|  |
| --- |
| openvpn安装与使用 |
| **作者：**  **归档：学习笔记** |
| **快捷键：**  Ctrl + 1 标题1  Ctrl + 2 标题2  Ctrl + 3 标题3  Ctrl + 4 实例  Ctrl + 5 程序代码  Ctrl + 6 正文 |
| **格式说明：**  蓝色字体：注释  黄色背景：重要  绿色背景：注意 |

目 录

[第1章 openvpn原理 1](#_Toc493429588)

[第2章 安装openvpn 1](#_Toc493429589)

[2.1 环境准备 1](#_Toc493429590)

[2.2 安装openvpn server 1](#_Toc493429591)

[2.3 安装easy-rsa用来制作openvpn相关证书 2](#_Toc493429592)

[第3章 制作相关证书 3](#_Toc493429593)

[3.1 生成CA证书 3](#_Toc493429594)

[3.2 生成server端证书和秘钥 5](#_Toc493429595)

[3.3 创建迪菲・赫尔曼密钥 生成传输进行秘钥交换时用到的交换秘钥协议文件 7](#_Toc493429596)

[3.4 生成client客户端证书和key 8](#_Toc493429597)

[第4章 配置server端 12](#_Toc493429598)

[第5章 client端配置 13](#_Toc493429599)

[5.1 在server端操作 13](#_Toc493429600)

[5.2 Windows客户端上操作 15](#_Toc493429601)

[第6章 实现访问内网网段 17](#_Toc493429602)

[第7章 openvpn客户端证书的撤销 20](#_Toc493429603)

[7.1 撤销单个证书 20](#_Toc493429604)

[7.2 取消撤销 22](#_Toc493429605)

[第8章 配置linux下vpn客户端 22](#_Toc493429606)

[第9章 多机房利用vpn互联解决方案 22](#_Toc493429607)

[9.1 利用server或者client的ip地址作为各自客户端的网关来实现： 23](#_Toc493429608)

[9.2 利用网络路由来实现 25](#_Toc493429609)

[第10章 openvpn通过服务器代理上网（翻墙） 28](#_Toc493429610)

[第11章 openvpn负载均衡高可用 29](#_Toc493429611)

# openvpn原理

OpenVPN是一个用于创建虚拟专用网络(Virtual Private Network)加密通道的免费开源软件。使用OpenVPN可以方便地在家庭、办公场所、住宿酒店等不同网络访问场所之间搭建类似于局域网的专用网络通道。OpenVPN使用方便，运行性能优秀，支持Solaris、Linux 2.2+(Linux 2.2+表示Linux 2.2及以上版本，下同)、OpenBSD 3.0+、FreeBSD、NetBSD、Mac OS X、Android和Windows 2000+的操作系统，并且采用了高强度的数据加密，再加上其开源免费的特性，使得OpenVPN成为中小型企业及个人的VPN首选产品。

OpenVPN的运行原理其实很简单，其核心机制就是在OpenVPN服务器和客户端所在的计算机上都安装一个虚拟网卡(又称虚拟网络适配器)，并获得一个对应的虚拟IP地址。OpenVPN的服务器和多个客户端就可以通过虚拟网卡，使用这些虚拟IP进行相互访问了。其中，OpenVPN服务器起到一个路由和控制的作用(相当于一个虚拟的路由器)。

在OpenVPN中，最常用的数据加密手段，就是采用SSL协议。使用SSL协议进行传输就需要相应的证书和密钥，因此我们使用OpenVPN之前，还需要在服务器端生成相应的证书、密钥

# 安装openvpn

## 环境准备

yum方式安装，此处统一使用aliyun的base和epel源

wget -O /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-7.repo

为避免出现错误关闭selinux

[root@centos7 ~]# cat /etc/redhat-release

CentOS Linux release 7.2.1511 (Core)

[root@centos7 ~]# getenforce

Disabled

systemctl stop firewalld.service

## 安装openvpn server

yum install -y openvpn

#查看版本

[root@centos7 yum.repos.d]# openvpn --version

OpenVPN 2.4.3 x86\_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jun 21 2017

library versions: OpenSSL 1.0.1e-fips 11 Feb 2013, LZO 2.06

Originally developed by James Yonan

## 安装easy-rsa用来制作openvpn相关证书

yum install -y easy-rsa

#查看easy-rsa安装的详细信息

[root@centos7 ~]# rpm -qa easy-rsa

easy-rsa-2.2.2-1.el7.noarch

[root@centos7 ~]# rpm -ql easy-rsa

/usr/share/doc/easy-rsa-2.2.2

/usr/share/doc/easy-rsa-2.2.2/COPYING

/usr/share/doc/easy-rsa-2.2.2/COPYRIGHT.GPL

/usr/share/doc/easy-rsa-2.2.2/doc

/usr/share/doc/easy-rsa-2.2.2/doc/Makefile.am

/usr/share/doc/easy-rsa-2.2.2/doc/README-2.0

/usr/share/easy-rsa

/usr/share/easy-rsa/2.0

/usr/share/easy-rsa/2.0/build-ca

/usr/share/easy-rsa/2.0/build-dh

/usr/share/easy-rsa/2.0/build-inter

/usr/share/easy-rsa/2.0/build-key

/usr/share/easy-rsa/2.0/build-key-pass

/usr/share/easy-rsa/2.0/build-key-pkcs12

/usr/share/easy-rsa/2.0/build-key-server

/usr/share/easy-rsa/2.0/build-req

/usr/share/easy-rsa/2.0/build-req-pass

/usr/share/easy-rsa/2.0/clean-all

/usr/share/easy-rsa/2.0/inherit-inter

/usr/share/easy-rsa/2.0/list-crl

/usr/share/easy-rsa/2.0/openssl-0.9.6.cnf

/usr/share/easy-rsa/2.0/openssl-0.9.8.cnf

/usr/share/easy-rsa/2.0/openssl-1.0.0.cnf

/usr/share/easy-rsa/2.0/pkitool

/usr/share/easy-rsa/2.0/revoke-full

/usr/share/easy-rsa/2.0/sign-req

/usr/share/easy-rsa/2.0/vars

/usr/share/easy-rsa/2.0/whichopensslcnf

# 制作相关证书

## 生成CA证书

openvpn与easy-rsa安装完毕后，我们可以直接在/usr/share/easy-rsa/2.0 制作相关的证书，但是为了后续的管理证书的方便，我们需要在/etc/openvpn/目录下创建easy-rsa文件夹， 然后把/usr/share/easy-rsa/目录下的所有文件全部复制到/etc/openvpn/easy-rsa/下：

[root@centos7 ~]# mkdir /etc/openvpn/easy-rsa

[root@centos7 ~]# cp -a /usr/share/easy-rsa/2.0/\* /etc/openvpn/easy-rsa/

[root@centos7 ~]# ls -l /etc/openvpn/easy-rsa/

总用量 112

-rwxr-xr-x 1 root root 119 11月 9 2013 build-ca

-rwxr-xr-x 1 root root 352 11月 9 2013 build-dh

-rwxr-xr-x 1 root root 188 11月 9 2013 build-inter

-rwxr-xr-x 1 root root 163 11月 9 2013 build-key

-rwxr-xr-x 1 root root 157 11月 9 2013 build-key-pass

-rwxr-xr-x 1 root root 249 11月 9 2013 build-key-pkcs12

-rwxr-xr-x 1 root root 268 11月 9 2013 build-key-server

-rwxr-xr-x 1 root root 213 11月 9 2013 build-req

-rwxr-xr-x 1 root root 158 11月 9 2013 build-req-pass

-rwxr-xr-x 1 root root 449 11月 9 2013 clean-all

-rwxr-xr-x 1 root root 1471 11月 9 2013 inherit-inter

-rwxr-xr-x 1 root root 302 11月 9 2013 list-crl

-rw-r--r-- 1 root root 7791 11月 9 2013 openssl-0.9.6.cnf

-rw-r--r-- 1 root root 8348 11月 9 2013 openssl-0.9.8.cnf

-rw-r--r-- 1 root root 8245 11月 9 2013 openssl-1.0.0.cnf

-rwxr-xr-x 1 root root 12966 11月 9 2013 pkitool

-rwxr-xr-x 1 root root 928 11月 9 2013 revoke-full

-rwxr-xr-x 1 root root 178 11月 9 2013 sign-req

-rw-r--r-- 1 root root 2077 11月 9 2013 vars

-rwxr-xr-x 1 root root 740 11月 9 2013 whichopensslcnf

#编辑vars文件，修改生成证书需要的信息

[root@centos7 ~]# cd /etc/openvpn/easy-rsa/

[root@centos7 easy-rsa]# cp vars{,.bak}

[root@centos7 easy-rsa]# vim vars

...

export KEY\_COUNTRY="CN" #国家

export KEY\_PROVINCE="BJ" #省

export KEY\_CITY="Beijing" #市

export KEY\_ORG="user" #组织

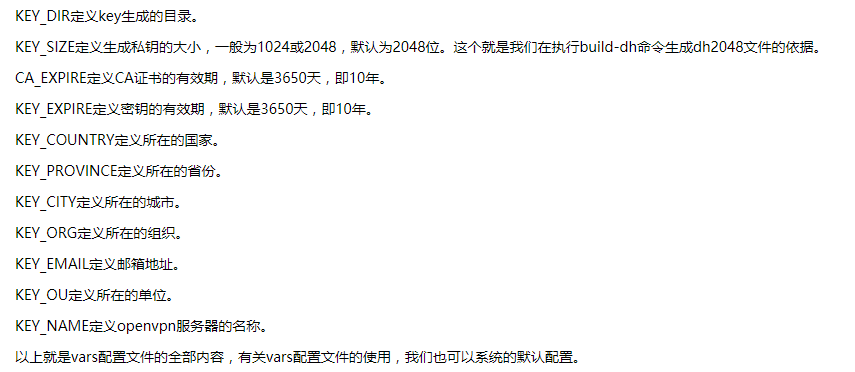
export KEY\_EMAIL="123@qq.com" #邮件

export KEY\_CN=oldboy

export KEY\_NAME=beyond #定义openvpn服务器的名称

export KEY\_OU=beyond #定义所在的单位

...



#用source命令使配置生效

[root@centos7 easy-rsa]# source vars

NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys

[root@centos7 easy-rsa]# ./clean-all #清除所有证书相关内容

[root@centos7 easy-rsa]# #开始生成CA证书 一路回车即可

[root@centos7 easy-rsa]# ./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) [BJ]:

Locality Name (eg, city) [Beijing]:

Organization Name (eg, company) [user]:

Organizational Unit Name (eg, section) [beyond]:

Common Name (eg, your name or your server's hostname) [oldboy]:

Name [beyond]:

Email Address [123@qq.com]:

#查看生成的证书

[root@centos7 easy-rsa]# ll keys/

总用量 12

-rw-r--r-- 1 root root 1635 9月 10 18:31 ca.crt

-rw------- 1 root root 1704 9月 10 18:31 ca.key

-rw-r--r-- 1 root root 0 9月 10 18:30 index.txt

-rw-r--r-- 1 root root 3 9月 10 18:30 serial

#我们可以看到已经生成了ca.crt和ca.key两个文件，其中ca.crt就是我们所说的CA证书，把该CA证书的ca.crt文件复制到openvpn的启动目录/etc/openvpn下：

[root@centos7 easy-rsa]# cp keys/ca.crt /etc/openvpn/

[root@centos7 easy-rsa]# ll /etc/openvpn/

总用量 8

-rw-r--r-- 1 root root 1635 9月 10 18:37 ca.crt

drwxr-x--- 2 root root 6 6月 21 18:23 client

drwxr-xr-x 3 root root 4096 9月 10 18:30 easy-rsa

drwxr-x--- 2 root root 6 6月 21 18:23 server

## 生成server端证书和秘钥

[root@centos7 easy-rsa]# ./build-key-server vpnserver

Generating a 2048 bit RSA private key

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

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

writing new private key to 'vpnserver.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) [BJ]:

Locality Name (eg, city) [Beijing]:

Organization Name (eg, company) [user]:

Organizational Unit Name (eg, section) [beyond]:

Common Name (eg, your name or your server's hostname) [vpnserver]:

Name [beyond]:

Email Address [123@qq.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:123456 #秘钥保护的密码 可以为空

An optional company name []:oldboy #可选的组织名 可以为空

Using configuration from /etc/openvpn/easy-rsa/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:'BJ'

localityName :PRINTABLE:'Beijing'

organizationName :PRINTABLE:'user'

organizationalUnitName:PRINTABLE:'beyond'

commonName :PRINTABLE:'vpnserver'

name :PRINTABLE:'beyond'

emailAddress :IA5STRING:'123@qq.com'

Certificate is to be certified until Sep 8 10:46:28 2027 GMT (3650 days)

Sign the certificate? [y/n]:y #签署的证书吗?



1 out of 1 certificate requests certified, commit? [y/n]y #1/1的证书请求认证，提交?

Write out database with 1 new entries

Data Base Updated

[root@centos7 easy-rsa]# #查看生成的证书

[root@centos7 easy-rsa]# ll keys/

总用量 48

-rw-r--r-- 1 root root 5337 9月 10 18:46 01.pem

-rw-r--r-- 1 root root 1635 9月 10 18:31 ca.crt

-rw------- 1 root root 1704 9月 10 18:31 ca.key

-rw-r--r-- 1 root root 116 9月 10 18:46 index.txt

-rw-r--r-- 1 root root 21 9月 10 18:46 index.txt.attr

-rw-r--r-- 1 root root 0 9月 10 18:30 index.txt.old

-rw-r--r-- 1 root root 3 9月 10 18:46 serial

-rw-r--r-- 1 root root 3 9月 10 18:30 serial.old

-rw-r--r-- 1 root root 5337 9月 10 18:46 vpnserver.crt

-rw-r--r-- 1 root root 1119 9月 10 18:46 vpnserver.csr

-rw------- 1 root root 1704 9月 10 18:46 vpnserver.key

## 创建迪菲・赫尔曼密钥 生成传输进行秘钥交换时用到的交换秘钥协议文件

[root@centos7 easy-rsa]# ./build-dh #这个过程持续时间长，请耐心等待

Generating DH parameters, 2048 bit long safe prime, generator 2 #生成DH参数，2048位长安全质数，发电机2

This is going to take a long time

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

#查看生成的文件

[root@centos7 easy-rsa]# ll keys/

总用量 52

-rw-r--r-- 1 root root 5337 9月 10 18:46 01.pem

-rw-r--r-- 1 root root 1635 9月 10 18:31 ca.crt

-rw------- 1 root root 1704 9月 10 18:31 ca.key

-rw-r--r-- 1 root root 424 9月 10 18:54 dh2048.pem

-rw-r--r-- 1 root root 116 9月 10 18:46 index.txt

-rw-r--r-- 1 root root 21 9月 10 18:46 index.txt.attr

-rw-r--r-- 1 root root 0 9月 10 18:30 index.txt.old

-rw-r--r-- 1 root root 3 9月 10 18:46 serial

-rw-r--r-- 1 root root 3 9月 10 18:30 serial.old

-rw-r--r-- 1 root root 5337 9月 10 18:46 vpnserver.crt

-rw-r--r-- 1 root root 1119 9月 10 18:46 vpnserver.csr

-rw------- 1 root root 1704 9月 10 18:46 vpnserver.key

已经生成了dh文件dh2048.pem。 把vpnserver.crt、vpnserver.key、dh2048.pem复制到/etc/openvpn/目录下

[root@centos7 easy-rsa]# cp keys/dh2048.pem keys/vpnserver.crt keys/vpnserver.key /etc/openvpn/

## 生成client客户端证书和key

[root@centos7 easy-rsa]# ./build-key vpnclient #拨号时不需要密码

Generating a 2048 bit RSA private key

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

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

writing new private key to 'vpnclient.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) [BJ]:

Locality Name (eg, city) [Beijing]:

Organization Name (eg, company) [user]:

Organizational Unit Name (eg, section) [beyond]:

Common Name (eg, your name or your server's hostname) [vpnclient]:

Name [beyond]:

Email Address [123@qq.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:123456 #此处密码与服务端一致即可

An optional company name []:oldboy

Using configuration from /etc/openvpn/easy-rsa/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:'BJ'

localityName :PRINTABLE:'Beijing'

organizationName :PRINTABLE:'user'

organizationalUnitName:PRINTABLE:'beyond'

commonName :PRINTABLE:'vpnclient'

name :PRINTABLE:'beyond'

emailAddress :IA5STRING:'123@qq.com'

Certificate is to be certified until Sep 8 11:44:26 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

#查看生成的文件

[root@centos7 easy-rsa]# ll keys/

总用量 84

-rw-r--r-- 1 root root 5337 9月 10 18:46 01.pem

-rw-r--r-- 1 root root 5219 9月 10 19:44 02.pem

-rw-r--r-- 1 root root 1635 9月 10 18:31 ca.crt

-rw------- 1 root root 1704 9月 10 18:31 ca.key

-rw-r--r-- 1 root root 424 9月 10 18:54 dh2048.pem

-rw-r--r-- 1 root root 232 9月 10 19:44 index.txt

-rw-r--r-- 1 root root 21 9月 10 19:44 index.txt.attr

-rw-r--r-- 1 root root 21 9月 10 18:46 index.txt.attr.old

-rw-r--r-- 1 root root 116 9月 10 18:46 index.txt.old

-rw-r--r-- 1 root root 3 9月 10 19:44 serial

-rw-r--r-- 1 root root 3 9月 10 18:46 serial.old

-rw-r--r-- 1 root root 5219 9月 10 19:44 vpnclient.crt

-rw-r--r-- 1 root root 1119 9月 10 19:44 vpnclient.csr

-rw------- 1 root root 1704 9月 10 19:44 vpnclient.key

-rw-r--r-- 1 root root 5337 9月 10 18:46 vpnserver.crt

-rw-r--r-- 1 root root 1119 9月 10 18:46 vpnserver.csr

-rw------- 1 root root 1704 9月 10 18:46 vpnserver.key

#生成拨号时需要密码的客户端文件和证书，和上面两者选择一种就可以

[root@centos7 easy-rsa]# ./build-key-pass vpnbeyond

Generating a 2048 bit RSA private key

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

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

writing new private key to 'vpnbeyond.key'

Enter PEM pass phrase:123456 #质子交换膜（PEM）通段。

Verifying - Enter PEM pass phrase:123456

-----

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) [BJ]:

Locality Name (eg, city) [Beijing]:

Organization Name (eg, company) [user]:

Organizational Unit Name (eg, section) [beyond]:

Common Name (eg, your name or your server's hostname) [vpnbeyond]:

Name [beyond]:

Email Address [123@qq.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:123456

An optional company name []:oldboy

Using configuration from /etc/openvpn/easy-rsa/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:'BJ'

localityName :PRINTABLE:'Beijing'

organizationName :PRINTABLE:'user'

organizationalUnitName:PRINTABLE:'beyond'

commonName :PRINTABLE:'vpnbeyond'

name :PRINTABLE:'beyond'

emailAddress :IA5STRING:'123@qq.com'

Certificate is to be certified until Sep 8 11:48:10 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

#查看生成的文件

[root@centos7 easy-rsa]# ll keys/

总用量 108

-rw-r--r-- 1 root root 5337 9月 10 18:46 01.pem

-rw-r--r-- 1 root root 5219 9月 10 19:44 02.pem

-rw-r--r-- 1 root root 5219 9月 10 19:48 03.pem

-rw-r--r-- 1 root root 1635 9月 10 18:31 ca.crt

-rw------- 1 root root 1704 9月 10 18:31 ca.key

-rw-r--r-- 1 root root 424 9月 10 18:54 dh2048.pem

-rw-r--r-- 1 root root 348 9月 10 19:48 index.txt

-rw-r--r-- 1 root root 21 9月 10 19:48 index.txt.attr

-rw-r--r-- 1 root root 21 9月 10 19:44 index.txt.attr.old

-rw-r--r-- 1 root root 232 9月 10 19:44 index.txt.old

-rw-r--r-- 1 root root 3 9月 10 19:48 serial

-rw-r--r-- 1 root root 3 9月 10 19:44 serial.old

-rw-r--r-- 1 root root 5219 9月 10 19:48 vpnbeyond.crt

-rw-r--r-- 1 root root 1119 9月 10 19:48 vpnbeyond.csr

-rw------- 1 root root 1834 9月 10 19:48 vpnbeyond.key

-rw-r--r-- 1 root root 5219 9月 10 19:44 vpnclient.crt

-rw-r--r-- 1 root root 1119 9月 10 19:44 vpnclient.csr

-rw------- 1 root root 1704 9月 10 19:44 vpnclient.key

-rw-r--r-- 1 root root 5337 9月 10 18:46 vpnserver.crt

-rw-r--r-- 1 root root 1119 9月 10 18:46 vpnserver.csr

-rw------- 1 root root 1704 9月 10 18:46 vpnserver.key

已经生成了vpnclient.csr、vpnclient.crt和vpnclient.key这个三个文件, vpnclient.crt和vpnclient.key两个文件是我们要使用的。至此，Client端证书就制作完毕。

# 配置server端

[root@centos7 easy-rsa]# cp /usr/share/doc/openvpn-2.4.4/sample/sample-config-files/server.conf /etc/openvpn/server.conf.bak

[root@centos7 easy-rsa]# cd /etc/openvpn/

[root@centos7 openvpn]# grep -Ev "^;|^#|^$" server.conf.bak >server.conf

[root@centos7 openvpn]# vim server.conf

port 1194

proto tcp

dev tun

ca ca.crt

cert vpnserver.crt

key vpnserver.key # This file should be kept secret

dh dh2048.pem

server 10.8.0.0 255.255.255.0

push "route 172.16.1.0 255.255.255.0"

ifconfig-pool-persist ipp.txt

keepalive 10 120

comp-lzo

persist-key

persist-tun

status openvpn-status.log

verb 3

client-to-client

duplicate-cn

log /var/log/openvpn.log

~

~

"server.conf" 19L, 360C 已写入

#启动服务

[root@centos7 openvpn]# systemctl start openvpn@server

[root@centos7 openvpn]# ss -lntup |grep openvpn

tcp LISTEN 0 1 \*:1194 \*:\* users:(("openvpn",pid=19333,fd=6))

# Windows client端配置

## 在server端操作

创建客户端文件夹并拷贝客户端文件到该文件夹配置完成后打包压缩下载到本地Windows端

[root@centos7 openvpn]# mkdir vpnclient

[root@centos7 openvpn]# cp /usr/share/doc/openvpn-2.4.4/sample/sample-config-files/client.conf ./vpnclient/vpnclient.ovpn

[root@centos7 openvpn]# pwd

/etc/openvpn

[root@centos7 openvpn]# cp easy-rsa/keys/vpnclient.crt easy-rsa/keys/vpnclient.key easy-rsa/keys/ca.crt easy-rsa/keys/ca.key ./vpnclient/

[root@centos7 openvpn]# ls -l vpnclient/

总用量 24

-rw-r--r-- 1 root root 1635 9月 10 21:22 ca.crt

-rw------- 1 root root 1704 9月 10 21:22 ca.key

-rw-r--r-- 1 root root 5219 9月 10 21:22 vpnclient.crt

-rw------- 1 root root 1704 9月 10 21:22 vpnclient.key

-rw-r--r-- 1 root root 3584 9月 10 21:17 vpnclient.ovpn

[root@centos7 openvpn]# cp vpnclient/vpnclient.ovpn{,.bak}

[root@centos7 openvpn]# vim vpnclient/vpnclient.ovpn

ns-cert-type server

client

dev tun

proto tcp

remote 10.0.0.201 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert vpnclient.crt

key vpnclient.key

ns-cert-type server

comp-lzo

verb 3

~

"vpnclient/vpnclient.ovpn" 14L, 184C 已写入

[root@centos7 openvpn]# zip -r vpnclient.zip ./vpnclient/

adding: vpnclient/ (stored 0%)

adding: vpnclient/vpnclient.crt (deflated 47%)

adding: vpnclient/vpnclient.key (deflated 23%)

adding: vpnclient/ca.crt (deflated 35%)

adding: vpnclient/ca.key (deflated 23%)

adding: vpnclient/vpnclient.ovpn.bak (deflated 54%)

adding: vpnclient/vpnclient.ovpn (deflated 30%)

[root@centos7 openvpn]# ls

ca.crt easy-rsa server vpnclient vpnserver.key

client ipp.txt server.conf vpnclient.zip

dh2048.pem openvpn-status.log server.conf.bak vpnserver.crt

[root@centos7 openvpn]# sz vpnclient.zip -y

rz

zmodem trl+C ȡ

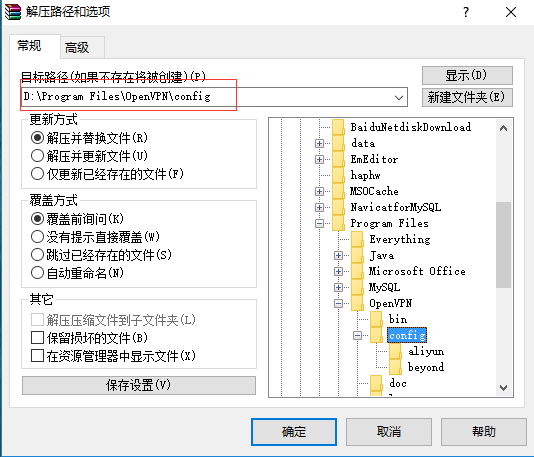
100% 9 KB 9 KB/s 00:00:01 0 Errors

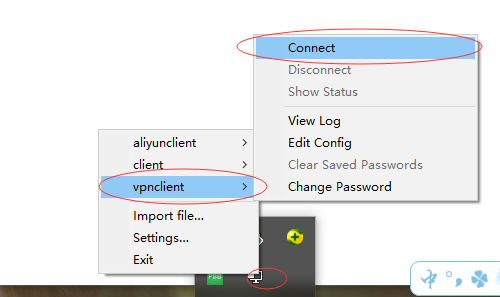
## Windows客户端上操作

在windows的Client端，安装完毕Openvpn后，程序安装路径是：D:\ProgramFiles\OpenVPN\，如下图解压sz下载的压缩包到config目录下：

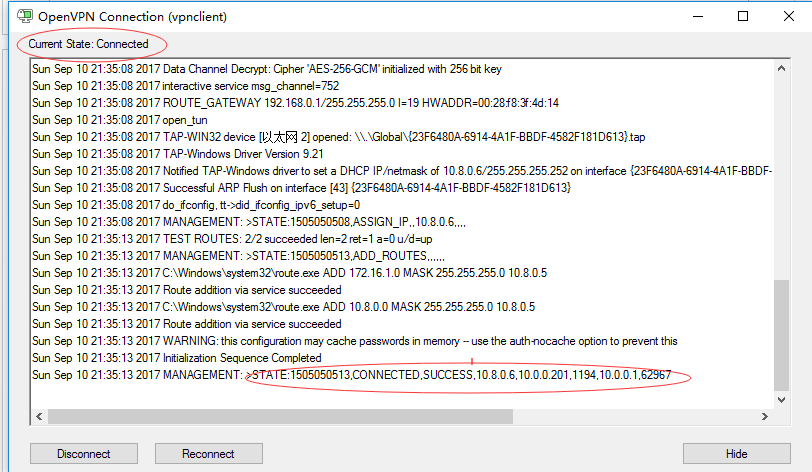
<http://openvpn.ustc.edu.cn/> #windows客户端openvpn安装包网站地址



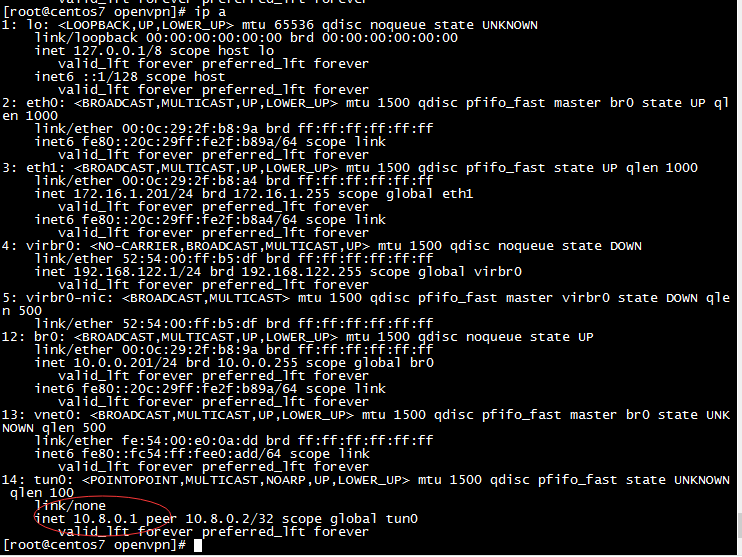


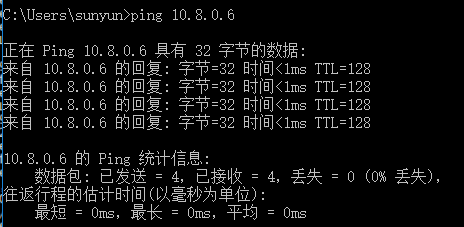


双击桌面openvpn图标如上图点击连接后会成功拨号如下所示（win10系统右击后直接出现connect）：分配的ip地址是10.8.0.6



在vpnserver端查看IP地址如下图分配的IP地址是10.8.0.1，然后在Windows端ping10.8.0.6即可ping通，当然用crt或者xshell也可连接上





# 实现访问内网网段

#开启ipv4转发

[root@centos7 openvpn]# echo 'net.ipv4.ip\_forward =1' >> /etc/sysctl.conf [root@centos7 openvpn]# sysctl -p

net.ipv4.ip\_forward = 1

[root@centos7 openvpn]# grep net.ip /etc/sysctl.conf

net.ipv4.ip\_forward =1

#抓包

[root@centos7 openvpn]# yum install tcpdump -y #若没有tcpdump这个命令，请提前安装

[root@centos7 openvpn]# tcpdump -i eth1 #再开一台同网段的机器

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes

22:41:22.362365 ARP, Request who-has 172.16.1.62 tell 172.16.1.201, length 28

22:41:22.362767 ARP, Reply 172.16.1.62 is-at 00:0c:29:e7:44:c0 (oui Unknown), length 46

22:41:22.362778 IP 10.8.0.6 > 172.16.1.62: ICMP echo request, id 1, seq 329, length 40

22:41:27.032841 IP 10.8.0.6 > 172.16.1.62: ICMP echo request, id 1, seq 330, length 40

22:41:32.032299 IP 10.8.0.6 > 172.16.1.62: ICMP echo request, id 1, seq 331, length 40

22:41:37.032198 IP 10.8.0.6 > 172.16.1.62: ICMP echo request, id 1, seq 332, length 40

#通过抓包可以发现数据包到达vpn的内部机器上没有返回

#解决方法1：在vpn的内部机器上添加返回路由或干脆把vpn server作为vpn内部机器的网关

#在vpn内部机器172.16.1.62上配置

[root@localhost ~]# ip a

3: eth1: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP qlen 1000

link/ether 00:0c:29:e7:44:c0 brd ff:ff:ff:ff:ff:ff

inet 172.16.1.62/24 brd 172.16.1.255 scope global eth1

inet6 fe80::20c:29ff:fee7:44c0/64 scope link

valid\_lft forever preferred\_lft forever

[root@localhost ~]# route add -net 10.8.0.0/24 gw 172.16.1.201

[root@localhost ~]# tcpdump -i eth1

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes

22:52:47.063020 IP 10.8.0.6 > 172.16.1.62: ICMP echo request, id 1, seq 366, length 40

22:52:47.063044 IP 172.16.1.62 > 10.8.0.6: ICMP echo reply, id 1, seq 366, length 40

22:52:48.063590 ARP, Request who-has 172.16.1.62 tell 172.16.1.201, length 46

22:52:48.063605 ARP, Reply 172.16.1.62 is-at 00:0c:29:e7:44:c0 (oui Unknown), length 28

22:52:48.065214 IP 10.8.0.6 > 172.16.1.62: ICMP echo request, id 1, seq 367, length 40

22:52:48.065231 IP 172.16.1.62 > 10.8.0.6: ICMP echo reply, id 1, seq 367, length 40

[root@localhost ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0

10.8.0.0 172.16.1.201 255.255.255.0 UG 0 0 0 eth1

172.16.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1002 0 0 eth0

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

0.0.0.0 10.0.0.254 0.0.0.0 UG 0 0 0 eth0

#或者：

route add default gw 172.16.1.201

#此方法虽然实现了访问vpn内部机器的功能，但是当vpn内部机器有很多台的时候此方法就不好了，所以有第二种方法：在vpn服务器上配置防火墙转发

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth1 -j MASQUERADE #伪装，适合没有固定IP的

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth1 -j SNAT --to-source 172.16.1.201 #有固定IP地址，注意这里区分大小写

iptables -F

iptables -t nat -L -n

iptables -t filter -L -n

#/etc/init.d/iptables save

#/etc/init.d/iptables restart

[root@localhost ~]# tcpdump -i eth1

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes

23:51:59.411144 IP 172.16.1.201 > 172.16.1.62: ICMP echo request, id 1, seq 393, length 40

23:51:59.411190 IP 172.16.1.62 > 172.16.1.201: ICMP echo reply, id 1, seq 393, length 40

23:52:00.412799 IP 172.16.1.201 > 172.16.1.62: ICMP echo request, id 1, seq 394, length 40

23:52:00.412819 IP 172.16.1.62 > 172.16.1.201: ICMP echo reply, id 1, seq 394, length 40

# openvpn客户端证书的撤销

## 撤销单个证书

[root@centos7 sample-config-files]# cd /etc/openvpn/easy-rsa/

[root@centos7 easy-rsa]# ls

build-ca build-key-pkcs12 inherit-inter openssl-1.0.0.cnf vars.bak

build-dh build-key-server keys pkitool whichopensslcnf

build-inter build-req list-crl revoke-full

build-key build-req-pass openssl-0.9.6.cnf sign-req

build-key-pass clean-all openssl-0.9.8.cnf vars

[root@centos7 easy-rsa]# source vars

NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys

[root@centos7 easy-rsa]# ./revoke-full vpnclient

Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf

Revoking Certificate 02.

Data Base Updated

Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf

vpnclient.crt: C = CN, ST = BJ, L = Beijing, O = user, OU = beyond, CN = vpnclient, name = beyond, emailAddress = 123@qq.com

error 23 at 0 depth lookup:certificate revoked

[root@centos7 easy-rsa]# ll keys/crl.pem

-rw-r--r-- 1 root root 715 9月 11 00:42 keys/crl.pem

[root@centos7 easy-rsa]# cat keys/crl.pem

-----BEGIN X509 CRL-----

MIIB5jCBzzANBgkqhkiG9w0BAQsFADCBiTELMAkGA1UEBhMCQ04xCzAJBgNVBAgT

AkJKMRAwDgYDVQQHEwdCZWlqaW5nMQ0wCwYDVQQKEwR1c2VyMQ8wDQYDVQQLEwZi

ZXlvbmQxDzANBgNVBAMTBm9sZGJveTEPMA0GA1UEKRMGYmV5b25kMRkwFwYJKoZI

hvcNAQkBFgoxMjNAcXEuY29tFw0xNzA5MTAxNjQyMDBaFw0xNzEwMTAxNjQyMDBa

MBQwEgIBAhcNMTcwOTEwMTY0MjAwWjANBgkqhkiG9w0BAQsFAAOCAQEAFPEKfUoF

wayBHlI1FE3prhAN53C0wJm0IUpwBuRDC8XbPLPMTX3dzps1Jmatw0BVX++IlvGJ

z7lrxZpFXPbCr44m9rDpOMHdbwgrqchMCpyBX4N3qRAd1rDXbeahb/n0GhRbPudD

EeRodU07aT9AQ5kpp0occPZsiSFuypwemegdan3l2KNus4vdABrE6bRpCfE1Xizb

NqKDNIf44ewvelP8m9XGR8o84hD5jgJtL2Cqx5Hfc7vxm8PIIn4Ne1KfdgT6U0pB

ssyXsAAMfTTrDiiazcu8PFaomMBhtDJghZLs1td5bkYSLbkpgT4hKQumcZgZqj9V

F4aCaqe6+wQjXA==

-----END X509 CRL-----

[root@centos7 easy-rsa]# cat keys/index.txt

V 270908104628Z 01 unknown /C=CN/ST=BJ/L=Beijing/O=user/OU=beyond/CN=vpnserver/name=beyond/emailAddress=123@qq.com

R 270908114426Z 170910164200Z 02 unknown /C=CN/ST=BJ/L=Beijing/O=user/OU=beyond/CN=vpnclient/name=beyond/emailAddress=123@qq.com

V 270908114810Z 03 unknown /C=CN/ST=BJ/L=Beijing/O=user/OU=beyond/CN=vpnbeyond/name=beyond/emailAddress=123@qq.com

#编辑vpn服务端配置文件增加如下配置

crl-verify /etc/openvpn/easy-rsa/keys/crl.pem

#重启服务

[root@centos7 easy-rsa]# systemctl restart openvpn@server.service

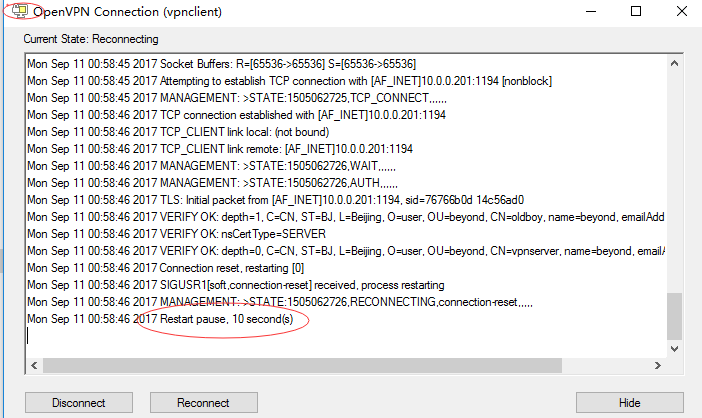
[root@centos7 easy-rsa]# systemctl stop openvpn@server.service

[root@centos7 easy-rsa]# ss -lntup|grep openvpn

[root@centos7 easy-rsa]# systemctl start openvpn@server.service

[root@centos7 easy-rsa]# ss -lntup|grep openvpn

tcp LISTEN 0 1 \*:1194 \*:\* users:(("openvpn",pid=22972,fd=6))



此时会发现证书已吊销无法登陆。

## 取消撤销

如果发现撤销错误需要回退的时候只需要将配置文件中加的内容注释掉然后再重启服务即可。

# 配置linux下vpn客户端

安装过程和linux下vpn server端一样

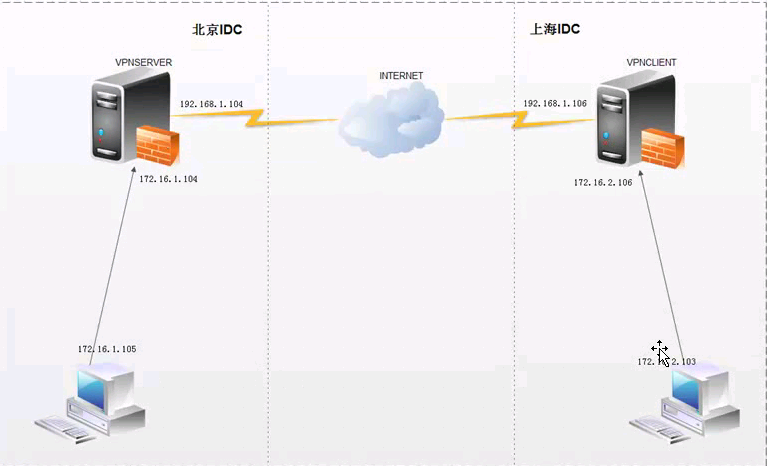
yum install -y openvpn

将window客户端config文件夹下的客户端文件打成zip包上传到linux客户端服务器的/etc/openvpn目录下并解压，将配置文件重命名为client.conf

#启动：

openvpn /etc/openvpn/client.conf &

# 多机房利用vpn互联解决方案



* 用vpnserver和vpnclient的eth1 ip地址作为各自客户端的网关
* 添加网络路由

## 利用server或者client的ip地址作为各自客户端的网关来实现：

服务端的配置：

[root@localhost openvpn]# cat /etc/openvpn/server.conf

port 1194

proto tcp

dev tun

ca ca.crt

cert vpnserver.crt

key vpnserver.key # This file should be kept secret

dh dh2048.pem

client-config-dir /etc/openvpn/ccd

server 10.8.0.0 255.255.255.0

push "route 172.16.1.0 255.255.255.0"

#push "route 192.168.1.0 255.255.255.0"

#route 172.16.1.0 255.255.255.0

route 192.168.1.0 255.255.255.0

ifconfig-pool-persist ipp.txt

keepalive 10 120

comp-lzo

persist-key

persist-tun

status openvpn-status.log

verb 3

client-to-client

log /var/log/openvpn.log

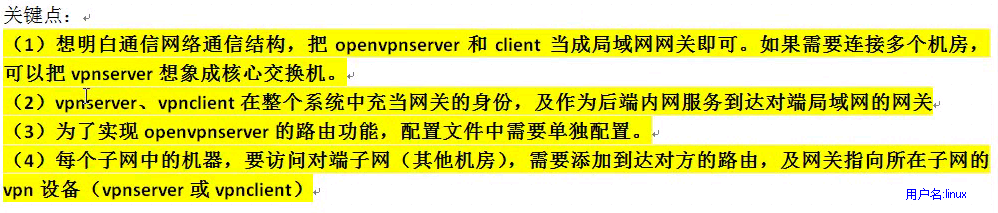
mkdir /etc/openvpn/ccd

[root@localhost openvpn]# cat ccd/beyond

iroute 192.168.1.0 255.255.255.0

ifconfig-push 10.8.0.3 10.8.0.4

#配置完成后重启openvpn服务



## 利用网络路由来实现

#在172.16.1.6上操作

[root@lb02 ~]# ifconfig eth1

eth1 Link encap:Ethernet HWaddr 00:0C:29:CF:56:A0

inet addr:172.16.1.6 Bcast:172.16.1.255 Mask:255.255.255.0

[root@lb02 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

172.16.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

0.0.0.0 172.16.1.62 0.0.0.0 UG 0 0 0 eth1

[root@lb02 ~]# route del default gw 172.16.1.62

[root@lb02 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

172.16.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

#在192.168.1.5上操作

[root@lb01 ~]# ifconfig eth1

eth1 Link encap:Ethernet HWaddr 00:0C:29:7D:A8:DF

inet addr:192.168.1.5 Bcast:192.168.1.255 Mask:255.255.255.0

[root@lb01 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

0.0.0.0 192.168.1.51 0.0.0.0 UG 0 0 0 eth1

[root@lb01 ~]# route del default gw 192.168.1.51

[root@lb01 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

#进行ping测试

[root@lb01 ~]# ping 172.16.1.6

connect: Network is unreachable

#在192.168.1.5上操作

[root@lb01 ~]# ifconfig eth1

eth1 Link encap:Ethernet HWaddr 00:0C:29:7D:A8:DF

inet addr:192.168.1.5 Bcast:192.168.1.255 Mask:255.255.255.0

[root@lb01 ~]# route add -net 172.16.1.0/24 gw 192.168.1.51 #让去往172网段的走192.168.1.51出口

[root@lb01 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

172.16.1.0 192.168.1.51 255.255.255.0 UG 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

#在172.16.1.6上操作 添加回包的路由

[root@lb02 ~]# ifconfig eth1

eth1 Link encap:Ethernet HWaddr 00:0C:29:CF:56:A0

inet addr:172.16.1.6 Bcast:172.16.1.255 Mask:255.255.255.0

[root@lb02 ~]# ping 192.168.1.5

connect: Network is unreachable

[root@lb02 ~]# route add -net 192.168.1.0/24 gw 172.16.1.62

[root@lb02 ~]# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.1.0 172.16.1.62 255.255.255.0 UG 0 0 0 eth1

172.16.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1

169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

[root@lb02 ~]# ping 192.168.1.5

PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.

64 bytes from 192.168.1.5: icmp\_seq=1 ttl=62 time=0.748 ms

64 bytes from 192.168.1.5: icmp\_seq=2 ttl=62 time=0.577 ms

^C

--- 192.168.1.5 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1309ms

rtt min/avg/max/mdev = 0.577/0.662/0.748/0.089 ms

# openvpn通过服务器代理上网（翻墙）

更改配置文件（此功能是在阿里云服务器上实现）：

[root@beyond ~]# cat /etc/openvpn/server.conf

port 1194

proto tcp

dev tun

ca ca.crt

cert vpnserver.crt

key vpnserver.key # This file should be kept secret

dh dh2048.pem

server 10.8.0.0 255.255.255.0

push "route 172.17.57.0 255.255.255.0"

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

push "dhcp-option DNS 223.5.5.5"

push "dhcp-option DNS 8.8.8.8"

ifconfig-pool-persist ipp.txt

keepalive 10 120

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

;cipher AES-256-CBC

comp-lzo

persist-key

persist-tun

status openvpn-status.log

verb 3

client-to-client

log /var/log/openvpn.log

#添加防火墙转发规则

#添加NAT  10.8.0.0/24是OPENVPN的地址 10.162.xxx.xxx是阿里ECS的内网地址(ifconfig eth0)   
#iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source 10.162.xxx.xxx   
#保存iptables   
service iptables save

[root@beyond ~]# iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source 172.17.57.178

[root@beyond ~]# iptables -t nat -L -n

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

SNAT all -- 10.8.0.0/24 0.0.0.0/0 to:172.17.57.178

SNAT all -- 10.8.0.0/24 0.0.0.0/0 to:172.17.57.178

#重启服务

[root@beyond ~]# systemctl restart openvpn@server

# openvpn负载均衡高可用

## 一套客户端配置文件使用情况

需要在客户端配置文件添加如下内容

rmote 10.0.0.62 1194

rmote 10.0.0.201 1194

remote-random

resolv-retry 30