**Linxu下OpenVPN安装**

**1、安装前准备**

# 关闭selinux

setenforce 0

sed -i '/^SELINUX=/c\SELINUX=disabled' /etc/selinux/config

# 安装openssl和lzo，lzo用于压缩通讯数据加快传输速度

yum -y install openssl openssl-devel

yum -y install lzo

# 安装epel源

yum install –y epel\*

**2、安装及配置OpenVPN和easy-rsa**

# 安装openvpn和easy-rsa

yum -y install openvpn easy-rsa

# 修改vars文件

cd /usr/share/easy-rsa/2.0/

vim vars

# 修改注册信息，比如公司地址、公司名称、部门名称等。

export KEY\_COUNTRY="CN"

export KEY\_PROVINCE="Shandong"

export KEY\_CITY="Qingdao"

export KEY\_ORG="MyOrganization"

export KEY\_EMAIL="me@myhost.mydomain"

export KEY\_OU="MyOrganizationalUnit"

# 初始化环境变量

source vars

# 清除keys目录下所有与证书相关的文件

# 下面步骤生成的证书和密钥都在/usr/share/easy-rsa/2.0/keys目录里

./clean-all

# 生成根证书ca.crt和根密钥ca.key（一路按回车即可）

./build-ca

# 为服务端生成证书和密钥（一路按回车，直到提示需要输入y/n时，输入y再按回车，一共两次）

./build-key-server server

# 每一个登陆的VPN客户端需要有一个证书，每个证书在同一时刻只能供一个客户端连接，下面建立2份

# 为客户端生成证书和密钥（一路按回车，直到提示需要输入y/n时，输入y再按回车，一共两次）

./build-key client1

./build-key client2

# 创建迪菲 赫尔曼密钥，会生成dh2048.pem文件（生成过程比较慢，在此期间不要去中断它）

./build-dh

# 生成ta.key文件（防DDos攻击、UDP淹没等恶意攻击）

openvpn --genkey --secret keys/ta.key



**3、创建服务器端配置文件**

# 在openvpn的配置目录下新建一个keys目录

mkdir /etc/openvpn/keys

# 将需要用到的openvpn证书和密钥复制一份到刚创建好的keys目录中

cp /usr/share/easy-rsa/2.0/keys/{ca.crt,server.{crt,key},dh2048.pem,ta.key} /etc/openvpn/keys/

# 复制一份服务器端配置文件模板server.conf到/etc/openvpn/

cp /usr/share/doc/openvpn-2.3.2/sample/sample-config-files/server.conf /etc/openvpn/

# 查看server.conf里的配置参数

grep '^[^#;]' /etc/openvpn/server.conf

# 编辑server.conf

vim /etc/openvpn/server.conf

port 1194

# 改成tcp，默认使用udp，如果使用HTTP Proxy，必须使用tcp协议

proto tcp

dev tun

# 路径前面加keys，全路径为/etc/openvpn/keys/ca.crt

ca keys/ca.crt

cert keys/server.crt

key keys/server.key # This file should be kept secret

dh keys/dh2048.pem

# 默认虚拟局域网网段，不要和实际的局域网冲突即可

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

# 10.0.0.0/8是我这台VPN服务器所在的内网的网段，读者应该根据自身实际情况进行修改

push "route 10.0.0.0 255.0.0.0"

# 可以让客户端之间相互访问直接通过openvpn程序转发，根据需要设置

client-to-client

# 如果客户端都使用相同的证书和密钥连接VPN，一定要打开这个选项，否则每个证书只允许一个人连接VPN

duplicate-cn

keepalive 10 120

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

comp-lzo

persist-key

persist-tun

# OpenVPN的状态日志，默认为/etc/openvpn/openvpn-status.log

status openvpn-status.log

# OpenVPN的运行日志，默认为/etc/openvpn/openvpn.log

log-append openvpn.log

# 改成verb 5可以多查看一些调试信息

verb 5

4、配置内核和防火墙，启动服务

# 开启路由转发功能

sed -i '/net.ipv4.ip\_forward/s/0/1/' /etc/sysctl.conf

sysctl -p

# 配置防火墙，别忘记保存

iptables –F

iptables -X

iptables -I INPUT -p tcp --dport 1194 -m comment --comment "openvpn" -j ACCEPT

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

service iptables save

# 启动openvpn并设置为开机启动

service openvpn start

chkconfig openvpn on

**5、创建客户端配置文件**

# 复制一份client.conf模板命名为client.ovpn

cp /usr/share/doc/openvpn-2.3.2/sample/sample-config-files/client.conf client.ovpn

# 编辑client.ovpn

vim client.ovpn

client

dev tun

# 改为tcp

proto tcp

# OpenVPN服务器的外网IP和端口

remote 203.195.xxx.xxx 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

# client1的证书

cert client1.crt

# client1的密钥

key client1.key

ns-cert-type server

# 去掉前面的注释

tls-auth ta.key 1

comp-lzo

verb 3

6、导出客户端配置文件

安装openvpn软件并将OpenVPN服务器上的client.ovpn、ca.crt、client1.crt、client1.key、ta.key上传到Windows客户端安装目录下的config文件夹（C:\Program Files\OpenVPN\config）