

最近准备上一套新项目，云服务器也重新买了一套，还是老样子，后端节点和数据库木有公网 IP，叫我明天一天搞完，今天晚上买的服务器，我擦咧，这下有事情做了，总比闲着强吧，然后今天就是把 vpn，和 SNAT 做了，因为只有一个公网 IP。由于这种 vpn 是第一次搞，记录一下，下面使用的是 Debian7.0 操作系统，开撸开撸。

## 安装 openvpn 要求

openvpn 需要 tun 和 iptables\_nat 模块支持，检查一下

```
root@10-9-128-245:~# cat /dev/net/tun
cat: /dev/net/tun: File descriptor in bad state
```

返回信息是 cat: /dev/net/tun: File descriptor in bad state 说明可以使用

## 安装 openvpn

OpenVPN 需要 lzo 支持，可以 OpenVPN 与 lzo 一起安装

```
root@10-9-128-245:~# apt-get update
root@10-9-128-245:~# apt-get install openvpn lzo
```

## openvpn 配置

### 1. 生成证书

```
root@10-9-128-245:~# cp -r /usr/share/doc/openvpn/examples/easy-rsa/ /etc/openvpn/
root@10-9-128-245:~# cd /etc/openvpn/easy-rsa/2.0
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# source vars
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./clean-all
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./build-ca
```

一路 y 回车

### 2. 生成服务器端证书和秘钥

```
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./build-key-server server
```

一路 y 回车

我还是先回家吧，明天继续

2016 年 12 月 15 日 21:50:28

### 3. 生成客户端证书和密钥

```
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./build-key client
```

一路 y 回车

### 4. 生成 Diffie Hellman 参数:

```
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./build-dh
```

### 5. 配置 OpenVPN 服务器端文件

编辑 /etc/openvpn/server.conf 文件，没有就手动创建，我的配置文件如下。尽量不要使用 upd 协议和 1194 端口，因为在国内很多接入商都不允许，导致 1194 端被封不能用。当然你也可以试一下，如果被封了就换一下。

```
local 11.1.1.1      ##服务器IP
port 12306         #占用端口，保证和其他没冲突，
proto tcp          #使用TCP协议
dev tun            #使用tun模式，也可以使用tap

ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key
dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem #指定证书路径

ifconfig-pool-persist /etc/openvpn/ipp.txt      #存放每个人所使用的IP

server 12.166.221.0 255.255.255.0      #客户端dhcp，不要和客户端冲突
push "route 10.9.0.0 255.255.0.0"      #vpn访问网段，就是服务器地址段，我的是1
0.9网段的
client-to-client                        #允许客户端之间互相访问

keepalive 20 120 #保持连接时间
comp-lzo        #开启vpn压缩
#duplicate-cn   #如果不止一个人使用该证书，去掉注释

user openvpn    #运行属主
group openvpn   #运行属组

persist-key
persist-tun    ##持久化选项可以尽量避免访问在重启时由于用户权限降低而无法访问
的某些资源。
status openvpn-status1.log
log-append openvpn1.log
verb 1        #日志级别 0-9 等级越高，记录的越多
mute 20
```

## 配置 iptables 及转发

```
root@10-9-128-245:~# iptables -t nat -A POSTROUTING -s 12.166.221.0/24 -o eth0 -j MASQUERADE
```

注意，12.166 的那个换成自己的客户端地址 我的 eth0 是内网网卡，eth1 是外网网卡。这条策略是将所有的 12.166.221.0 网段的包转发给 eth0

iptables 保存配置文件

```
root@10-9-128-245:~# iptables-save > /etc/iptables-rules #保存配置
root@10-9-128-245:~# vim /etc/iptables-rules #编辑保存的配置文件，不要的删掉
root@10-9-128-245:~# iptables-restore < /etc/iptables-rules #恢复配置文件
```

修改 /sysctl.conf

```
root@10-9-128-245:~# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
root@10-9-128-245:~# sysctl -p #重新载入，立即生效
```

重启 openvpn，然后 ifconfig 看一下，会多一个 tun0 虚拟网卡

```
root@10-9-128-245:~# /etc/init.d/openvpn restart
[ ok ] Stopping virtual private network daemon: server.
[ ok ] Starting virtual private network daemon: server.
root@10-9-128-245:~# ifconfig
```

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:12.166.221.1  P-t-P:12.166.221.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

## 客户端配置

### 1. 添加 openvpn 用户

```
root@10-9-128-245:~# cd /etc/openvpn/easy-rsa/2.0/
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# source vars ###必需步骤
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./build-key dalin #用户名，一路回车y
```

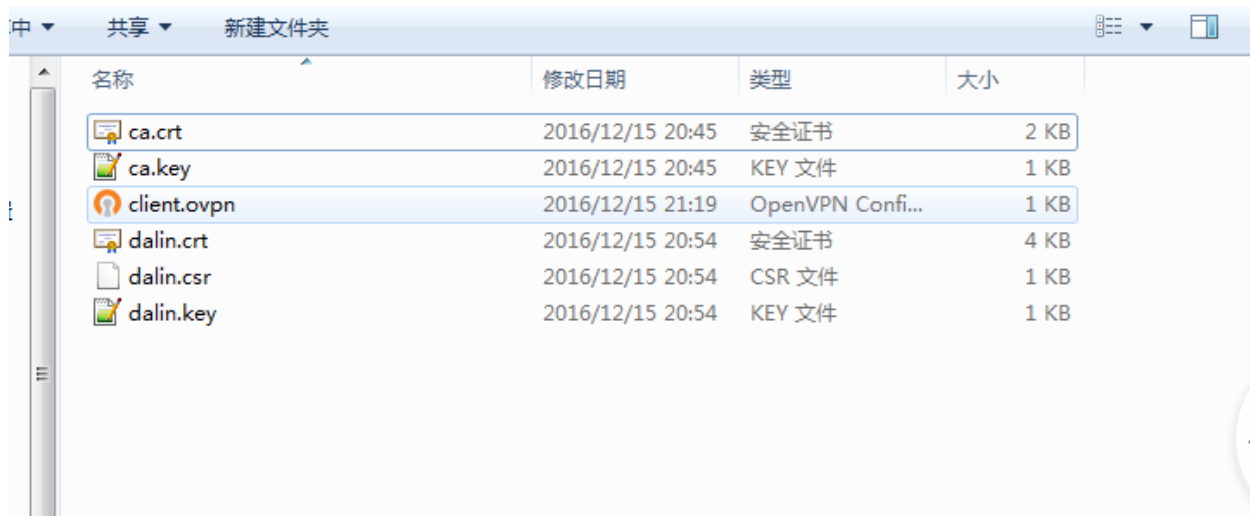
## 2. 删除 openvpn 用户

```
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# source vars
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0# ./revoke-full username
```

## 3. 添加完成之后进到 keys 里面下载对应的一切

```
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0/keys# sz dalin.*
root@10-9-128-245:/etc/openvpn/easy-rsa/2.0/keys# sz ca.*
```

全部下载下来，一共是 5 个，如果所示，除了 client.ovpn 文件，需要手动创建



名称	修改日期	类型	大小
ca.crt	2016/12/15 20:45	安全证书	2 KB
ca.key	2016/12/15 20:45	KEY 文件	1 KB
client.ovpn	2016/12/15 21:19	OpenVPN Confi...	1 KB
dalin.crt	2016/12/15 20:54	安全证书	4 KB
dalin.csr	2016/12/15 20:54	CSR 文件	1 KB
dalin.key	2016/12/15 20:54	KEY 文件	1 KB

## 编辑 client.ovpn 文件

```
client    #这个不能改
proto tcp  #要与server.conf一致
dev tun    #要与server.conf一致
remote 主机外网IP 12306

ca ca.crt
cert dalin.crt
key dalin.key      #对应所下载的证书

resolv-retry infinite
nobind
mute-replay-warnings

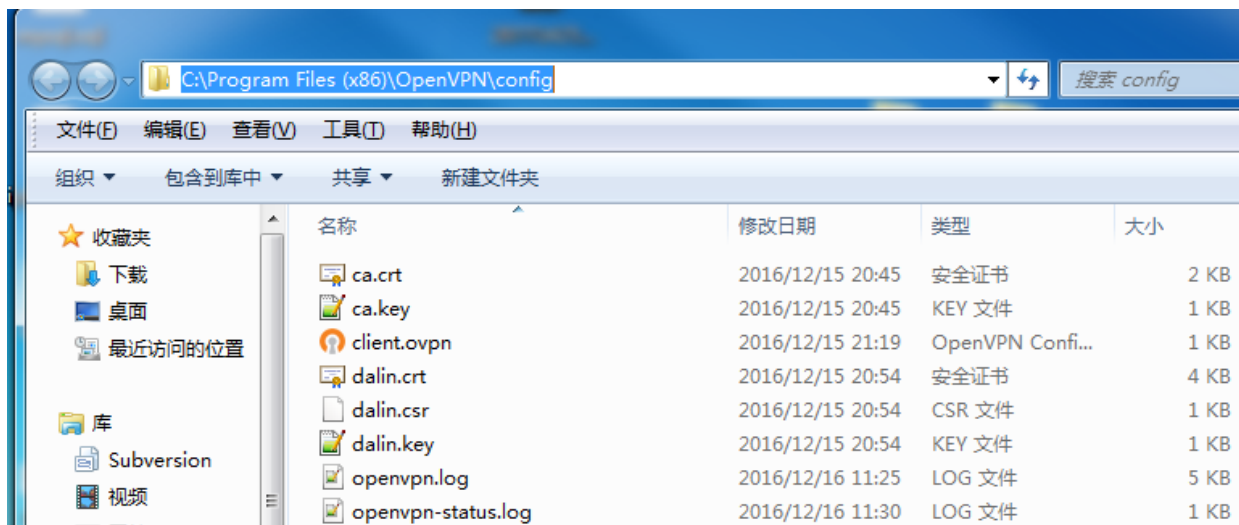
keepalive 20 120
comp-lzo
#user openvpn
#group openvpn

persist-key
persist-tun
```

```
status openvpn-status.log
log-append openvpn.log
verb 3
mute 20
```

## 安装 vpn 客户端

把以上文件全部放到 \$OPENVPN\_HOME\_CONFIG 里面，设置好一起开始连接



## linux 连接 vpn

### 1. 安装 vpn

```
root@localhost:~# apt-get install openvpn #debian/ubuntu
root@localhost:~# yum -y install openvpn #redhat/centos
root@localhost:~/config# openvpn --config client.ovpn &
root@localhost:~# ifconfig
```

```
root@localhost:~/config# openvpn --config client.ovpn &
[1] 25529
root@localhost:~/config# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:96:2c:84
          inet addr:192.168.1.96  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe96:2c84/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19479349 errors:0 dropped:859 overruns:0 frame:0
          TX packets:3156724 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3574951783 (3.3 GiB)  TX bytes:402174430 (383.5 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:79396 errors:0 dropped:0 overruns:0 frame:0
          TX packets:79396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9109509 (8.6 MiB)  TX bytes:9109509 (8.6 MiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.166.222.54  P-t-P:10.166.222.53  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@localhost:~/config#
```

注意一下，如果在 client.ovpn 配置了运行属主属组，服务器需要有相对应的用户，linux&Mac 都要这样，windows 就无所谓了。

[debian](#)[vpn](#)

最后编辑于: 2018 年 12 月 12 日

[返回文章列表](#)[文章二维码](#)[打赏](#)