<http://www.centoscn.com/CentosServer/test/2014/1120/4153.html>

https://help.aliyun.com/knowledge\_detail/42521.html?spm=5176.11065259.1996646101.searchclickresult.5af47c2dMDNOd2

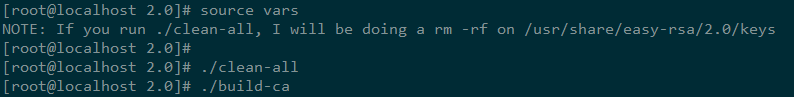
**1、安装前准备**

|  |
| --- |
| # 安装openssl和lzo，lzo用于压缩通讯数据加快传输速度  yum -y install openssl openssl-devel  yum -y install lzo |

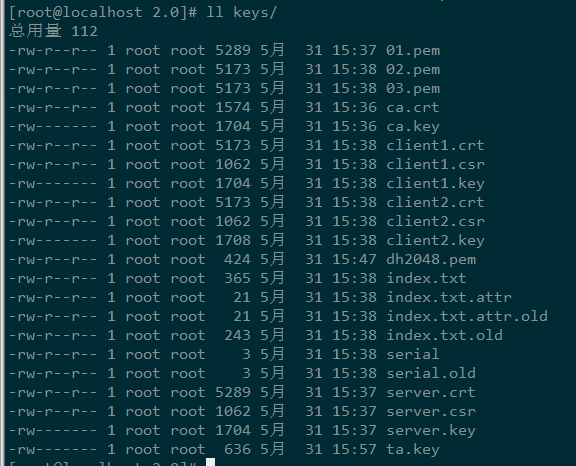
**2、安装及配置OpenVPN和easy-rsa**

|  |
| --- |
| # 安装openvpn和easy-rsa  yum -y install openvpn easy-rsa    # 修改vars文件  cd /usr/share/easy-rsa/2.0/  vim vars |
| # 修改注册信息，比如公司地址、公司名称、部门名称等。  export KEY\_COUNTRY="CN"  export KEY\_PROVINCE="Shandong"  export KEY\_CITY="Qingdao"  export KEY\_ORG="MyOrganization"  export KEY\_EMAIL="me@myhost.mydomain"  export KEY\_OU="MyOrganizationalUnit" |

|  |
| --- |
| # 初始化环境变量  source vars    # 清除keys目录下所有与证书相关的文件  # 下面步骤生成的证书和密钥都在/usr/share/easy-rsa/2.0/keys目录里  ./clean-all    # 生成根证书ca.crt和根密钥ca.key（一路按回车即可）  ./build-ca    # 为服务端生成证书和密钥（一路按回车，直到提示需要输入y/n时，输入y再按回车，一共两次）  ./build-key-server server    # 每一个登陆的VPN客户端需要有一个证书，每个证书在同一时刻只能供一个客户端连接  # 为客户端生成证书和密钥（一路按回车，直到提示需要输入y/n时，输入y再按回车，一共两次）  ./build-key zhangchen  # 创建迪菲·赫尔曼密钥，会生成dh2048.pem文件（生成过程比较慢，在此期间不要去中断它）  ./build-dh    # 生成ta.key文件（防DDos攻击、UDP淹没等恶意攻击）  openvpn --genkey --secret keys/ta.key |



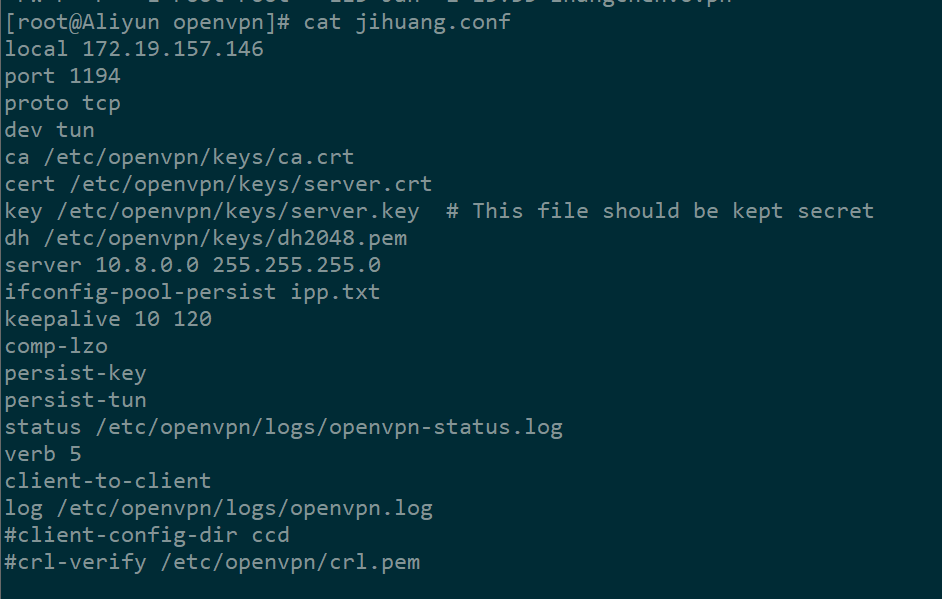
查看keys目录下生成的文件：



**3、创建服务器端配置文件**

|  |
| --- |
| # 在openvpn的配置目录下新建一个keys目录  mkdir /etc/openvpn/keys    # 将需要用到的openvpn证书和密钥复制一份到刚创建好的keys目录中  cp /usr/share/easy-rsa/2.0/keys/{ca.crt,server.{crt,key},dh2048.pem,ta.key} /etc/openvpn/keys/    # 复制一份服务器端配置文件模板server.conf到/etc/openvpn/  cp /usr/share/doc/openvpn-2.3.11/sample/sample-config-files/server.conf /etc/openvpn/  # 编辑server.conf  vim /etc/openvpn/server.conf |
| port 1194  # 改成tcp，默认使用udp，如果使用HTTP Proxy，必须使用tcp协议  proto tcp  dev tun  # 路径前面加keys，全路径为/etc/openvpn/keys/ca.crt  ca keys/ca.crt  cert keys/server.crt  key keys/server.key  # This file should be kept secret  dh keys/dh2048.pem  # 默认虚拟局域网网段，不要和实际的局域网冲突即可  server 10.8.0.0 255.255.255.0  ifconfig-pool-persist ipp.txt  # 10.0.0.0/8是我这台VPN服务器所在的内网的网段，读者应该根据自身实际情况进行修改  push "route 10.0.0.0 255.0.0.0"  # 可以让客户端之间相互访问直接通过openvpn程序转发，根据需要设置  client-to-client  # 如果客户端都使用相同的证书和密钥连接VPN，一定要打开这个选项，否则每个证书只允许一个人连接VPN  duplicate-cn  keepalive 10 120  tls-auth keys/ta.key 0 # This file is secret  comp-lzo  persist-key  persist-tun  # OpenVPN的状态日志，默认为/etc/openvpn/openvpn-status.log  status openvpn-status.log  # OpenVPN的运行日志，默认为/etc/openvpn/openvpn.log  log-append openvpn.log  # 改成verb 5可以多查看一些调试信息  verb 5  更改配置后的server.conf |

创建新的jihuang.conf ，内容如下：

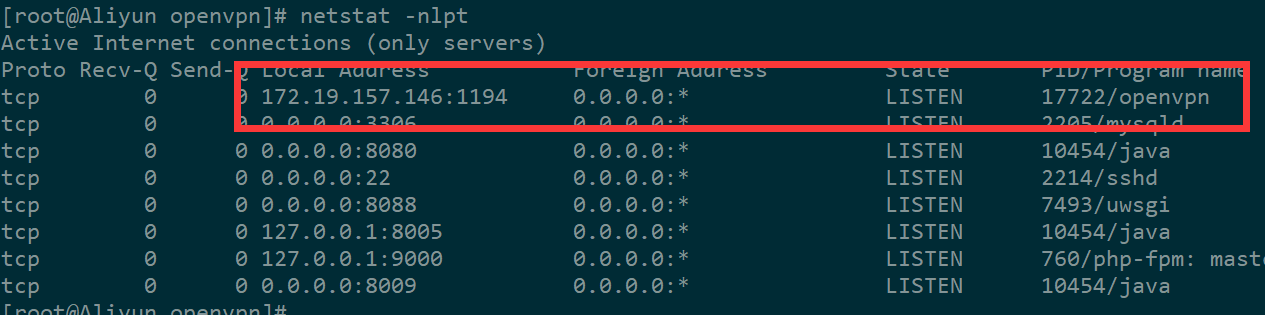


**4、配置内核和防火墙，启动服务**

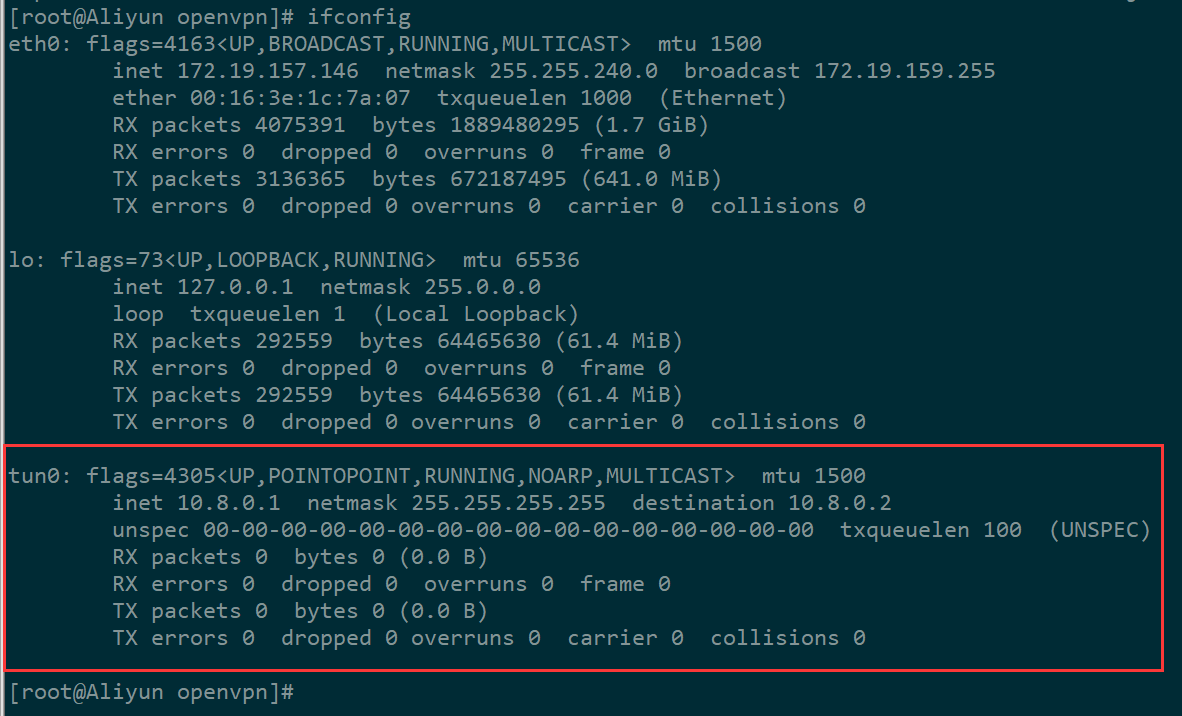
|  |
| --- |
| # 开启路由转发功能  将文件/etc/sysctl.conf里面的net.ipv4.ip\_forward=1的注释去除  让上述配置生效  sysctl -p    # 配置防火墙，别忘记保存  iptables -I INPUT -p tcp --dport 1194 -m comment --comment "openvpn" -j ACCEPT  iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j MASQUERADE  service iptables save    # 启动openvpn  /usr/sbin/openvpn --config /etc/openvpn/jihuang.conf |

**查看是否正常是否**

**看端口**



看ip



**5、创建客户端配置文件**

|  |
| --- |
| # 复制一份client.conf模板命名为zhangchen.ovpn  cp /usr/share/doc/openvpn-2.3.11/sample/sample-config-files/client.conf zhangchen.ovpn  # 编辑zhangchen.ovpn  vim zhangchen.ovpn |
| client  proto tcp  remote 106.14.135.171 1194  dev tun  comp-lzo  ca ca.crt  cert zhangchen.crt  key zhangchen.key  verb 3 |

**二、Windows客户端安装及配置**

    客户端系统：Windows7 64位

    内网IP：172.16.4.4

    OpenVPN版本：OpenVPN 2.3.3 Windows 64位

**1、下载安装OpenVPN**

    OpenVPN 2.3.3 Windows 32位 安装文件：

    http://swupdate.openvpn.org/community/releases/openvpn-install-2.3.3-I002-i686.exe

    OpenVPN 2.3.3 Windows 64位 安装文件：

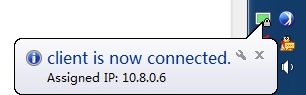
    http://swupdate.openvpn.org/community/releases/openvpn-install-2.3.3-I002-x86\_64.exe

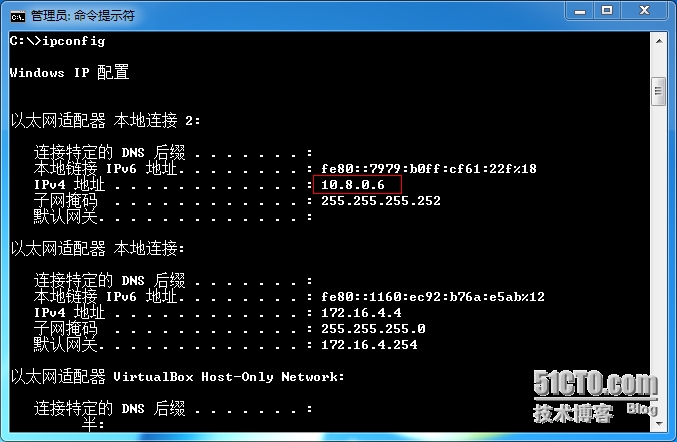
**2、配置client**

    将OpenVPN服务器上的zhangchen.ovpn、ca.crt、zhangchen.crt、zhangchen.key、ta.key上传到Windows客户端安装目录下的config文件夹（C:\Program Files\OpenVPN\config）

**3、启动OpenVPN GUI**

    在电脑右下角的openvpn图标上右击，选择“Connect”。正常情况下应该能够连接成功，分配正常的IP。



****

**4、测试**



    ping通服务器的内网IP，说明已经接入到服务器的内部网络。

    到OpenVPN服务器上查看客户端的连接情况，查看状态文件/etc/openvpn/openvpn-status.log：

# 新增用户

安装好openvpn后，生成了client1.crt  client1.key,client1.ovpn(ovpn文件可以自己创建)等相关文件，在一个时间段内只能一个人使用，别人要是使用会连接不上，如果想让更多人使用，可以创建更多的客户端配置文件，比如client2、client3。

下面介绍方法：

1，进入/etc/openvpn/easy-rsa/2.0目录 （cd /etc/openvpn/easy-rsa/2.0）

2，source vars 或者 . vars (注意. vars 中间有空格)

ps：如果不执行这步，执行第三步./build-key client2会导致如下问题：

Please edit the vars script to reflect your configuration,  
  then source it with "source ./vars".  
  Next, to start with a fresh PKI configuration and to delete any  
  previous certificates and keys, run "./clean-all".  
  Finally, you can run this tool (pkitool) to build certificates/keys.

3,./build-key client2

安装提示输入相关信息即可，有的不输入也没问题。

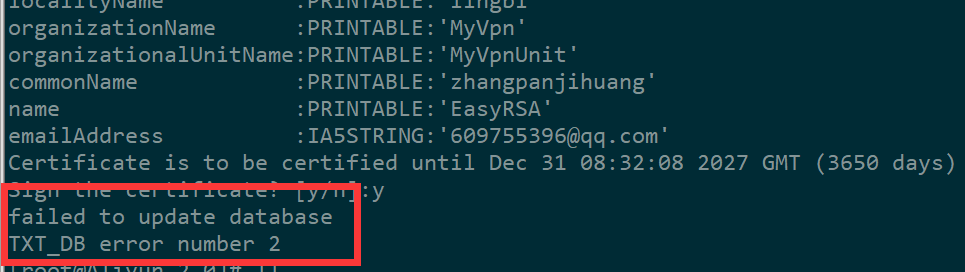
执行完这步后，会在keys目录下生成client2.crt client2.csr client2.key三个文件。

4，手动创建zhangpan.ovpn文件，按照zhangchen.ovpn的改写cert key内容就成。

比如可以是这样：



1. 把keys中的ca.crt ca.key复制，并把client2.ovpn client2.crt client2.csr client2.key文件 一同放在一个新的文件夹中，下载下来就可以使用了。

新建账号 提示

原因是账号之前已经创建一次了，，数据库里已经有记录了，解决办法是先备份echo >keys/index.txt文件，再把keys/index.txt文件里刚才创建失败的账号记录删掉，重新创建就可以了。

