CentOS6 安装 openvpn(路由模式证书认证)

服务器端配置

1、安装 openvpn

rpm -ivh http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
yum install openvpn -y
当然也可以从这个页面下载：http://openvpn.net/index.php/download.html

2、配置服务器

2.1 初始化服务端

cd /etc/openvpn/
cp /usr/share/doc/openvpn-2.2.2/sample-config-files/server.conf .
mkdir -p easy-rsa/keys && cd easy-rsa
cp -rf /usr/share/doc/openvpn-2.2.2/easy-rsa/2.0/* . && chmod +x *

2.2 配置 PKI

vi 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"
export KEY_EMAIL=mail@host.domain
export KEY_CN=changeme
export KEY_NAME=changeme
export KEY_OU=changeme
export PKCS11_MODULE_PATH=changeme
export PKCS11_PIN=1234

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。

3、产生证书

3.1、产生 CA 证书

. ./vars 或者: source ./vars

注意：前面是点儿空格再点儿

./clean-all && cp openssl-1.0.0.cnf openssl.cnf && ./build-ca

在这之前执行 yum install openssl -y

狂敲回车即可，也可以随便写点资料。

3.2、产生服务器证书

./build-key-server myServer
myServer 即服务器名，可以随便起，但要记住，后面要用到。
一路回车，遇到询问一律输入 y

3.3、生成 DH 验证文件

./build-dh
这个没什么好说的，让服务器飞一会。

3.4、生成客户端证书

./build-key client1
client1 替换成需要的用户，一路回车，遇到询问一律输入 y

3.5、编辑服务配置文件

vi /etc/openvpn/server.conf

- 找到 port 一行，后面的 1194 是端口号，根据需要进行调整
- 找到 ca ca.crt 这行，ca.crt 替换为/etc/openvpn/easy-rsa/keys/ca.crt
- cert 这行后面的 server.crt 替换为/etc/openvpn/easy-rsa/keys/myServer.crt
- key 这行后面的 server.key 替换为/etc/openvpn/easy-rsa/keys/myServer.key
- dh 这行后面的 dh1024.pem 替换为/etc/openvpn/easy-rsa/keys/dh1024.pem
  注意上面两行的 myServer.crt 和 myServer.key 就是前面生成的东西。
- 找到;push "redirect-gateway def1 bypass-dhcp"，去掉最前面的注释符号，并且删除 def1 后面的 bypass-dhcp，也就是将这行替换成：push "redirect-gateway def1"
- 找到 ;push "dhcp-option DNS 208.67.222.222"以及;push "dhcp-option DNS 208.67.222.220" 替换为 push "dhcp-option DNS 8.8.8.8"以及 push "dhcp-option DNS 8.8.4.4" 同样是去掉前面的注释符号，这个可以根据自己的情况进行更改。

其他默认就可以了，保存配置。

4、启动服务

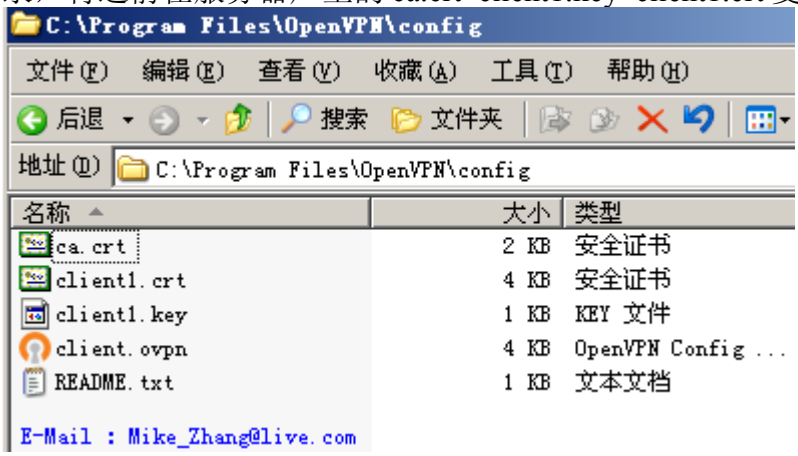
service openvpn start
或者
/etc/init.d/openvpn start
如果遭遇启动失败的情况，可以在配置文件中加上一行 log-append openvpn.log
再尝试启动，然后到/etc/openvpn/检查 openvpn.log 文件来查看错误发生原因最后执行一行
chkconfig --level 235 openvpn on
将 openvpn 加入启动项
设置外网访问
vi /etc/sysctl.conf

找到 net.ipv4.ip_forward = 0
把 0 改成 1
sysctl -p
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source 2.2.2.2
把 2.2.2.2 替换成你自己 VPS 的 IP
/etc/init.d/iptables save
/etc/init.d/iptables restart

客户端配置

下载地址：http://openvpn.net/index.php/download.html
Windows 链接：http://swupdate.openvpn.org/community/releases/openvpn-2.2.2-install.exe

进入 C:\Program Files\OpenVPN 目录，将 sample-config 下的 client.ovpn 文件复制到 config 目录，将之前在服务器产生的 ca.crt client1.key client1.crt 复制到 config 目录。



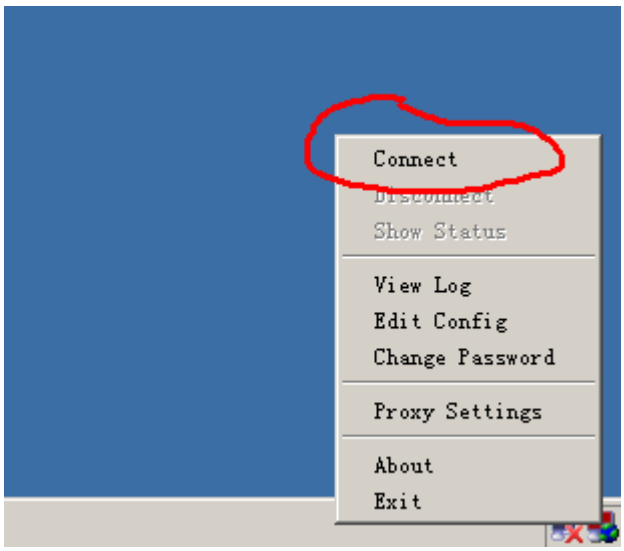
进行如下修改：
找到“remote my-server-1 1194”，修改成服务器相应配置

ca ca.crt
cert client.crt
key client.key

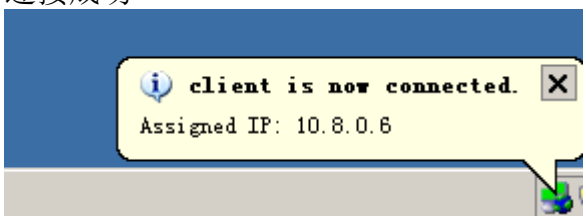
改为如下配置：
ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\client1.crt"
key "C:\\Program Files\\OpenVPN\\config\\client1.key"

其它不变。

在这里进行连接


Connect
Disconnect
Show Status
View Log
Edit Config
Change Password
Proxy Settings
About
Exit

连接成功


client is now connected.
Assigned IP: 10.8.0.6