~/client-configs/files
```

2、创建基本设置：

```
    $ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
~/client-configs/base.conf
    $ nano ~/client-configs/base.conf
```

在文件`~/client-configs/base.conf`作以下修改：

（1）输入服务器公网IP，即120.79.31.227



```
. . .
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote server_IP_address 1194
. . .
```

（2）将前面的`;`号去掉：

```
    # Downgrade privileges after initialization (non-Windows only)
    ;user nobody
    ;group nogroup
```

（3）将客户证书和密钥加上注释：

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

（4）加入加密算法信息：

```
    cipher AES-128-CBC
    auth SHA256
    key-direction 1
```

然后创建一个文件`~/client-configs/make_config.sh`，并在里面输入以下内容：

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=~/openvpn-ca/keys
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-auth>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-auth>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

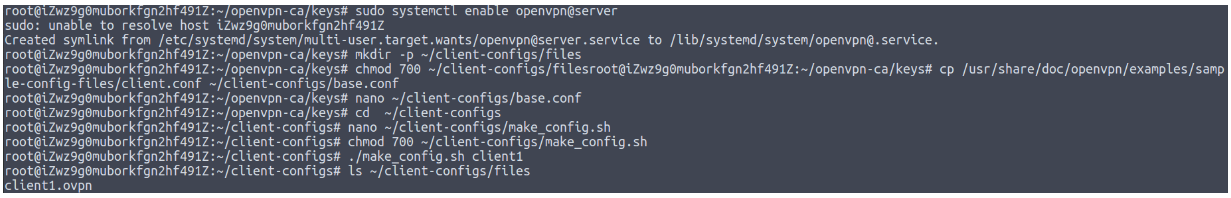
保存好并让它可以执行：

```
$ chmod 700 ~/client-configs/make_config.sh
```

十一、生成客户端配置文件

输入以下命令得到配置文件：

```
$ cd ~/client-configs
$ ./make_config.sh client1
```



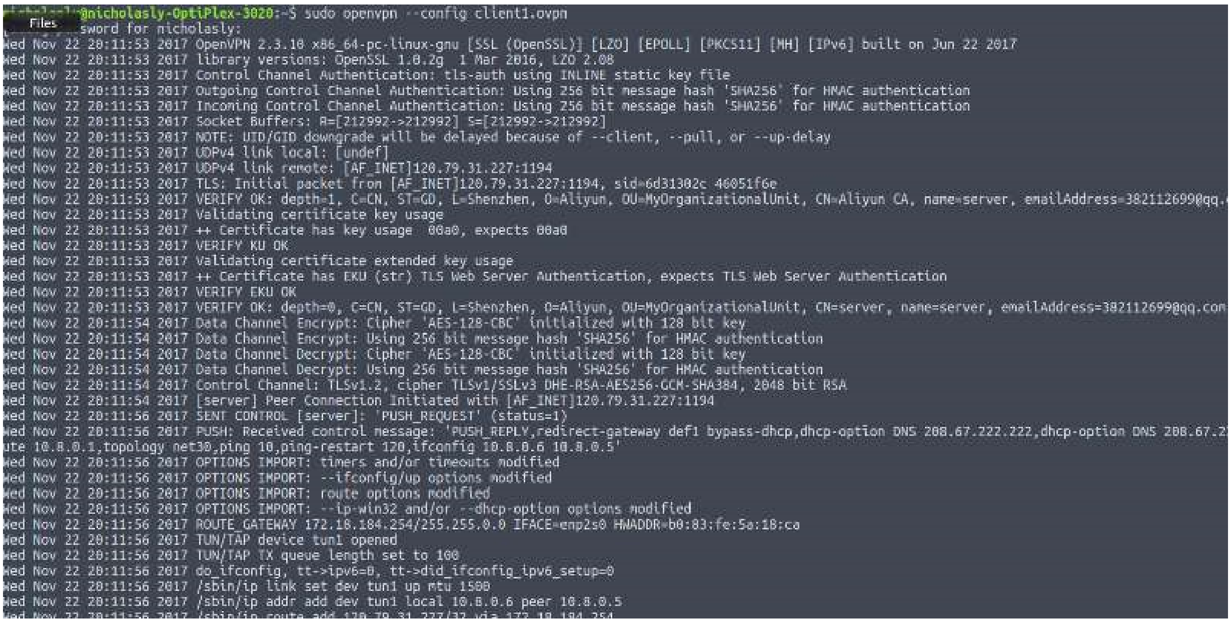
```
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# sudo systemctl enable openvpn@server
sudo: unable to resolve host iZwz9g0muborkfgn2hf491Z
Created symlink from /etc/systemd/system/multi-user.target.wants/openvpn@server.service to /lib/systemd/system/openvpn@.service.
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# mkdir -p ~/client-configs/files
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# chmod 700 ~/client-configs/filesroot@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# cp /usr/share/doc/openvpn/examples/samp
le-config-files/client.conf ~/client-configs/base.conf
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# nano ~/client-configs/base.conf
root@iZwz9g0muborkfgn2hf491Z:~/openvpn-ca/keys# cd  ~/client-configs
root@iZwz9g0muborkfgn2hf491Z:~/client-configs# nano ~/client-configs/make_config.sh
root@iZwz9g0muborkfgn2hf491Z:~/client-configs# chmod 700 ~/client-configs/make_config.sh
root@iZwz9g0muborkfgn2hf491Z:~/client-configs# ./make_config.sh client1
root@iZwz9g0muborkfgn2hf491Z:~/client-configs# ls ~/client-configs/files
client1.ovpn
```

我们可以看到目录`~/client-configs/keys`下有文件`client1.ovpn`。

十二、执行文件查看是否可以连接成功

在目录`~/client-configs/keys`下输入命令：

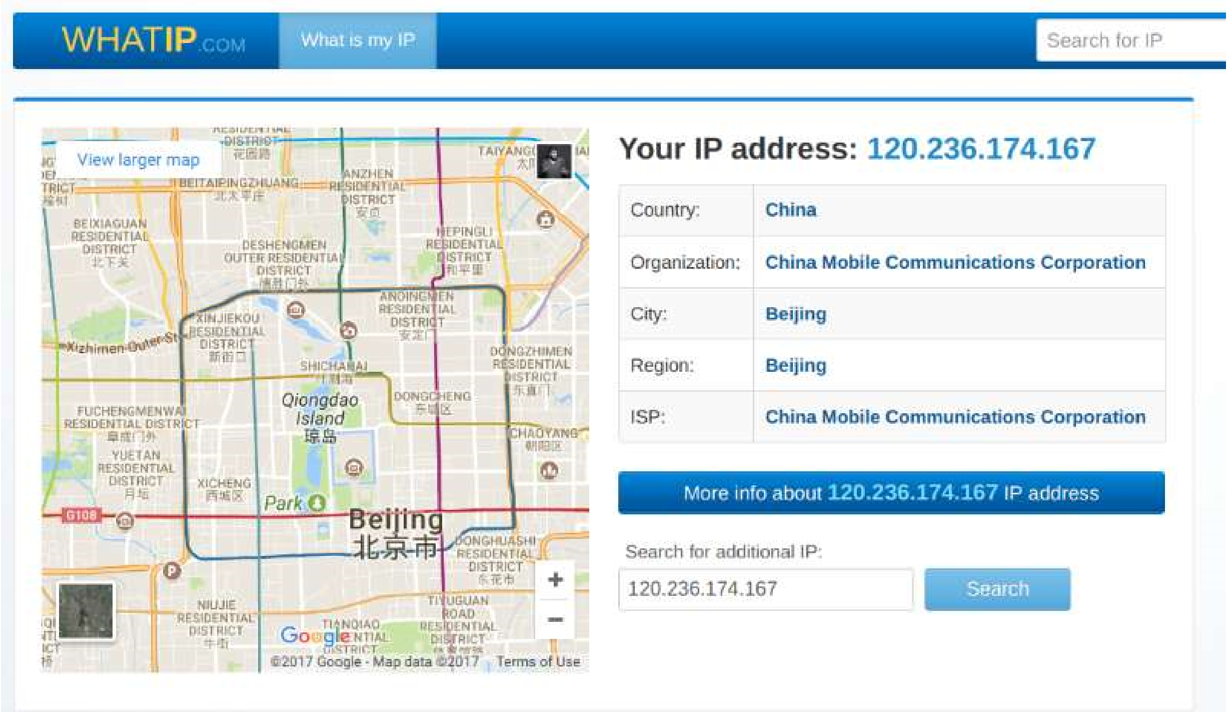
```
$ sudo openvpn --config client1.ovpn
```



```
nicholasly@nicholasly-OptiPlex-3020:~$ sudo openvpn --config client1.ovpn
[sudo] password for nicholasly:
Wed Nov 22 20:11:53 2017 OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Jun 22 2017
Wed Nov 22 20:11:53 2017 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Wed Nov 22 20:11:53 2017 Control Channel Authentication: tls-auth using INLINE static key file
Wed Nov 22 20:11:53 2017 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed Nov 22 20:11:53 2017 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed Nov 22 20:11:53 2017 Socket Buffers: R=[212992->212992] S=[212992->212992]
Wed Nov 22 20:11:53 2017 NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-delay
Wed Nov 22 20:11:53 2017 UDPv4 link local: [undef]
Wed Nov 22 20:11:53 2017 UDPv4 link remote: [AF_INET]120.79.31.227:1194
Wed Nov 22 20:11:53 2017 TLS: Initial packet from [AF_INET]120.79.31.227:1194, sid=6d31302c 46051f6e
Wed Nov 22 20:11:53 2017 VERIFY OK: depth=1, C=CN, ST=GD, L=Shenzhen, O=Aliyun, OU=MyOrganizationalUnit, CN=Aliyun CA, name=server, emailAddress=382112699@qq.c
Wed Nov 22 20:11:53 2017 Validating certificate key usage
Wed Nov 22 20:11:53 2017 ++ Certificate has key usage  00a0, expects 00a0
Wed Nov 22 20:11:53 2017 VERIFY KU OK
Wed Nov 22 20:11:53 2017 Validating certificate extended key usage
Wed Nov 22 20:11:53 2017 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Wed Nov 22 20:11:53 2017 VERIFY EKU OK
Wed Nov 22 20:11:53 2017 VERIFY OK: depth=0, C=CN, ST=GD, L=Shenzhen, O=Aliyun, OU=MyOrganizationalUnit, CN=server, name=server, emailAddress=382112699@qq.com
Wed Nov 22 20:11:54 2017 Data Channel Encrypt: Cipher 'AES-128-CBC' initialized with 128 bit key
Wed Nov 22 20:11:54 2017 Data Channel Encrypt: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed Nov 22 20:11:54 2017 Data Channel Decrypt: Cipher 'AES-128-CBC' initialized with 128 bit key
Wed Nov 22 20:11:54 2017 Data Channel Decrypt: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed Nov 22 20:11:54 2017 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Wed Nov 22 20:11:54 2017 [server] Peer Connection Initiated with [AF_INET]120.79.31.227:1194
Wed Nov 22 20:11:56 2017 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Wed Nov 22 20:11:56 2017 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 208.67.222.222,dhcp-option DNS 208.67.2
ute 10.8.0.1,topology net30,ping 10,ping-restart 120,ifconfig 10.8.0.6 10.8.0.5'
Wed Nov 22 20:11:56 2017 OPTIONS IMPORT: timers and/or timeouts modified
Wed Nov 22 20:11:56 2017 OPTIONS IMPORT: --ifconfig/up options modified
Wed Nov 22 20:11:56 2017 OPTIONS IMPORT: route options modified
Wed Nov 22 20:11:56 2017 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Wed Nov 22 20:11:56 2017 ROUTE_GATEWAY 172.18.184.254/255.255.0.0 IFACE=enp2s0 HWADDR=b0:83:fe:5a:18:ca
Wed Nov 22 20:11:56 2017 TUN/TAP device tun1 opened
Wed Nov 22 20:11:56 2017 TUN/TAP TX queue length set to 100
Wed Nov 22 20:11:56 2017 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Nov 22 20:11:56 2017 /sbin/ip link set dev tun1 up mtu 1500
Wed Nov 22 20:11:56 2017 /sbin/ip addr add dev tun1 local 10.8.0.6 peer 10.8.0.5
Wed Nov 22 20:11:56 2017 /sbin/ip route add 120.79.31.227/32 via 172.18.184.254
```

可以看到VPN已经连接成功。

我们再看看IP是否有修改。连接之前，在网站http://www.whatip.com/上查看原来的IP：



Your IP address: 120.236.174.167

Country:	China
Organization:	China Mobile Communications Corporation
City:	Beijing
Region:	Beijing
ISP:	China Mobile Communications Corporation

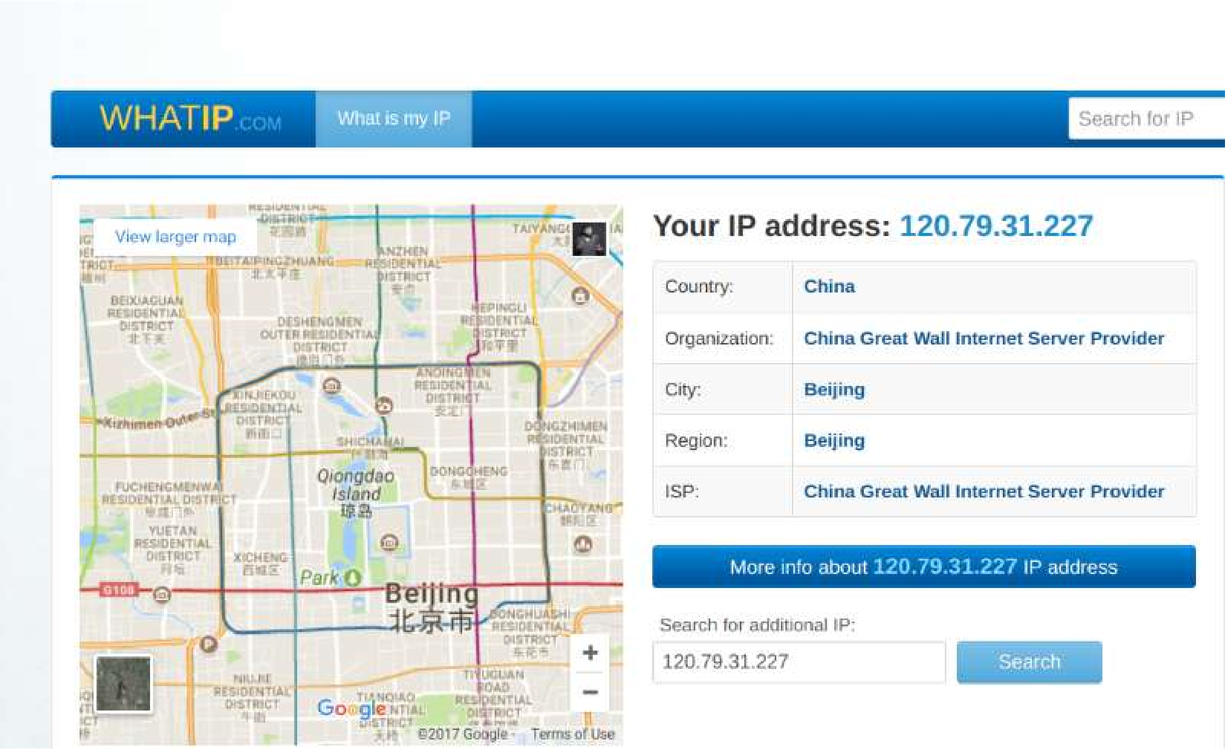
More info about 120.236.174.167 IP address

Search for additional IP:

120.236.174.167

Search

连接之后，IP被修改了：



Your IP address: 120.79.31.227

Country:	China
Organization:	China Great Wall Internet Server Provider
City:	Beijing
Region:	Beijing
ISP:	China Great Wall Internet Server Provider

More info about 120.79.31.227 IP address

Search for additional IP:

120.79.31.227

Search

IP为120.79.31.227说明VPN已经成功连接上云服务器。