# Cenos7 下搭建 OpenVPN 过程记录

2019-06-16

| 分类于 OpenVPN | 浏览 3780次


## OpenVPN 服务端安装配置

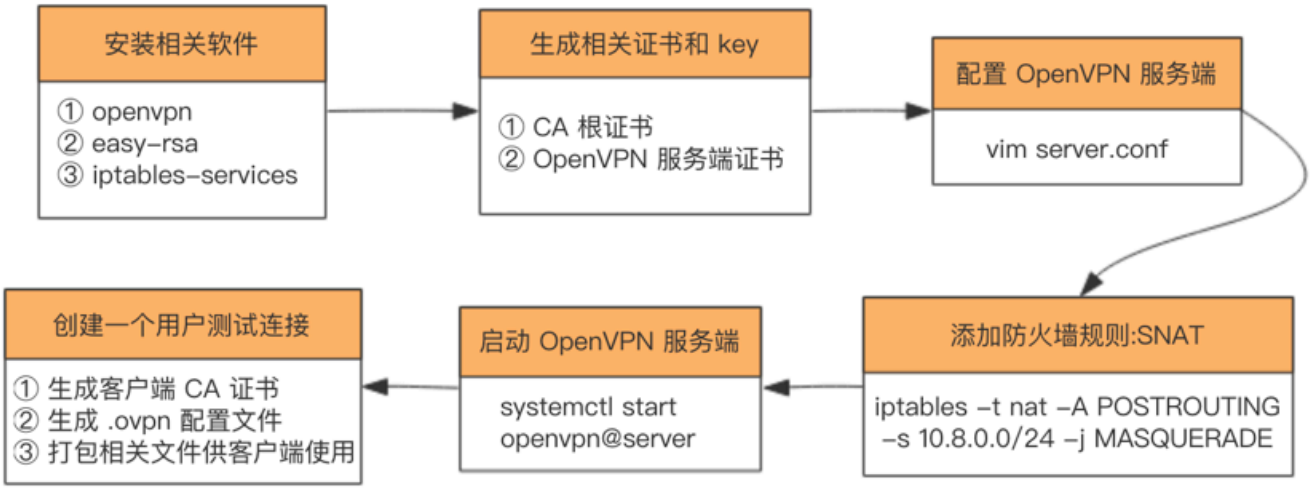
由于不同环境及软件版本命令使用略有差异，特别是 easy-rsa 的使用在 2.0 和 3.0 的差别有点大，所以在此先说明下安装环境及相关软件版本：

- **系统平台：** Centos7
- **OpenVPN 版本：** 2.4.7
- **easy-rsa 版本：** 3.0.3

**尽管不同环境及软件版本命令使用略有所差异，但是整个搭建过程都是一致的：**

> 安装相关软件—>生成相关证书：CA 根证书、服务器证书—>配置 open VPN 服务端—>添加防火墙规则：snat—>启动 open VPN 服务端—>创建一个用户测试连接：创建客户端 CA 证书、生成 .ovpn 配置文件、打

> 包相关文件供客户端使用。




1.安装 openvpn、easy-rsa、iptables-services

```
yum -y install epel-release
yum -y install openvpn easy-rsa iptables-services
```

2.使用 easy-rsa 生成需要的证书及相关文件，在这个阶段会产生一些 key 和证书：

- CA 根证书
- OpenVPN 服务器 ssl 证书
- Diffie-Hellman 算法用到的 key

2.1 将 easy-rsa 脚本复制到 /etc/openvpn/，该脚本主要用来方便地生成 CA 证书和各种 key

```
cp -r /usr/share/easy-rsa/ /etc/openvpn/
```

2.2 跳到 easy-rsa 目录并编辑 vars 文件，添加一些生成证书时用到的变量

```
cd /etc/openvpn/easy-rsa/<easy-rsa 版本号>/  # 查看 easy-rsa 版本号：y
vim vars  # 没这个文件的话新建，填写如下内容（变量值根据实际情况随便填写）：
```

```
export KEY_COUNTRY="***"
export KEY_PROVINCE="***"
export KEY_CITY="***"
export KEY_ORG="***"
export KEY_EMAIL="***"
source ./vars   # 使变量生效
```

## 2.3 生成 CA 根证书

```
./easyrsa init-pki
./easyrsa build-ca nopass
```

## 2.4 生成 OpenVPN 服务器证书和密钥

第一个参数 server 为证书名称，可以随便起，比如 `./easyrsa build-server-full openvpn nopass`

```
./easyrsa build-server-full server nopass
```

## 2.5 生成 Diffie-Hellman 算法需要的密钥文件

## 2.6 生成 tls-auth key，这个 key 主要用于防止 DoS 和 TLS 攻击，这一步其实是可选的，但为了安全还是生成一下，该文件在后面配置 open VPN 时会用到。

## 2.7 将上面生成的相关证书文件整理到 /etc/openvpn/server/certs （这一步完全是为了维护方便）

```
mkdir /etc/openvpn/server/certs && cd /etc/openvpn/server/certs/
cp /etc/openvpn/easy-rsa/3/pki/dh.pem ./     # SSL 协商时 Diffie-Hel
cp /etc/openvpn/easy-rsa/3/pki/ca.crt ./        # CA 根证书
cp /etc/openvpn/easy-rsa/3/pki/issued/server.crt ./    # open VPN 服
cp /etc/openvpn/easy-rsa/3/pki/private/server.key ./   # open VPN 服
cp /etc/openvpn/easy-rsa/3/ta.key ./   # tls-auth key
```

## 2.8 创建 open VPN 日志目录

```
mkdir -p /var/log/openvpn/
chown openvpn:openvpn /var/log/openvpn
```

## 3.配置 OpenVPN

可以从 /usr/share/doc/openvpn-/sample/sample-config-files 复制一份 demo 到 /etc/openvpn/（openvpn 版本号查看：yum info openvpn。）然后改改，或者从头开始创建一个新的配置文件。我选择新建配置:

`cd /etc/openvpn/`

`vim server.conf` 填入如下内容（很多配置项不需要特别了解，重要的配置这里注释出来了，其他相关配置项想了解的话见 这里）：

server.conf:

```
port 1194   # 监听的端口号
proto udp   # 服务端用的协议，udp 能快点，所以我选择 udp
dev tun
ca /etc/openvpn/server/certs/ca.crt  #   CA 根证书路径
cert /etc/openvpn/server/certs/server.crt  # open VPN 服务器证书路径
key /etc/openvpn/server/certs/server.key  # open VPN 服务器密钥路径，
dh /etc/openvpn/server/certs/dh.pem  # Diffie-Hellman 算法密钥文件路径
tls-auth /etc/openvpn/server/certs/ta.key 0 #  tls-auth key，参数 0

server 10.8.0.0 255.255.255.0   # 该网段为 open VPN 虚拟网卡网段，不要和
push "dhcp-option DNS 8.8.8.8"  # DNS 服务器配置，可以根据需要指定其他 r
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway def1"   # 客户端所有流量都通过 open VPN 转发，类
compress lzo
duplicate-cn   # 允许一个用户多个终端连接
keepalive 10 120
comp-lzo
persist-key
persist-tun
user openvpn  # open VPN 进程启动用户，openvpn 用户在安装完 openvpn 后就
group openvpn
log /var/log/openvpn/server.log  # 指定 log 文件位置
log-append /var/log/openvpn/server.log
```

```
status /var/log/openvpn/status.log
verb 3
explicit-exit-notify 1
```

4.防火墙相关配置（使用 iptables 添加 snat 规则）
4.1 禁用 Centos7 默认的 firewalld，使用经典的 iptables 防火墙管理软件：

```
systemctl stop firewalld
systemctl mask firewalld
```

4.2 禁用 SELinux
马上关闭：setenforce 0 | 马上生效
永久关闭：sed -i ‘s/SELINUX=enforcing/SELINUX=disabled/g’ /etc/selinux/config | 需要重启服务器生效

4.3 启用iptables

```
systemctl enable iptables
systemctl start iptables
iptables -F
```

4.4 添加防火墙规则，将 openvpn 的网络流量转发到公网： snat 规则

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j MASQUERADE
iptables-save > /etc/sysconfig/iptables   # iptables 规则持久化保存
```

4.5 Linux 服务器启用地址转发

```
echo net.ipv4.ip_forward = 1 >> /etc/sysctl.conf
sysctl -p
```

5.启动 open VPN

```
systemctl start openvpn@server
systemctl enable openvpn@server
systemctl status openvpn@server
```

## 添加一个 OpenVPN 用户

OpenVPN 服务端搭建完了，但是我们该如何使用呢？下面以 Mac 平台下使用为例：

要连接到 open VPN 服务端首先得需要一个客户端软件，在 Mac 下推荐使用 Tunnelblick，下载地址：https://tunnelblick.net/。Tunnelblick 是一个开源、免费的 Mac 版 open VPN 客户端软件。

接下来在服务端创建一个 open VPN 用户：其实创建用户的过程就是生成客户端 SSL 证书的过程，然后将其他相关的证书文件、key、.ovpn 文件（客户端配置文件）打包到一起供客户端使用。由于创建一个用户的过程比较繁琐，所以在此将整个过程写成了一个脚本 ovpn_user.sh，脚本内容比较简单，一看就懂：

首先创建一个客户端配置模板文件 sample.ovpn，该文件在脚本中会用到，放到 /etc/openvpn/client/ 目录，内容如下：
sample.ovpn:

```
client
proto udp
dev tun
```

```
remote [open VPN服务端公网 ip，根据实际情况填写] 1194
ca ca.crt
cert admin.crt
key admin.key
tls-auth ta.key 1
remote-cert-tls server
persist-tun
persist-key
comp-lzo
verb 3
mute-replay-warnings
```

下面为创建 open VPN 用户脚本：

./ovpn_user.sh:

```


set -e

OVPN_USER_KEYS_DIR=/etc/openvpn/client/keys
EASY_RSA_VERSION=3
EASY_RSA_DIR=/etc/openvpn/easy-rsa/
PKI_DIR=$EASY_RSA_DIR/$EASY_RSA_VERSION/pki

for user in "$@"
do
  if [ -d "$OVPN_USER_KEYS_DIR/$user" ]; then
    rm -rf $OVPN_USER_KEYS_DIR/$user
    rm -rf  $PKI_DIR/reqs/$user.req
    sed -i '/'"$user"'/d' $PKI_DIR/index.txt
  fi
  cd $EASY_RSA_DIR/$EASY_RSA_VERSION

  ./easyrsa build-client-full $user nopass

  mkdir -p  $OVPN_USER_KEYS_DIR/$user
  cp $PKI_DIR/ca.crt $OVPN_USER_KEYS_DIR/$user/
  cp $PKI_DIR/issued/$user.crt $OVPN_USER_KEYS_DIR/$user/
  cp $PKI_DIR/private/$user.key $OVPN_USER_KEYS_DIR/$user/
  cp /etc/openvpn/client/sample.ovpn $OVPN_USER_KEYS_DIR/$user/$us
  sed -i 's/admin/'"$user"'/g' $OVPN_USER_KEYS_DIR/$user/$user.ovp
  cp /etc/openvpn/server/certs/ta.key $OVPN_USER_KEYS_DIR/$user/ta
  cd $OVPN_USER_KEYS_DIR
  zip -r $user.zip $user
done
exit 0
```

执行上面脚本创建一个用户：`sh ovpn_user.sh <username>`，会在 /etc/openvpn/client/keys 目录下生成以用户名命名的 zip 打包文件，将该压缩包下载到本地解压，然后将里面的 .ovpn 文件拖拽到 Tunnelblick 客户端软件即可使用。
压缩包里面文件有如下，示例：

```
.
├── ca.crt
├── username.crt
├── username.key
├── username.ovpn
└── ta.key
```

## 删除一个 OpenVPN 用户

上面我们知道了如何添加一个用户，那么如果公司员工离职了或者其他原因，想删除对应用户 OpenVPN 的使用权，该如何操作呢？其实很简单，OpenVPN 的客户端和服务端的认证主要通过 SSL 证书进行双向认证，所以只要吊销对应用户的 SSL 证书即可。

1. 编辑 OpenVPN 服务端配置 server.conf 添加如下配置:

```
crl-verify /etc/openvpn/easy-rsa/3/pki/crl.pem
```

2. 吊销用户证书，假设要吊销的用户名为 username

```
cd /etc/openvpn/easy-rsa/3/
./easyrsa revoke username
./easyrsa gen-crl
```

3. 重启 OpenVPN 服务端使其生效

```
systemctl start openvpn@server
```

为了方便，也将上面步骤整理成了一个脚本，可以一键删除用户：
del_ovpn_user.sh:

```
set -e
OVPN_USER_KEYS_DIR=/etc/openvpn/client/keys
EASY_RSA_VERSION=3
EASY_RSA_DIR=/etc/openvpn/easy-rsa/
for user in "$@"
do
  cd $EASY_RSA_DIR/$EASY_RSA_VERSION
  echo -e 'yes\n' | ./easyrsa revoke $user
  ./easyrsa gen-crl

  if [ -d "$OVPN_USER_KEYS_DIR/$user" ]; then
    rm -rf $OVPN_USER_KEYS_DIR/${user}*
  fi
  systemctl restart openvpn@server
done
exit 0
```

## 安装过程中遇到的问题及解决方法

**问题 1：open VPN 客户端可以正常连接到服务端，但是无法上网，ping 任何地址都不通，只有服务端公网 ip 可以 ping 通。**

问题原因及解决方法：主要原因是服务的地址转发功能没打开，其实我前面配置
了 echo net.ipv4.ip_forward = 1 >> /etc/sysctl.conf，但是

没有执行 sysctl -p 使其
立即生效，所以才导致出现问题。因此一定要记得两条命令都要执行。

**问题 2: open VPN 可以正常使用，但是看客户端日志却有如下错误：**

```
2019-06-15 02:39:03.957926 AEAD Decrypt error: bad packet ID (may b
2019-06-15 02:39:23.413750 AEAD Decrypt error: bad packet ID (may b
```

问题原因及解决方法：
其实这个问题一般在 open VPN 是 UDP 服务的情况下出现，主要原因是 UDP 数据包重复发送导致，在 Wi-Fi 网络下经常出现，这并不影响使用，但是我们可以选择禁止掉该错误：根据错误提示可知使用 –mute-replay-warnings 参数可以消除该警告，我们使用的 open VPN 是 GUI 的，所以修改客户端 .ovpn 配置文件，末尾添加：mute-replay-warnings 即可解决。

该问题在这里有讨论：
https://sourceforge.net/p/openvpn/mailman/message/10655695/

## 相关文档

关于 open VPN 客户端和服务端配置文件配置项说明：很全面，可以随时查看不懂的配置项
https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

https://openvpn.net/ | OpenVPN 官网

https://www.fandenggui.com/post/centos7-install-openvpn.html | Centos7 安装 OpenVPN
https://www.howtoing.com/how-to-install-openvpn-on-centos-7 | Centos7 安装 OpenVPN

https://www.xiaohui.com/dev/server/20070904-revoke-openvpn-client.htm | 吊销客户端证书
https://scott.stevensononthe.net/2015/02/how-to-addremove-additional-users-to-openvpn/ | 吊销客户端证书
https://tunnelblick.net/cConnectedBut.html | open VPN 一些常见问题
https://tunnelblick.net/ipinfo | 本地公网 ip 查看