1 安装

yum install strongswan xl2tpd

2.安装xl2tpd

 在CentOS 6官方的yum源中，没有这个软件包。CentOS6 X64 Xl2tp安装包对应下载地址：

       wget <http://dl.fedoraproject.org/pub/epel/6/x86_64/xl2tpd-1.3.6-2.el6.x86_64.rpm>

   yum install xl2tpd-1.3.6-2.el6.x86\_64.rpm（其它版本请自行修改包名）

yum install ppp

2調整kernel和iptables

/etc/sysctl.conf

net.ipv4.ip\_forward = 1

cat /etc/sysconfig/iptables  
# Generated by iptables-save v1.4.7 on Fri Nov 11 15:23:57 2016  
\*filter  
:INPUT ACCEPT [55:3688]  
:FORWARD ACCEPT [0:0]  
:OUTPUT ACCEPT [39:3232]  
-A INPUT -p esp -j ACCEPT   
-A INPUT -p ah -j ACCEPT   
-A INPUT -p udp -m udp --dport 500 -j ACCEPT   
-A INPUT -p udp -m udp --dport 4500 -j ACCEPT   
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  
-A INPUT -p udp -m policy --dir in --pol ipsec -m udp --dport 1701 -j ACCEPT   
COMMIT  
# Completed on Fri Nov 11 15:23:57 2016  
# Generated by iptables-save v1.4.7 on Fri Nov 11 15:23:57 2016  
\*nat  
:PREROUTING ACCEPT [205:13689]  
:POSTROUTING ACCEPT [0:0]  
:OUTPUT ACCEPT [58:4176]  
-A POSTROUTING -m policy --dir out --pol none -j MASQUERADE   
COMMIT

3 设置ipsec配置文件，编辑/etc/ipsec.conf

[root@localhost ]# cat ipsec.conf

# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup

# strictcrlpolicy=yes

# uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed

# leftsubnet=10.1.0.0/16

# leftcert=selfCert.der

# leftsendcert=never

# right=192.168.0.2

# rightsubnet=10.2.0.0/16

# rightcert=peerCert.der

# auto=start

#conn sample-with-ca-cert

# leftsubnet=10.1.0.0/16

# leftcert=myCert.pem

# right=192.168.0.2

# rightsubnet=10.2.0.0/16

# rightid="C=CH, O=Linux strongSwan CN=peer name"

# auto=start

conn %default

ikelifetime=60m

keylife=20m

rekeymargin=3m

keyingtries=1

conn l2tp

keyexchange=ikev1

left= x.x.x.x vpn服务器ip

leftsubnet=0.0.0.0/0

leftprotoport=17/1701

authby=secret

leftfirewall=no

right=%any

rightprotoport=17/%any

type=transport

auto=add

配置ipsec预共享密钥

[root@localhost ]# cat ipsec.secrets 设置密钥

: PSK "public"

[root@localhost ]# cat xl2tpd.conf

[global]

listen-addr = x.x.x.x vpn服务器ip地址

[lns default]

ip range = 192.168.100.100-192.168.100.200

local ip = 192.168.100.1

refuse chap = yes

refuse pap = yes

require authentication = yes

ppp debug = yes

pppoptfile = /etc/ppp/options.xl2tpd

length bit = yes

assign ip = yes

name = VPNServer 对应chap-secrets中的server

如果上面的xl2tpd.conf使用了pam驗證，要修改下面這個

**/etc/pam.d/ppp**

|  |  |
| --- | --- |
| 1  2  3  4  5 | #%PAM-1.0  auth    required        pam\_nologin.so  auth    required        pam\_unix.so  account required        pam\_unix.so  session required        pam\_unix.so |

[root@localhost ]# cat options.xl2tpd 此文档默认就好

ipcp-accept-local

ipcp-accept-remote

ms-dns 8.8.8.8

noccp

auth

crtscts

idle 1800

mtu 1410

mru 1410

nodefaultroute

debug

lock

proxyarp

connect-delay 5000

Login

[root@localhost vpn]# cat chap-secrets

# Secrets for authentication using CHAP

# client server secret IP addresses

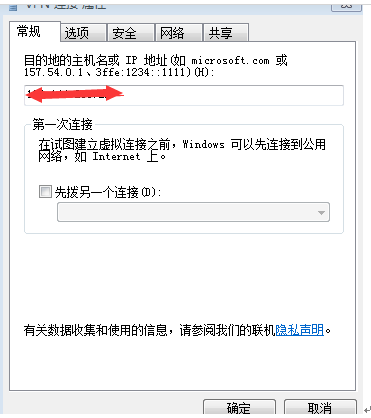
test VPNServer test \*

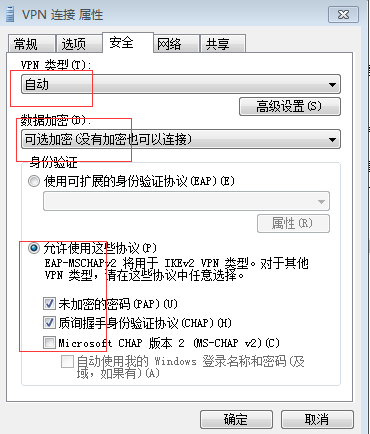
test1 VPNServer test1 \*

設定就到這邊為止，接著就可以啟動VPN了

|  |  |
| --- | --- |
| 1  2 | service strongswan start  service xl2tpd start |

客户端设置,填写vpn服务器的ip.





设置密钥,密钥为ipsec.secrets这个文件里的内容

