**OpenVPN for CentOS**

**服务器端配置**

**1、安装openvpn**

首先安装依赖库

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

我们这边用yum安装，当然你也可以自己编译安装（从这个页面下载：<http://openvpn.net/index.php/download.html>）。

# yum install openvpn

**2、配置服务器**

**2.1初始化服务端**

# cp /usr/share/doc/openvpn-2.3.1/sample/sample-config-files/server.conf /etc/openvpn/

注：2.3版本需要独立下载个easy-rsa，该包用来制作ca证书，服务端证书，客户端证书,openvpn2.3.0该版本源码不包含easy-rsa,所以需要单独下载安装用来配合openvpn实现证书生成。

# wget -c https://github.com/OpenVPN/easy-rsa/archive/master.zip

# unzip master

# mv easy-rsa-master easy-rsa

# cp -rf easy-rsa /etc/openvpn

**2.2配置PKI**

# cd /etc/openvpn/easy-rsa/easy-rsa/2.0

# vim vars

找到”export KEY\_SIZE=”这行，根据情况把1024改成2048或者4096

再定位到最后面，会看到类似下面这样的

export KEY\_COUNTRY=”US”

export KEY\_PROVINCE=”CA”

export KEY\_CITY=”SanFrancisco”

export KEY\_ORG=”Fort-Funston”

export KEY\_EMAIL=”[me@myhost.mydomain](mailto:me%40myhost.mydomain)“

这个自己根据情况改一下，不改也可以运行。其实不改vars这个文件，vpn也可以跑起来。

例如：

export KEY\_COUNTRY=”CN”

export KEY\_PROVINCE=”SH”

export KEY\_CITY=”Shanghai”

export KEY\_ORG=”xxx”

export KEY\_EMAIL=”[xxx@xxx.cn](mailto:xxx%40xxx.cn)“

注：在后面生成服务端ca证书时，这里的配置会作为缺省配置

做SSL配置文件软链：

# ln -s openssl-1.0.0.cnf openssl.cnf

修改vars文件可执行并调用

# chmod +x vars

**3、产生证书**

**3.1、产生CA证书**

# source ./vars

NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/easy-rsa/2.0/keys

注：也就是如果执行./clean-all，就会清空/etc/openvpn/easy-rsa/easy-rsa/2.0/keys下所有文件

开始配置证书：

* 清空原有证书

# ./clean-all

注：下面这个命令在第一次安装时可以运行，以后在添加完客户端后慎用，因为这个命令会清除所有已经生成的证书密钥，和上面的提示对应

* 生成服务器端ca证书

# ./build-ca

注：由于之前做过缺省配置，这里一路回车即可

**3.2、产生服务器证书**

# ./build-key-server openvpn.example.com

生成服务器端密钥证书, 后面这个openvpn.example.com就是服务器名，也可以自定义，可以随便起，但要记住，后面要用到。

**3.3、生成DH验证文件**

# ./build-dh

生成diffie hellman参数，用于增强openvpn安全性（生成需要漫长等待），让服务器飞一会。

**3.4、生成客户端证书**

# ./build-key client1

# ./build-key client2

（名字任意，建议写成你要发给的人的姓名，方便管理）

注：这里与生成服务端证书配置类似，中间一步提示输入服务端密码，其他按照缺省提示一路回车即可。

**3.5、编辑服务配置文件**

# vim /etc/openvpn/server.conf

注：可按照默认模板配置，本例为自定义配置文件：

# 设置监听IP，默认是监听所有IP

;local a.b.c.d

# 设置监听端口，必须要对应的在防火墙里面打开

port 1194

# 设置用TCP还是UDP协议？

;proto tcp

proto tcp

# 设置创建tun的路由IP通道，还是创建tap的以太网通道路由IP容易控制，所以推荐使用它；

# 但如果如IPX等必须使用第二层才能通过的通讯，则可以用tap方式，tap也就是以太网桥接

;dev tap

dev tun

# 这里是重点，必须指定SSL/TLS root certificate (ca),

# certificate(cert), and private key (key)

# ca文件是服务端和客户端都必须使用的，但不需要ca.key

# 服务端和客户端指定各自的.crt和.key

# 请注意路径,可以使用以配置文件开始为根的相对路径,

# 也可以使用绝对路径

# 请小心存放.key密钥文件

ca /etc/openvpn/easy-rsa/easy-rsa/2.0/keys/ca.crt

cert /etc/openvpn/easy-rsa/easy-rsa/2.0/keys/openvpn.example.com.crt

key /etc/openvpn/easy-rsa/easy-rsa/2.0/keys/openvpn.example.com.key # This file should be kept secret

# 指定Diffie hellman parameters.

dh /etc/openvpn/easy-rsa/easy-rsa/2.0/keys/dh2048.pem

# 配置VPN使用的网段，OpenVPN会自动提供基于该网段的DHCP服务，但不能和任何一方的局域网段重复，保证唯一

server 10.8.0.0 255.255.255.0

# 维持一个客户端和virtual IP的对应表，以方便客户端重新连接可以获得同样的IP

ifconfig-pool-persist ipp.txt

# 为客户端创建对应的路由,以另其通达公司网内部服务器

# 但记住，公司网内部服务器也需要有可用路由返回到客户端

;push "route 192.168.20.0 255.255.255.0"

push "route 10.6.0.0 255.255.0.0"

# 若客户端希望所有的流量都通过VPN传输,则可以使用该语句

# 其会自动改变客户端的网关为VPN服务器,推荐关闭

# 一旦设置，请小心服务端的DHCP设置问题

;push "redirect-gateway"

# 用OpenVPN的DHCP功能为客户端提供指定的DNS、WINS等

;push "dhcp-option DNS 10.8.0.1"

;push "dhcp-option WINS 10.8.0.1"

# 默认客户端之间是不能直接通讯的，除非把下面的语句注释掉

client-to-client

# 下面是一些对安全性增强的措施

# For extra security beyond that provided by SSL/TLS, create an "HMAC firewall"

# to help block DoS attacks and UDP port flooding.

#

# Generate with:

# openvpn --genkey --secret ta.key

#

# The server and each client must have a copy of this key.

# The second parameter should be 0 on the server and 1 on the clients.

tls-auth ta.key 0 # This file is secret

# 使用lzo压缩的通讯,服务端和客户端都必须配置

comp-lzo

# 输出短日志,每分钟刷新一次,以显示当前的客户端

status /var/log/openvpn/openvpn-status.log

# 缺省日志会记录在系统日志中，但也可以导向到其他地方

# 建议调试的使用先不要设置,调试完成后再定义

log /var/log/openvpn/openvpn.log

log-append /var/log/openvpn/openvpn.log

# 设置日志的级别

#

# 0 is silent, except for fatal errors

# 4 is reasonable for general usage

# 5 and 6 can help to debug connection problems

# 9 is extremely verbose

verb 3

创建日志目录：

# mkdir -p /var/log/openvpn/

**4、启动服务**

# service openvpn start

或者

# /etc/init.d/openvpn start

如果遭遇启动失败的情况，可以在配置文件中加上一行log-append openvpn.log

再尝试启动，然后到/var/log/openvpn/检查openvpn.log文件来查看错误发生原因。

最后执行

# chkconfig openvpn on

将openvpn加入启动项

设置外网访问

# vim /etc/sysctl.conf

找到net.ipv4.ip\_forward = 0

把0改成1

# sysctl -p

设置iptables（这一条至关重要，通过配置nat将vpn网段IP转发到server内网）

# iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

设置openvpn端口通过：

# iptables -A INPUT -p TCP --dport 1194 -j ACCEPT

# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

重启iptables:

注：这里提一下,INPUT策略是执行后即时生效的，POSTROUTING需要保存并重启服务才能生效

# service iptables save

# service iptables restart

配置iptables开机启动

# chkconfig iptables on

**5、开通防火墙端口**

注：可以参考这个帮助文档：<http://docs.ucloud.cn/unetwork/unetwork.html#id1>

在后台，“防火墙管理”，选中您主机应用的防火墙，点击编辑。

点击“添加规则”，增加如下TCP 1194，然后“应用规则”。

**客户端配置**

**将服务器端生成的key（ca.crt，client.crt，client.key，ta.key）下载到本地。**

进入客户端OpenVPN目录，将sample-config下的client.ovpn文件复制到config目录，

client端做相应的修改：

remote xxx.xxx.xxx.xxx 1194

proto tcp

dev tun

ca ca.crt

cert xxx.crt

key xxx.key

tls-auth ta.key 1

comp-lzo

user nobody

group nobody

persist-key

persist-tun

**Windows客户端**

下载地址：<http://openvpn.net/index.php/download.html>

<http://swupdate.openvpn.org/community/releases/openvpn-2.2.2-install.exe>

将key和新建的client.ovpn放到C:/Program Files/OpenVPN/config目录下，到桌面双击openvpn图标即可。

**Mac客户端**

<https://code.google.com/p/tunnelblick/>

1.打开Tunnelblick

2.点击左下角+

3.我有设置文件

4.OpenVPN设置

5.打开私人设置文件夹

6.将key和新建的client.ovpn放到此目录下

**Linux客户端**

# yum install openvpn

# openvpn --daemon --config client.ovpn