# OpenVPN安装教程

## 一、简介

OpenVPN是一免费开源软件，以路由或桥接模式配置和远程访问设备的方式实现虚拟专用网络（vpn）创建安全的点 对点或站对站连接的解决方案。它使用SSL / TLS安全加密，具有穿越网络地址转换（NAT）和防火墙的功能。

## 二、服务端安装

## 服务器：CentOS Linux 6.6

本次部署openvpn服务端使用openvpn2.3.11，下载地址<https://openvpn.net/index.php/open-source/downloads.html>

这个版本中不包含easy-rsa，官网上也指明的：

”Starting with openvpn-2.3\_alpha2 easy-rsa is no longer part of the OpenVPN source or binary packages. It can be downloaded separately from it's GitHub project page.“

可以从github上下载easy-rsa3 ，下载地址<https://github.com/OpenVPN/openvpn>

### 1、安装lzo

lzo是致力于解压速度的一种数据压缩算法，可以使用源码包也可以使用yum安装

yum -y install lzo lzo-devel

备注：#如果有的话就不用安装openssl，一般CentOS已装

安装openssl 在linux终端输入以下命令

rpm -qa |grep openssl

yum install -y openssl openssl-devel

### 2、源码安装openvpn

将下载好的源码包上传到服务器的/soft目录下

[[root@localhost](mailto:root@localhost) ~]# ls -l /soft/openvpn-2.3.11.tar.gz

-rw-r--r--. 1 root root 1242816 May 27 10:07 /soft/openvpn-2.3.11.tar.gz

[[root@localhost](mailto:root@localhost) ~]# cd /soft/

[[root@localhost](mailto:root@localhost) soft]# tar -zxvf openvpn-2.3.11.tar.gz && cd openvpn-2.3.11

[[root@localhost](mailto:root@localhost) openvpn-2.3.11]# mkdir /usr/local/openvpn

[[root@localhost](mailto:root@localhost) openvpn-2.3.11]# ./configure --prefix=/usr/local/openvpn

[[root@localhost](mailto:root@localhost) openvpn-2.3.11]# make && make install

### 3、配置easyrsa服务端

[[root@localhost](mailto:root@localhost) openvpn-2.3.11]# cd /usr/local/openvpn/ [[root@localhost](mailto:root@localhost) openvpn]# git clone <https://github.com/OpenVPN/easy-rsa.git>

[[root@localhost](mailto:root@localhost) openvpn]# cd /usr/local/openvpn/easy-rsa/easyrsa3

[root@localhost easyrsa3]# cp vars.example vars

[root@localhost easyrsa3]# cat >>　vars　<< END

> set\_var EASYRSA\_REQ\_COUNTRY "CN"

> set\_var EASYRSA\_REQ\_PROVINCE "Shanghai"

> set\_var EASYRSA\_REQ\_CITY "Shanghai"

> set\_var EASYRSA\_REQ\_ORG "huatong Certificate"

> set\_var EASYRSA\_REQ\_EMAIL "barrywang@huatongsilver.com"

> set\_var EASYRSA\_REQ\_OU "huatong openvpn"

> END

[root@localhost easyrsa3]# grep ^set\_var vars

set\_var EASYRSA\_REQ\_COUNTRY "CN"

set\_var EASYRSA\_REQ\_PROVINCE "Shanghai"

set\_var EASYRSA\_REQ\_CITY "Shanghai"

set\_var EASYRSA\_REQ\_ORG "huatong Certificate"

set\_var EASYRSA\_REQ\_EMAIL "barrywang@huatongsilver.com"

set\_var EASYRSA\_REQ\_OU "huatong openvpn"

### 4、创建根证书、服务端证书和key

a、初始化pki目录

[[root@localhost](mailto:root@localhost) easyrsa3]# pwd

/usr/local/openvpn/easy-rsa/easyrsa3

[[root@localhost](mailto:root@localhost) easyrsa3]# ls

easyrsa openssl-1.0.cnf vars vars.example x509-types

[[root@localhost](mailto:root@localhost) easyrsa3]# ./easyrsa init-pki

Note: **using** Easy-RSA configuration **from**: ./vars

init-pki complete; you may now create a CA or requests.

Your newly created PKI dir **is**: /usr/local/openvpneasy-rsa/easyrsa3/pki

[[root@localhost](mailto:root@localhost) easyrsa3]# ls

easyrsa openssl-1.0.cnf pki vars vars.example x509-types

b、创建根证书

[root@localhost easyrsa3]# pwd

/usr/local/openvpn/easy-rsa/easyrsa3

[root@localhost easyrsa3]# ./easyrsa build-ca

Note: using Easy-RSA configuration from: ./vars

Generating a 2048 bit RSA **private** key

.............................................+++

........+++

writing **newprivate** key to '/usr/local/openvpn/easy-rsa/easyrsa3/pki/private/ca.key'

Enter PEM pass phrase: #输入密码，此密码用于证书签名

Verifying - Enter PEM pass phrase: #确认密码 如：vpn#2017

-----

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 **defaultvalue**,

If you enter '.', the field will be left blank.

-----

Common Name (eg: your user, host, or server name) [Easy-RSA CA]: server-openvpn

#输入一个Common Name普通名字 如server-openvpn

CA creation complete and you may now import and sign cert requests.

Your **new** CA certificate file **for** publishing **is** at:

/usr/local/openvpn/easy-rsa/easyrsa3/pki/ca.crt

c、创建服务端证书

[root@localhost easyrsa3]# ./easyrsa gen-req server nopass

Note: **using** Easy-RSA configuration **from**: ./vars

Generating a 2048 bit RSA **private** key

................................+++

......+++

writing **newprivate** key to '/usr/local/openvpn/easy-rsa/easyrsa3/pki/private/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 **defaultvalue**,

If you enter '.', the field will be left blank.

-----

Common Name (eg: your user, host, or server name) [server]:server

#该Common Name普通名字 一定不要与创建根证书的相同 如server

Keypair and certificate request completed. Your files are:

req: /usr/local/openvpn/easy-rsa/easyrsa3/pki/reqs/server.req

key: /usr/local/openvpn/easy-rsa/easyrsa3/pki/**private**/server.key

d、签约服务端证书

[root@vpn easyrsa3]*# ./easyrsa sign server server*

Note: using Easy-RSA configuration from: ./vars

You are about to sign the following certificate.

Please check over the details shown below **for** accuracy. Note that **this** request

has not been cryptographically verified. Please be sure it came from a trusted

source **or** that you have verified the request checksum with the sender.

Request subject, to be signed **as** a server certificate **for**3650 days:

subject=

commonName = server

Type the word 'yes' to **continue**, **or** any other input to abort.

Confirm request details: yes #输入yes继续

Using configuration from /root/openvpn-2.3.4/easy-rsa/easyrsa3/openssl-1.0.cnf

Enter pass phrase **for** /root/openvpn-2.3.4/easy-rsa/easyrsa3/pki/**private**/ca.key: #输入刚才创建根证书时的密码即vpn#2017

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

commonName :PRINTABLE:'server'

Certificate is to be certified until May 30 13:19:09 2026 GMT(3650 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /usr/local/openvpn/easy-rsa/easyrsa3/pki/issued/server.crt

### 5创建Diffie-Hellman，确保key穿越不安全网络的命令：

[root@vpn easyrsa3]**# ./easyrsa gen-dh**

Note: **using** Easy-RSA configuration **from**: ./vars

Generating DH parameters, 2048 bit **long** safe prime, generator 2

This **is** going to take a **long** time

...................................................................................................................................................................................................................+..........................................................................................................................+..................................................+.....................................................+..................................................................................................................................+............+............................................................................................................+...+............+...............+..............................................+.........................+..................................+.................+............................................................+..................................+........................................................................................................................................+................................................................+.......................................+...................................................................................................................................................++\*++\*

DH parameters of size 2048 created at /usr/local/openvpn/easy-rsa/easyrsa3/pki/dh.pem

把生成的 server.crt, server.key, dh.pem, ca.crt 拷贝到/usr/local/openvpn的ca目录，

[root@localhost openvpn]# pwd

/usr/local/openvpn

[root@localhost openvpn]# mkdir ca

[root@localhost openvpn]# cd ca

[root@localhost ca]#  find /usr/local/openvpn/easy-rsa/easyrsa3/ -name server.crt

/usr/local/openvpn/easy-rsa/easyrsa3/pki/issued/server.crt

[root@localhost ca]#  cp /usr/local/openvpn/easy-rsa/easyrsa3/pki/issued/server.crt .

[root@localhost ca]#  find /usr/local/openvpn/easy-rsa/easyrsa3/ -name server.key

/usr/local/openvpn/easy-rsa/easyrsa3/pki/private/server.key

[root@localhost ca]#  cp /usr/local/openvpn/easy-rsa/easyrsa3/pki/private/server.key .

[root@localhost ca]#  find /usr/local/openvpn/easy-rsa/easyrsa3/ -name dh.pem

/usr/local/openvpn/easy-rsa/easyrsa3/pki/dh.pem

[root@localhost ca]#  cp /usr/local/openvpn/easy-rsa/easyrsa3/pki/dh.pem .

[root@localhost ca]#  find /usr/local/openvpn/easy-rsa/easyrsa3/ -name ca.crt

/usr/local/openvpn/easy-rsa/easyrsa3/pki/ca.crt

[root@localhost ca]#  cp /usr/local/openvpn/easy-rsa/easyrsa3/pki/ca.crt .

[root@localhost ca]# ls

ca.crt dh.pem server.crt server.key

[root@localhost ca]# pwd

/usr/local/openvpn/ca

### 6、openvpn客户端证书生成

[root@localhost easyrsa3]# pwd

/usr/local/openvpn/easy-rsa/easyrsa3

[root@vpn easyrsa3]**#** ./easyrsa gen-req barry

Note: using Easy-RSA configuration from: ./vars

Generating a 2048 bit RSA private key

................+++

.........................................................+++

writing new private key to '/usr/local/openvpn/easy-rsa/easyrsa3/pki/private/barry.key.LsCjncfBX0'

Enter PEM pass phrase: #输入密码，此密码用于证书签名 此密码为 上面输入的vpn#2017

Verifying - Enter PEM pass phrase: #确认密码 vpn#2017

-----

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.

-----

Common Name (eg: your user, host, or server name) [barry]:barry

#输入一个Common Name普通名字 如barry

Keypair and certificate request completed. Your files are:

req: /usr/local/openvpn/easy-rsa/easyrsa3/pki/reqs/barry.req

key: /usr/local/openvpn/easy-rsa/easyrsa3/pki/private/barry.key

[root@vpn easyrsa3]**# ./easyrsa sign client barry**

Note: using Easy-RSA configuration from: ./vars

You are about to sign the following certificate.

Please check over the details shown below for accuracy. Note that this request

has not been cryptographically verified. Please be sure it came from a trusted

source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 3650 days:

subject=

commonName = barry

Type the word 'yes' to continue, or any other input to abort.

Confirm request details: yes

Using configuration from /usr/local/openvpn/easy-rsa/easyrsa3/openssl-1.0.cnf

Enter pass phrase for /usr/local/openvpn/easy-rsa/easyrsa3/pki/private/ca.key:

#输入密码，这里应是上面创建根证书时的密码 vpn#2017

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

commonName :PRINTABLE:'barry'

Certificate is to be certified until May 23 09:57:03 2027 GMT (3650 days)

Write out database with 1 new entries

Data Base Updated

Certificate created at: /usr/local/openvpn/easy-rsa/easyrsa3/pki/issued/barry.crt

### 7、修改服务端配置文件

当安装好openvpn时候，它会提供一个server配置的文件例子，根据需要修改配置文件

下面是我这边配置文件，根据需要修改

[root@localhost openvpn]# pwd

cd /usr/local/openvpn/

[root@localhost openvpn]# mkdir /var/log/openvpn

[root@localhost private]# view /var/log/openvpn/ipp.txt #如下可看到一些ip客户端信息

mapsic,172.25.10.4

zhao,172.25.10.8

lisizhen,172.25.10.12

cai,172.25.10.16

yfd,172.25.10.20

mu,172.25.10.24

ht01,172.25.10.28

ht02,172.25.10.32

[root@localhost openvpn]# find / -name server.conf -type f

/soft/openvpn-2.3.11/sample/sample-config-files/server.conf

[root@localhost openvpn]# cp /soft/openvpn-2.3.11/sample/sample-config-files/server.conf .

[[root@localhost](mailto:root@localhost) openvpn]# vim /usr/local/openvpn/server.conf

local 192.168.30.126

management localhost 1195

port 1194

proto tcp

dev tun

ca /usr/local/openvpn/ca/ca.crt

cert /usr/local/openvpn/ca/server.crt

key /usr/local/openvpn/ca/server.key

dh /usr/local/openvpn/ca/dh.pem

server 172.25.25.0 255.255.255.0

#配置VPN使用的网段，OpenVPN会自动提供基于该网段的DHCP服务，但不能和任何一方的局域网段重复，保证唯一这里我选择172.25.25.0。

ifconfig-pool-persist /var/log/openvpn/ipp.txt

# 维持一个客户端和virtual IP的对应表，以方便客户端重新连接可以获得同样的IP：/var/log/openvpn/ipp.txt

push "route 192.168.30.0 255.255.255.0"

push "route 192.168.90.0 255.255.255.0"

push "route 10.0.0.0 255.255.255.0"

# 为客户端创建对应的路由,以另其通达公司网内部服务器,这里push主要填写openvpn所在Linux服务器的局域网的网段.

client-to-client

# 默认客户端之间是不能直接通讯的，把语句的注释#去掉则客户端间可以通讯 client-to-client。

keepalive 10 120

comp-lzo # 使用lzo压缩的通讯

max-clients 100

# 如下让OpenVPN以nobody用户和组来运行（安全）

user nobody

group nobody

persist-key

persist-tun

status /var/log/openvpn/openvpn-status.log

log         /var/log/openvpn/openvpn.log

verb 3 # file verbosity.

### 8、开启路由转发

[[root@localhost](mailto:root@localhost) easyrsa3]# vim /etc/sysctl.conf

net.ipv4.ip\_forward = 1

[[root@localhost](mailto:root@localhost) easyrsa3]# sysctl -p

### 9、目的NAT转换

由于虚拟机没有公网地址，所以需要在路由器做nat转换

这一步就不截图了

iptables -t nat -A POSTROUTING -s 172.25.25.0/24 -o eth0 -j MASQUERADE

iptables -A INPUT -p TCP --dport 1194 -j ACCEPT

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

service iptables save

service iptables restart

### 10、配置静态路由

官网文档说明：Next, you must set up a route on the server-side LAN gateway to route the VPN client subnet (10.8.0.0/24) to the OpenVPN server (this is only necessary if the OpenVPN server and the LAN gateway are different machines).

在三层交换机上添加一条到172.25.10.0网络 即到vpn client子网的静态路由

### 11、启动OpenVPN

/usr/local/openvpn/sbin/openvpn --daemon --config /usr/local/openvpn/server.conf 回车

echo "/usr/local/openvpn/sbin/openvpn --daemon --config /usr/local/openvpn/server.conf & " >> /etc/rc.local回车

[root@ localhost openvpn]# ps -ef | grep openvpn

nobody 10389 1 0 08:43 ? 00:00:00 /usr/local/openvpn/sbin/openvpn --daemon --config /usr/local/openvpn/server.conf

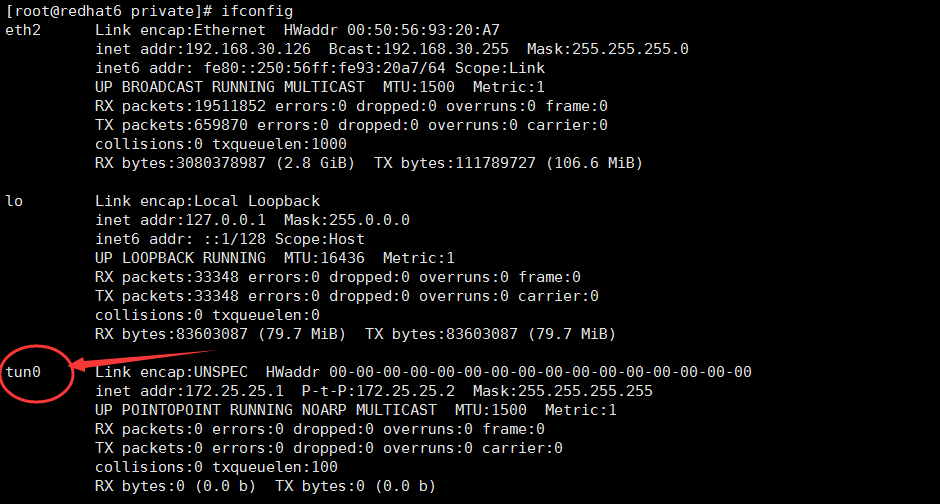
root 10406 115541 0 08:43 pts/2 00:00:00 grep openvpn

[root@ localhost openvpn]# netstat -lnatp | grep openvpn

tcp 0 0 127.0.0.1:1195 0.0.0.0:\* LISTEN 10389/openvpn

tcp 0 0 192.168.30.126:1194 0.0.0.0:\* LISTEN 10389/openvpn

**查看网卡信息： 注：其中tun0为虚拟出来的网卡。**



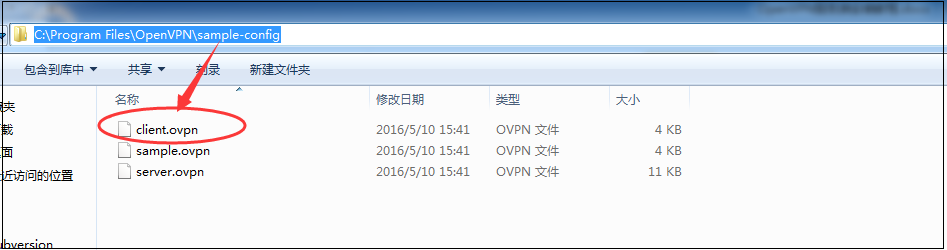
## 三、windows客户端配置

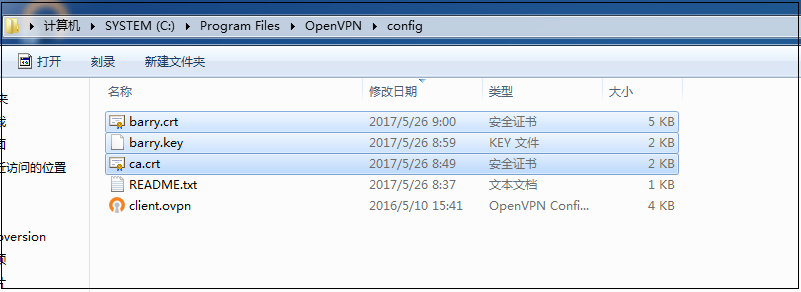
windows客户端安装openvpn-install-2.3.11-I001-x86\_64.exe，

将Linux服务器OPENVPN上面生成的三个文件(ca.crt, barry.crt，barry.key )下载到里面进行测试，

windows客户端上需要安装软件 软件下载路径：<https://openvpn.net/index.php/open-source/downloads.html>

复制证书和key文件到config目录下，并把如下windows客户端sample-config目录中的client.ovpn拷贝到config目录，





编辑client.ovpn（仅供参考根据需要修改）

client

dev tun

proto tcp

remote 192.168.30.126 1194 #这里是远程Linux的openvpn服务器ip和端口。

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert barry.crt

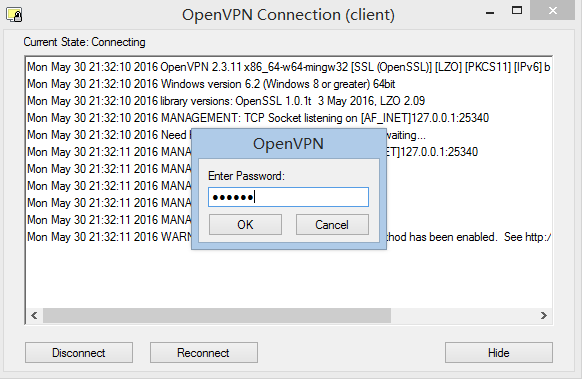
key  barry.key

comp-lzo

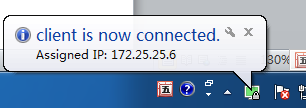
verb 3

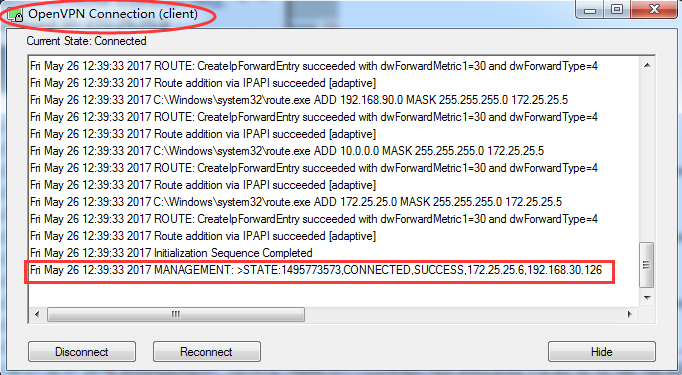
启动openvpn-gui测试, 输入证书密码 vpn#2017



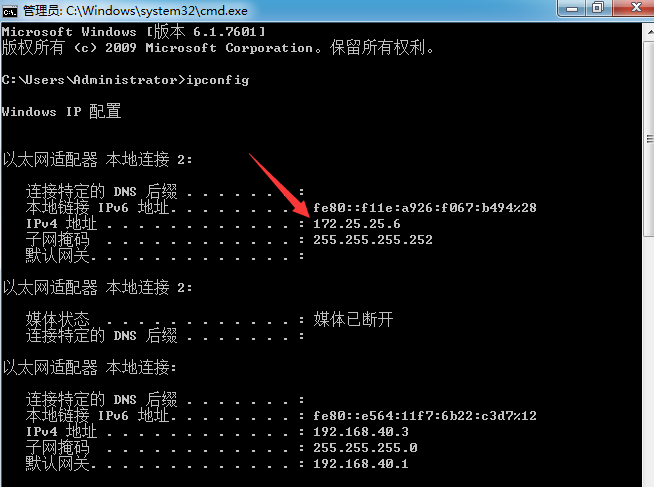


查看日志，连接成功

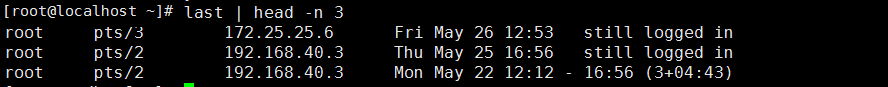




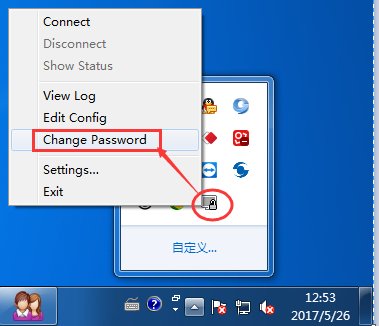
查看是否获取ip



访问虚拟机测试



修改密码的方式：尝试把原密码vpn#2017改为vpn#201705成功，





## 四、Linux客户端配置

1、直接用yum安装openvpn lzo openssl软件包

2、将ca证书用户证书和key复制到/etc/openvpn目录下

新建client.conf

client

dev tun

proto tcp

resolv-retry infinite

nobind

persist-key

persist-tun

ca /etc/openvpn/ca.crt

cert /etc/openvpn/mapsic.crt

key /etc/openvpn/mapsic.key

remote-cert-tls server

comp-lzo

verb 3

3开启

/usr/sbin/openvpn /etc/openvpn/client.conf

输入证书密码redhat

4访问测试

[[root@www](mailto:root@www) root]# telnet 192.168.30.61 22

Trying 192.168.30.61...

Connected to 192.168.30.61.

Escape character is '^]'.

SSH-2.0-OpenSSH\_5.3

5、关闭openvpn客户端直接用killall openvpn

[[root@www](mailto:root@www) ~]# killall openvpn