Centos 6.5 下配置L2tp Vpn

1.安装依赖包：yum install make gcc gcc-c++.

2.安装openswan xl2tpd

3.配置

（**1）编辑 /etc/ipsec.conf**

config setup

# Debug-logging controls: "none" for (almost) none, "all" for lots.

# klipsdebug=none

# plutodebug="control parsing"

# For Red Hat Enterprise Linux and Fedora, leave protostack=netkey

protostack=netkey

nat\_traversal=yes

virtual\_private=%v4:10.0.0.0/8

oe=off

# Enable this if you see "failed to find any available worker"

# nhelpers=0

#You may put your configuration (.conf) file in the "/etc/ipsec.d/" and uncomment this.

#include /etc/ipsec.d/\*.conf

conn L2TP-PSK-NAT

rightsubnet=vhost:%priv

also=L2TP-PSK-noNAT

conn L2TP-PSK-noNAT

authby=secret

pfs=no

auto=add

keyingtries=3

rekey=no

ikelifetime=8h

keylife=1h

type=transport

left=10.9.146.18

# left=106.75.95.237

leftprotoport=17/1701

right=%any

rightprotoport=17/%any

dpddelay=40

dpdtimeout=130

dpdaction=clear

leftnexthop=%defaultroute

rightnexthop=%defaultroute

**（2）编辑/etc/ipsec.secrets （设置ipsec密钥）**

include /etc/ipsec.d/\*.secrets

#106.75.95.237 %any: PSK "xinyuxiongdi"

10.9.146.18 %any: PSK "xinyuxiongdi"

**（3） 修改/添加 /etc/sysctl.conf并生效**

net.ipv4.ip\_forward = 1

net.ipv4.conf.default.rp\_filter = 0

net.ipv4.conf.all.send\_redirects = 0

net.ipv4.conf.default.send\_redirects = 0

net.ipv4.conf.all.log\_martians = 0

net.ipv4.conf.default.log\_martians = 0

net.ipv4.conf.default.accept\_source\_route = 0

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.default.accept\_redirects = 0

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

**（4）验证ipsec运行状态**

[root@10-9-146-18 ~]# ipsec verify

Verifying installed system and configuration files

Version check and ipsec on-path [OK]

Libreswan 3.15 (netkey) on 2.6.32-431.11.25.el6.ucloud.x86\_64

Checking for IPsec support in kernel [OK]

NETKEY: Testing XFRM related proc values

ICMP default/send\_redirects [OK]

ICMP default/accept\_redirects [OK]

XFRM larval drop [OK]

Pluto ipsec.conf syntax [OK]

Hardware random device [N/A]

Checking rp\_filter [OK]

Checking that pluto is running [OK]

Pluto listening for IKE on udp 500 [OK]

Pluto listening for IKE/NAT-T on udp 4500 [OK]

Pluto ipsec.secret syntax [OK]

Checking 'ip' command [OK]

Checking 'iptables' command [OK]

Checking 'prelink' command does not interfere with FIPSChecking for obsolete ipsec.conf options [OK]

Opportunistic Encryption [DISABLED]

**（5） 编辑 /etc/xl2tpd/xl2tpd.conf**

[global]

listen-addr = 10.9.146.18

; requires openswan-2.5.18 or higher - Also does not yet work in combination

; with kernel mode l2tp as present in linux 2.6.23+

; ipsec saref = yes

; Use refinfo of 22 if using an SAref kernel patch based on openswan 2.6.35 or

; when using any of the SAref kernel patches for kernels up to 2.6.35.

; saref refinfo = 30

; force userspace = yes

; debug tunnel = yes

[lns default]

ip range = 10.0.0.51-10.0.0.254

local ip = 10.0.0.1

require chap = yes

refuse pap = yes

require authentication = yes

name = LinuxVPNserver

ppp debug = yes

pppoptfile = /etc/ppp/options.xl2tpd

length bit = yes

**（6）配置用户名,密码:编辑 /etc/ppp/chap-secrets**

# Secrets for authentication using CHAP

# client server secret IP addresses

wangdong \* 1qaz2wsx3edc 10.0.0.55

zhaojianwei \* xyxd@1qaz2wsx3edc! 10.0.0.100

**（7）重启xl2tp ipsec，添加自启动**

/etc/init.d/xl2tp restart

/etc/init.d/ipsec restart

chkconfig xl2tpd on

chkconfig ipsec on

**（7）测试L2TP**

配置完成后在Windows上设置VPN登录。

登录成功后在服务器中会显示ppp0接口信息。

ppp0 Link encap:Point-to-Point Protocol

inet addr:10.0.0.1 P-t-P:10.0.0.55 Mask:255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1400 Metric:1

RX packets:38 errors:0 dropped:0 overruns:0 frame:0

TX packets:14 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:3

RX bytes:2947 (2.8 KiB) TX bytes:2167 (2.1 KiB)

如果服务器重启后连接L2TP不能上网，则看iptables服务器是否开启。