## [centos7 搭建openvpn服务器](https://www.cnblogs.com/fuyanwen/p/8195956.html)

1. 客户端连接openvpn；前提由于centos软件库默认不可用需安装EPEL

#Yum installepel-release



1. 安装插件

#yum install -y openssl openssl-devel lzo lzo-devel pam pam-devel automake pkgconfig makecache



1. 安装openvpn以及ca证书easy-rsa包

#yum install -y openvpn

#yum install -y easy-rsa





1. 配置openvpn

#cp -R /usr/share/easy-rsa /etc/openvpn/ \*拷贝rasy-rsa脚本文件

#cp /usr/share/doc/openvpn-2.4.7/sample/sample-config-files/server.conf /etc/openvpn \*拷贝server.conf

#cp -r /usr/share/doc/easy-rsa-3.0.3/vars/exmaple /etc/openvpn/easy-rsa/3.0/vars



#vi /etc/openvpn/server.conf(部分配置如下：)

port 1194

proto udp

dev tun

ca /etc/openvpn/easy-rsa/3.0.3/pki/ca.crt

cert /etc/openvpn/easy-rsa/3.0.3/pki/issued/wwwserver.crt

key /etc/openvpn/easy-rsa/3.0.3/pki/private/wwwserver.key

dh /etc/openvpn/easy-rsa/3.0.3/pki/dh.pem

tls-auth /etc/openvpn/ta.key

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

push "route 192.168.1.0 255.255.255.0"

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 223.5.5.5"

push "dhcp-option DNS 114.114.114.114"

keepalive 10 120

cipher AES-256-CBC

comp-lzo

max-clients 50

persist-key

persist-tun

status openvpn-status.log

log-append openvpn.log

verb 3

mute 20



1. CA证书制作

#vim /etc/openvpn/easy-rsa/3.0.3/vars(配置如下)

set\_var EASYRSA\_REQ\_COUNTRY "US" #国家

set\_var EASYRSA\_REQ\_PROVINCE "California" #省

set\_var EASYRSA\_REQ\_CITY "Shanghai" #城市

set\_var EASYRSA\_REQ\_ORG "Copyleft Certificate Co" #组织

set\_var EASYRSA\_REQ\_EMAIL "test@example.net" #邮箱

set\_var EASYRSA\_REQ\_OU "My Organizational Unit" #公司、组织

set\_var KEY\_CN=192.168.160.12 #本机ip


　　 #cd /etc/openvpn/easy-rsa/3.0.3

#./easyrsa init-pki

失败run init-pki first

#./easyrsa build-ca 设置密码：123456（自己定义）

#openvpn --genkey --secret ta.key

#cp ta.key /etc/openvpn/ 拷贝文件

1. DH证书制作

# ./easyrsa gen-dh /etc/openvpn/easy-rsa/3.0.3/pki/dh.pem

# ./easyrsa gen-dh

1. 服务端证书制作

#./easyrsa gen-req server 设置密码：123456(自己定义)

签发证书，签约服务端证书

#./easyrsa sign-req server server 输入”yes” 密码(ca):123456

注意：客户端证书

签发证书，签约客户端 (客户端需要的证书：client.crt、client.key、ca.crt、ta.key)

#./easyrsa build-client-full client 输入”yes” 密码(ca):123456

查看证书

#ls -l /etc/openvpn/easy-rsa/3.0.3/pki/issued/client.crt

#ls -l /etc/openvpn/easy-rsa/3.0.3/pki/issued/client.key

#vim /etc/sysctl.conf

net.ipv4\_forward =1

#sysctl -p

1. 启动openvpn
 systemctl -f enable openvpn@server.service #设置启动文件

systemctl start openvpn@server.service #启动openvpn的命令

1. 客户端证书

# mkdir -p /etc/openvpn/client

# cd /etc/openvpn/client

# cp -r /usr/share/easy-rsa/3.0.3/\* /etc/openvpn/client

# cp /usr/share/doc/easy-rsa-3.0.3/vars.example ./vars

# ./easyrsa init-pki

# ./easyrsa gen-req client nopass #client为证书名可自定义，nopass同样设置免密

# key: /etc/openvpn/client/pki/private/client.key #key路径

1. 对客户端证书签名

#切换到服务端easy-rsa目录下：

#cd /etc/openvpn/easy-rsa

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

#./easyrsa sign client client #签名,第一个client是固定的参数表示客户端，第二个client指上面导入的客户端证书名

#./easyrsa sign client client

1. 修改配置文件服务器端证书和密钥统一放到和server.conf一个目录下，便于配置

cp /etc/openvpn/easy-rsa/pki/ca.crt /etc/openvpn/

cp /etc/openvpn/easy-rsa/pki/private/server.key /etc/openvpn/

cp /etc/openvpn/easy-rsa/pki/issued/server.crt /etc/openvpn/

cp /etc/openvpn/easy-rsa/pki/dh.pem /etc/openvpn

cat /etc/openvpn/server.conf

1. 客户端需要的证书

/etc/openvpn/easy-rsa/pki/issued/client.crt #在服务端证书生成目录下

/etc/openvpn/client/pki/private/client.key #上面的客户端生成目录下

/etc/openvpn/easy-rsa/pki/ca.crt #ca证书

/etc/openvpn/ta.key