openvp搭建

# 基础环境准备

## 软件环境

操作系统：CentOS Linux release 7.7.1908 (Core)

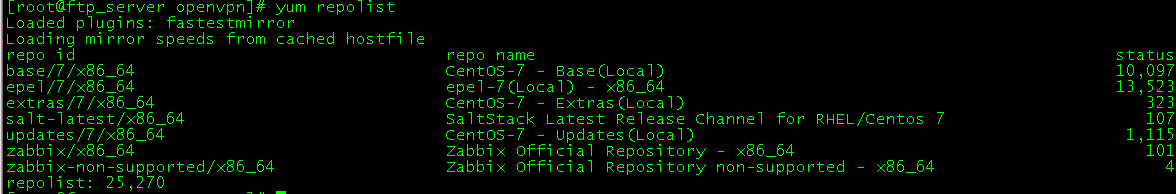
openvpn：2.4.8

easy-rsa：3.0.6

## 配置yum源

配置好base源和epel源。配置方法本文不再叙述。

#yum repolist

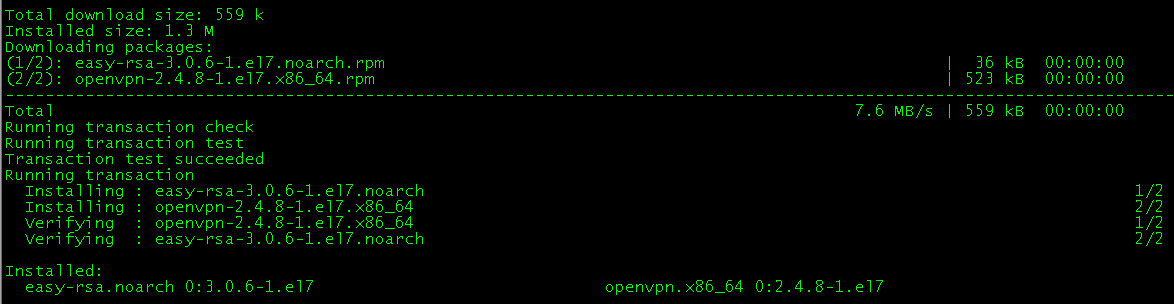


# 服务端安装配置

## 软件安装

配置好epel源后，直接yum安装即可

#yum install openvpn easy-rsa lrzsz -y



## easy-rsa配置

# mkdir /etc/openvpn/server/easy-rsa

# mkdir /etc/openvpn/client/easy-rsa

#cp -r /usr/share/easy-rsa/3/\* /etc/openvpn/server/easy-rsa/

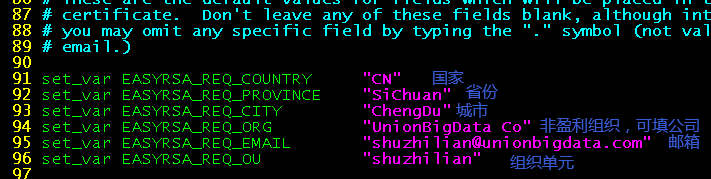
#cp /usr/share/doc/easy-rsa-3.0.6/vars.example /etc/openvpn/server/easy-rsa/vars

#cp -r /usr/share/easy-rsa/3/\* /etc/openvpn/client/easy-rsa/

## 配置vars

#cd /etc/openvpn/server/easy-rsa/

#vim vars

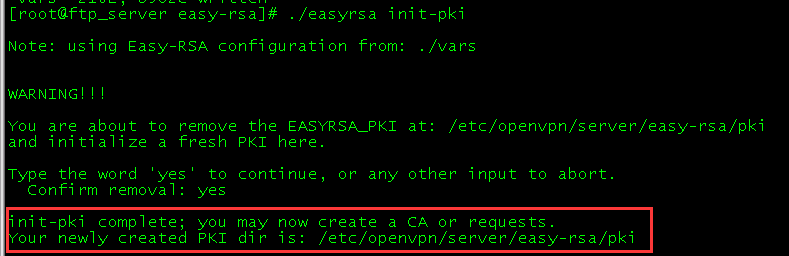


## 创建服务端证书和key

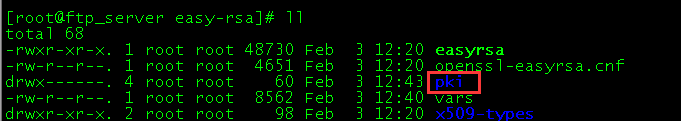
#cd /etc/openvpn/server/easy-rsa/

### 目录初始化

#./easyrsa init-pki

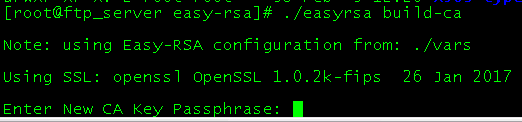


出现pki目录即为初始化成功。

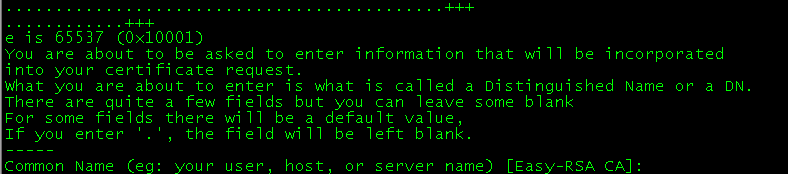


### 创建根证书

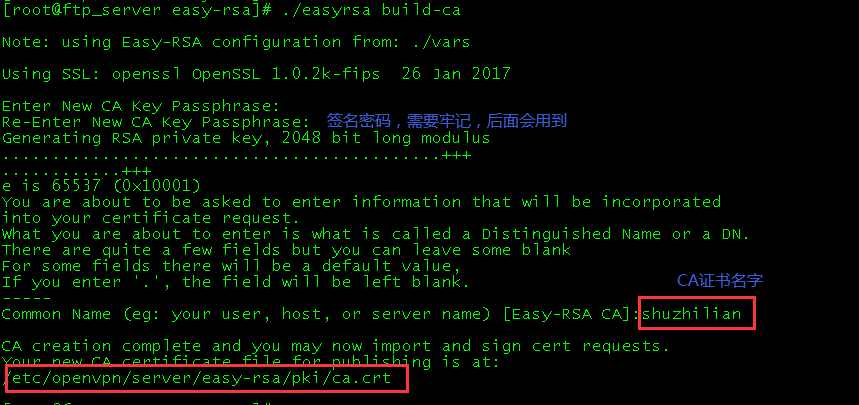
#./easyrsa build-ca



重复输入两次密码，这个密码要牢记，以后将用于证书签名。文档以：UnionBig@12#为例

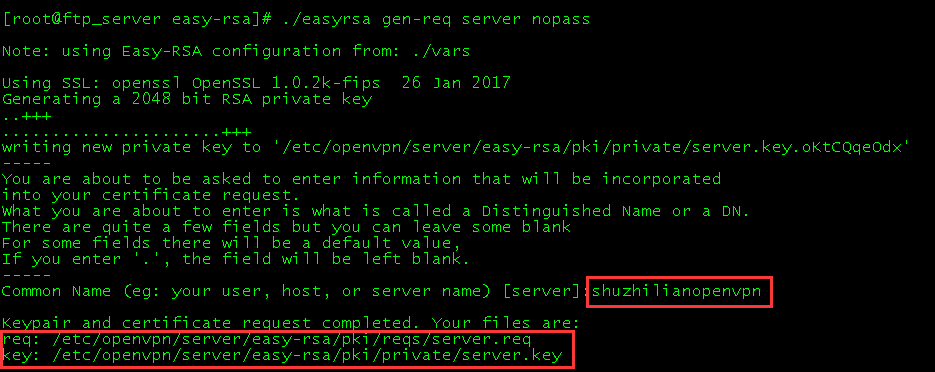


这里为CA证书起个通用的名字。文档以：shuzhilian为例



### 创建服务端证书

# ./easyrsa gen-req server nopass



同样起个好记的通用名字，不过就不能和前面根证书的一样，本文以：shuzhilianopenvpn为例

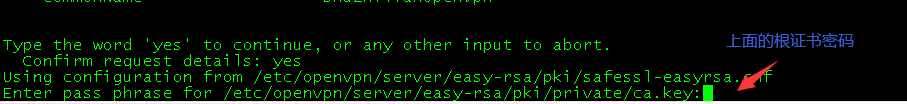
### 签约服务端证书

#./easyrsa sign server server

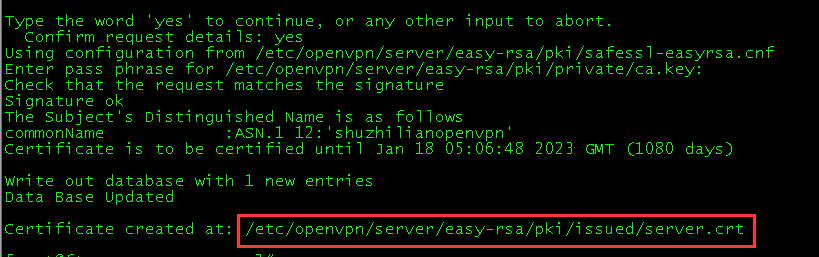
注：这里前一个server是命令表示注册的是server端，后一个server是可以自行定义的名字。



输入：yes



输入之前创建根证书时配置的密码，如果忘记了就得从创建根证书重新做起了。刚刚我们配置的为：UnionBig@12#

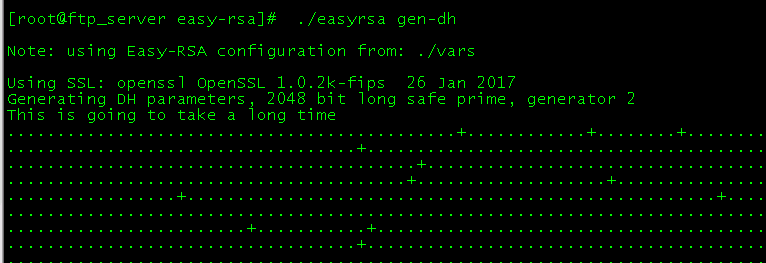


最终生成的文件为：/etc/openvpn/server/easy-rsa/pki/issued/server.crt

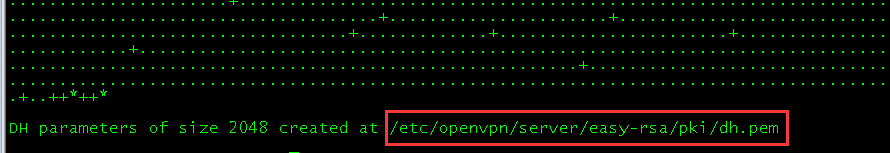
### 创建Diffie-Hellman

创建Diffie-Hellman，确保key穿越不安全网络

# ./easyrsa gen-dh



这里要多等一下。视机器配置情况，一般1-2分钟



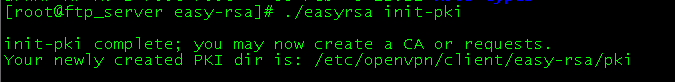
最终生成的文件为：/etc/openvpn/server/easy-rsa/pki/dh.pem

## 创建客户端证书和key

#cd /etc/openvpn/client/easy-rsa/

### 目录初始化

#./easyrsa init-pki



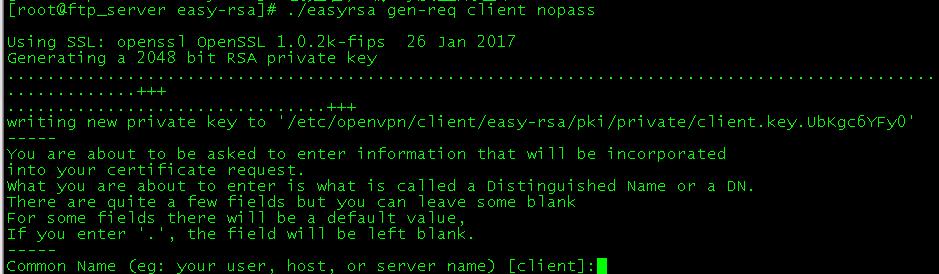
### 创建客户端key及生成证书

#./easyrsa gen-req client nopass

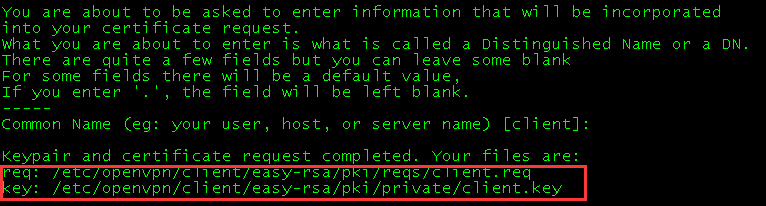
这里特别说明下：

client是客户端的名称，可以自定义的

nopass 可去掉，加上它是不用密码的意思。本文的连接方式是所有的客户端用同一个证书，通过脚本来调用用户名和密码进行二次认证。如果需要每个客户端单独证书的话，这里的nopass需要去掉，并在创建过程中输入密码。该密码用于单独证书的客户端的连接时使用。



默认，直接回车

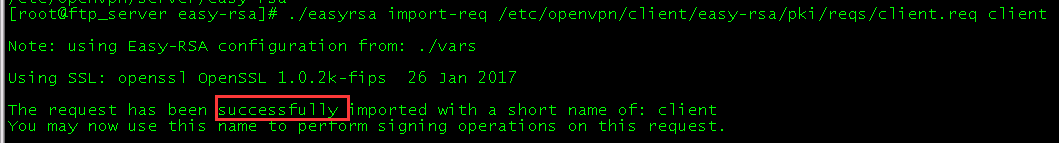


### 导入client.req

进入服务端的easy-rsa目录

#cd /etc/openvpn/server/easy-rsa/

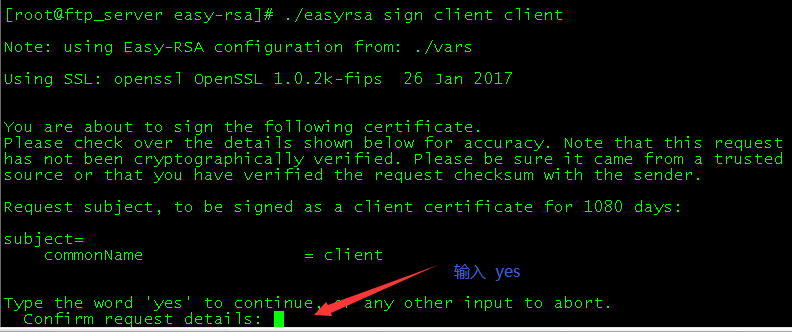
#./easyrsa import-req /etc/openvpn/client/easy-rsa/pki/reqs/client.req client



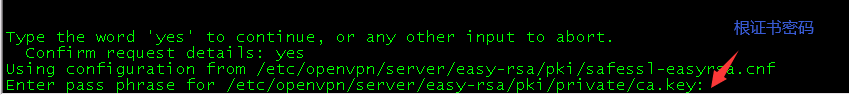
### 签约客户端证书

#./easyrsa sign client client

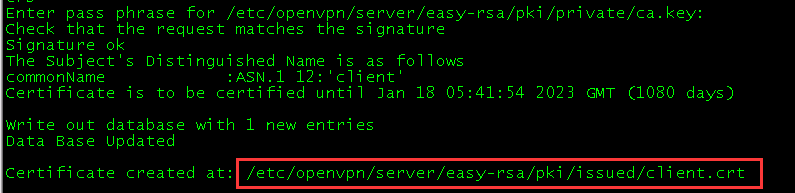
这里生成client所以第一个client位置必须为client，第二个参数client要与之前导入名字一致，导入的时候会要求输入密码，这个密码是第一次设置的根证书的密码，不要输错；因为openvpn是一个客户端对应一组证书密钥文件的。



输入 yes



输入之前创建根证书时配置的密码，如果忘记了就得从创建根证书重新做起了。刚刚我们配置的为：UnionBig@12#



生成的客户端证书：/etc/openvpn/server/easy-rsa/pki/issued/client.crt

## 整理证书和key

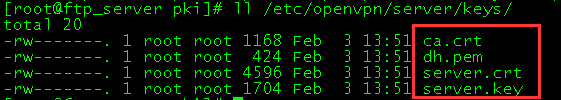
### 服务端

#mkdir /etc/openvpn/server/keys

#cd /etc/openvpn/server/easy-rsa/pki/

#cp ca.crt private/server.key issued/server.crt dh.pem /etc/openvpn/server/keys/

# ll /etc/openvpn/server/keys/



### 客户端

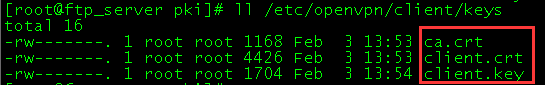
#mkdir /etc/openvpn/client/keys

#cd /etc/openvpn/server/easy-rsa/pki/

# cp ca.crt issued/client.crt /etc/openvpn/client/keys/

#cp /etc/openvpn/client/easy-rsa/pki/private/client.key /etc/openvpn/client/keys/

#ll /etc/openvpn/client/keys



### 文件用途



## 配置服务端

#cd /etc/openvpn/server/

#cp /usr/share/doc/openvpn-2.4.8/sample/sample-config-files/client.conf .

#cp client.conf client.conf.bak

#mkdir log

### 配置server.conf

#cat >/etc/openvpn/server/server.conf<<EOF

port 51148

proto tcp

dev tun

#证书绝对路径

ca /etc/openvpn/server/keys/ca.crt

cert /etc/openvpn/server/keys/server.crt

key /etc/openvpn/server/keys/server.key

dh /etc/openvpn/server/keys/dh.pem

#虚拟网络配置

server 10.100.118.0 255.255.255.0

ifconfig-pool-persist /etc/openvpn/server/ipp.txt

#指定需要访问的内网

push "route 172.27.15.0 255.255.255.0"

push "route 172.27.8.0 255.255.252.0"

# 启用该指令，所有客户端的默认网关都将重定向到VPN，这将导致诸如web浏览器、DNS查询等所有客户端流量都经过VPN。

#push "redirect-gateway def1 bypass-dhcp"

#push "dhcp-option DNS 223.5.5.5"

#开启client间互访

#client-to-client

keepalive 10 240

comp-lzo

persist-key

persist-tun

#允许一个用户登录多次,默认为禁止

#duplicate-cn

#客户端一直在线，默认一小时自动断开

reneg-sec 0

status /etc/openvpn/server/log/status.log

log /etc/openvpn/server/log/openvpn.log

log-append /etc/openvpn/server/log/openvpn.log

verb 3

script-security 3

#tls-auth ta.key 0

#调用脚本进行认证

auth-user-pass-verify /etc/openvpn/server/checkpsw.sh via-env

#仅用用户名/密码认证

#client-cert-not-required

username-as-common-name

EOF

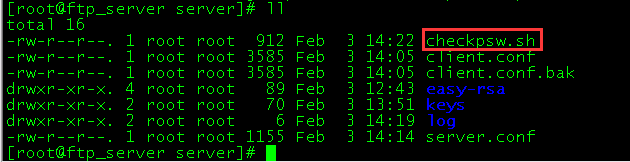
注意：文件路径需要是实际一致。

### 导入用户密码验证脚本

#cd /etc/openvpn/server/



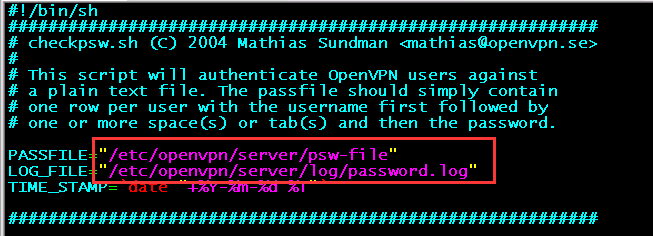
#rz –bye



注意文件中的日志文件路径需要和实际一致。

### 配置脚本

#vim checkpsw.sh



# chmod a+x checkpsw.sh

创建用户名密码文件

#vim /etc/openvpn/server/psw-file

该文件格式为：用户名+空格+密码 。每行为一个用户。暂停账号添加#，删除账号直接删除那行即可。



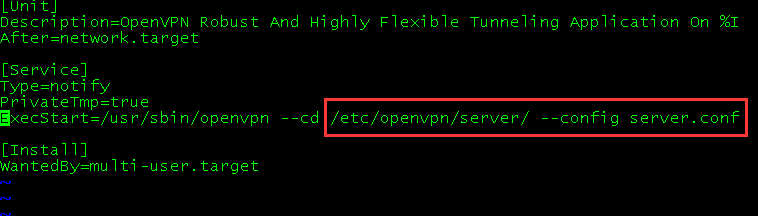
### 启动服务

#/usr/sbin/openvpn /etc/openvpn/server/server.conf &

### 配置systemctl

#systemctl -f enable openvpn@server.service

# vim /usr/lib/systemd/system/openvpn@.service

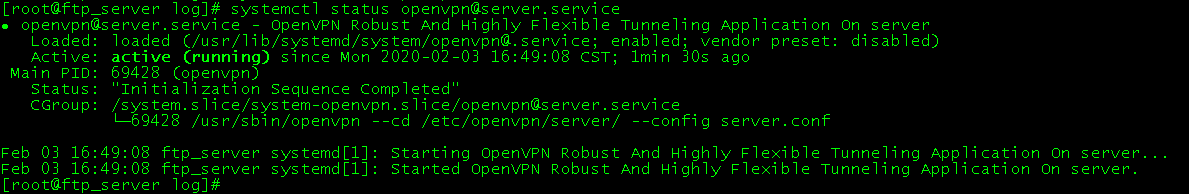


# systemctl daemon-reload

#pkill openvpn

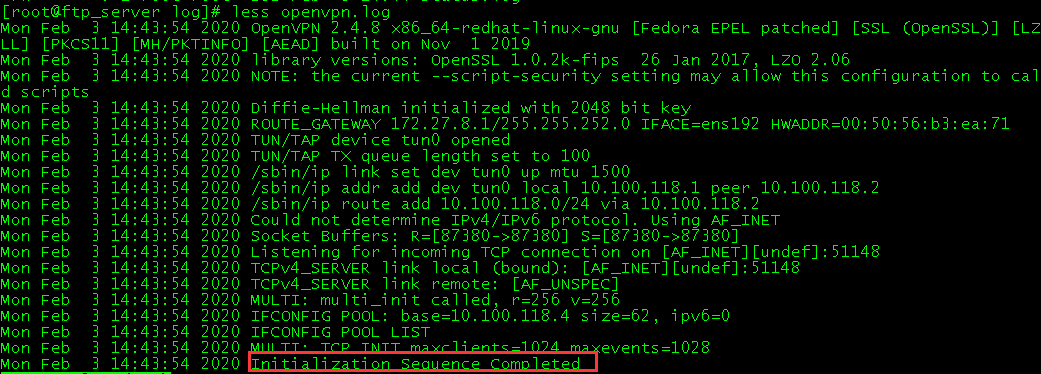
# systemctl start openvpn@server.service

# systemctl status openvpn@server.service



### 检查服务

#less /etc/openvpn/server/log/openvpn.log



显示Initialization Sequence Completed 即可服务启动成功。

#lsof –i:51148



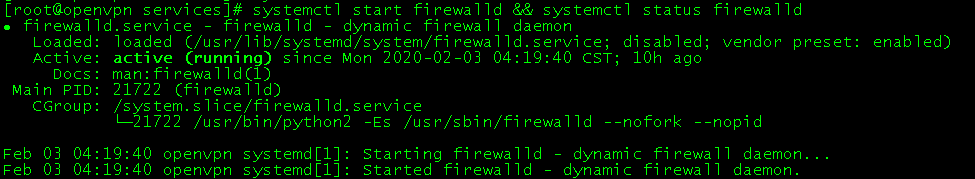
检测端口是否启动。有即为成功。

至此，openvpn服务端安装配置成功。**实际环境中需要将server的vpn端口（本文为：51148）映射至外网。**

# firewalld转发配置

## 开启firewalld

# systemctl start firewalld && systemctl status firewalld



# firewall-cmd --add-port=51148/tcp --permanent --zone=public

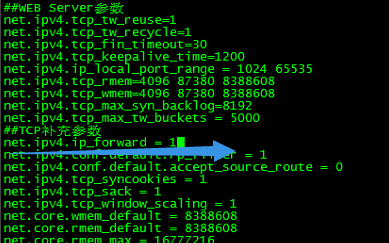
#firewall-cmd –reload

## 开启转发

#vim /etc/sysctl.conf

添加：net.ipv4.ip\_forward = 1

#sysctl –p



## 开启防火墙伪装

# firewall-cmd --add-masquerade –permanent

#firewall-cmd –reload

## 配置SNAT

#firewall-cmd --zone=public --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -d 172.27.15.0/24 -j SNAT --to-source 172.27.11.60

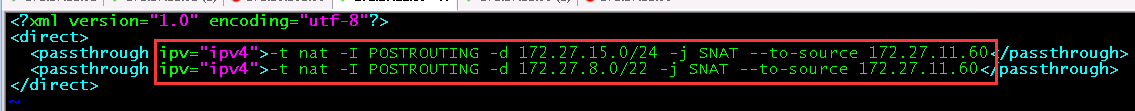
#firewall-cmd –reload

172.27.15.0/24是目标网段

172.27.11.60 为vpn服务器的内网IP

如果有多个网段需要访问，多条执行即可。

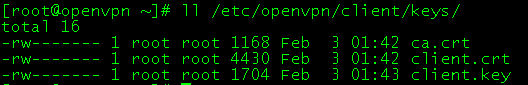
另：这里如果配置错误。可以通过：vim /etc/firewalld/direct.xml 进行手动调整。



# 客户端配置

## 证书文件

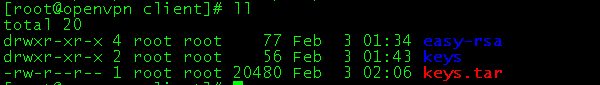
#ll /etc/openvpn/client/keys/



将这三个文件打包后下载至客户端

#cd /etc/openvpn/client/

#tar –cvf keys.tar keys



## 客户端配置文件

client

dev tun

proto tcp

remote 182.150.44.163 51148

resolv-retry infinite

nobind

persist-key

persist-tun

auth-user-pass

remote-cert-tls server

comp-lzo

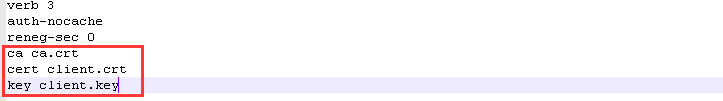
verb 3

auth-nocache

reneg-sec 0

其中remote 后面为服务器映射后的外网IP+端口

这里可以把ca、cert、key在配置文件中配置路径，如图：



也可以将三个的文件的密文复制在配置文件中。本文推荐第二种方式，这样方便配置文件传递。





## 客户端连接

客户端连接请参考客户端连接文档

# 日常维护

## 账号管理

# vim /etc/openvpn/server/psw-file



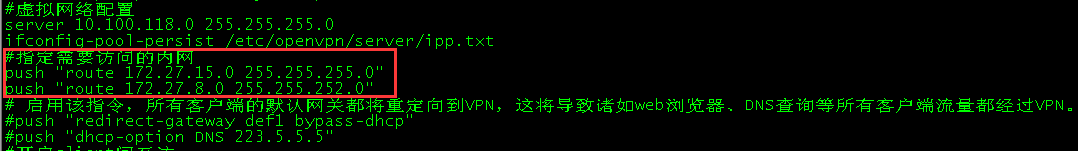
该文件格式为：用户名+空格+密码 。每行为一个用户。暂停账号添加#，删除账号直接删除那行即可。

需要批量导入，只需批量编辑导入该文件即可。

变更用户后，系统自动加载。无需重启openvpn服务。

## vpn网络配置

#vim /etc/openvpn/server/server.conf



push "route 172.27.15.0 255.255.255.0"

其中172.27.15.0 255.255.255.0 为客户机可以访问业务网络地址，可以是网段，也可以是单个ip。

另：这里添加后可能会调整firewalld的SNAT配置，调整方法请见本文档“三、4”

调整配置文件后，需重启openvpn服务，方可生效。

## 服务管理

开启：systemctl start openvpn@server.service

关闭：systemctl stop openvpn@server.service

重启：systemctl restart openvpn@server.service