## pptp服务器

1. 安装

# yum install -y epel-release

# yum install -y ppp pptpd

1. 修改配置文件

本地隧道网卡地址和客户端地址池

# vim /etc/pptpd.conf

localip 10.10.1.1

remoteip 10.10.1.10-100

隧道DNS

# vim /etc/ppp/options.pptpd

ms-dns 8.8.8.8

ms-dns 8.8.4.4

options.pptpd解析

refuse-pap 禁止认证方式

require-pap 允许认证方式

#chap mschap mschapv2用户管理 第一个\*是options.pptpd中name项

# vim /etc/ppp/chap-secrets

user \* 123456 \*

pap认证用户管理

# vim /etc/ppp/pap-secrets

user \* 123456 \*

允许系统路由转发

# vim /etc/sysctl.conf

net.ipv4.ip\_forward=1

1. 防火墙规则

放行pptp服务端口，设置nat规则， ens33网卡名称

# firewall-cmd --permanent --zone=public --add-port=1723/tcp

# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p gre -j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p gre -j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv4 filter FORWARD 0 -i ppp+ -o ens33 -j ACCEPT

# firewall-cmd --permanent --direct --add-rule ipv4 filter FORWARD 0 -i ens33 -o ppp+ -j ACCEPT

# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o ens33 -j MASQUERADE -s 10.10.1.0/24

# firewall-cmd –reload

1. 启动并设置开机自启pptpd服务

# systemctl restart pptpd && systemctl enable pptpd

## l2tp/ipsec服务器

同样需要ppp配置文件中编辑用户

使用strongswan

# yum install epel-release -y

# yum install ppp xl2tpd strongswan -y

修改配置文件

# vi /etc/strongswan/ipsec.conf

version 2

conn L2TP-PSK-NAT

authby=secret

auto=add

keyingtries=3

rekey=no

ikelifetime=8h

keylife=1h

type=transport

left=192.168.0.143

leftprotoport=17/1701

right=%any

rightprotoport=17/%any

dpddelay=30

dpdtimeout=120

dpdaction=clear

ike=aes128-sha1-modp1024,aes128-sha1-modp1536,aes128-sha1-modp2048,aes128-sha256-ecp256,aes128-sha256-modp1024,aes128-sha256-modp1536,aes128-sha256-modp2048,aes256-aes128-sha256-sha1-modp2048-modp4096-modp1024,aes256-sha1-modp1024,aes256-sha256-modp1024,aes256-sha256-modp1536,aes256-sha256-modp2048,aes256-sha256-modp4096,aes256-sha384-ecp384,aes256-sha384-modp1024,aes256-sha384-modp1536,aes256-sha384-modp2048,aes256-sha384-modp4096,aes256gcm16-aes256gcm12-aes128gcm16-aes128gcm12-sha256-sha1-modp2048-modp4096-modp1024,3des-sha1-modp1024!

esp=aes128-aes256-sha1-sha256-modp2048-modp4096-modp1024,aes128-sha1,aes128-sha1-modp1024,aes128-sha1-modp1536,aes128-sha1-modp2048,aes128-sha256,aes128-sha256-ecp256,aes128-sha256-modp1024,aes128-sha256-modp1536,aes128-sha256-modp2048,aes128gcm12-aes128gcm16-aes256gcm12-aes256gcm16-modp2048-modp4096-modp1024,aes128gcm16,aes128gcm16-ecp256,aes256-sha1,aes256-sha256,aes256-sha256-modp1024,aes256-sha256-modp1536,aes256-sha256-modp2048,aes256-sha256-modp4096,aes256-sha384,aes256-sha384-ecp384,aes256-sha384-modp1024,aes256-sha384-modp1536,aes256-sha384-modp2048,aes256-sha384-modp4096,aes256gcm16,aes256gcm16-ecp384,3des-sha1!

配置密钥

# vi /etc/strongswan/ipsec.secrets

%any %any : PSK “123456”

配置xl2tp

#vim /etc/xl2tpd/xl2tpd.conf

[lns default]

ip range = 192.168.10.10-192.168.10.100

local ip = 192.168.10.9

require chap = yes

refuse pap = yes

require authentication = yes

name = LinuxVPNserver

ppp debug = yes

pppoptfile = /etc/ppp/options.xl2tpd

length bit = yes

配置pppoptfile

#vim /etc/ppp/options.xl2tpd

ipcp-accept-local

ipcp-accept-remote

ms-dns 114.114.114.114

name xl2tpd

#noccp

auth

#crtscts

idle 1800

mtu 1410

mru 1410

nodefaultroute

debug

#lock

proxyarp

connect-delay 5000

refuse-pap

refuse-mschap

require-mschap-v2

persist

logfile /var/log/xl2tpd.log

防火墙规则，只要连接测试也可以直接关闭防火墙

#firewall-cmd --permanent --add-service=ipsec

#firewall-cmd --permanent --add-port=1701/udp

#firewall-cmd --permanent --add-masquerade

#firewall-cmd --reload

开启

systemctl start strongswan

systemctl start xl2tpd

centos l2tp客户端

# yum install NetworkManager-l2tp NetworkManager-l2tp-gnome

centos pptp客户端

# yum install NetworkManager-pptp NetworkManager-pptp-gnome