### vpn服务器操作手册

**前言：**

1.蓝色字体表示命令行命令，正式执行时不要复制前面的#号，#号只是提示应该使用root权限操作

2.绿色字体表示注释，有时注释太多就不用绿色表示了

3.注意：本文档的所有操作请先在在测环境进行实践，请不要直接在真实的服务器中操作！

**版权声明**：

本文档以开源的形式发布，所有条款如下：

1. 无担保：作者不保证文档内容的准确无误，亦不承担由于使用此文档所导致的任何后果

2. 自由使用：任何人可以出于任何目的而自由地 阅读/链接/打印/转载/引用/再创作 此文档，无需任何附加条件

若您 阅读/链接/打印/转载/引用/再创作 本文档，则说明接受以上2个条款。

作者：李茂福

时间：2023-03-18

**第0章、VPN简介**

**VPN解决的问题：**

①不同的用户可使用重叠（相同）的ip地址段，在转发时互不干扰，路由表隔离开来

②用户的ip地址不暴露在外网上，是以隧道的方式传递的（将用户流量封装在外网流量之上）

**VPN隧道分类：**

①pptp/l2tp/vxlan这些是将用户的二层流量（mac帧）封装在外网的udp报文之上，也称为二层隧道协议

②ipsec这种是将用户的三层流量（ip报文）封装在外网的ip报文之上，也称为三层隧道协议

③mpls vpn这种是在用户的三层流量之前插入一个mpls Label，在外网上只根据mpls label进行转发，也称为第二层之上和第三层之下的隧道技术

④OpenVPN既支持将用户的二层流量封装在传输层之上，也可将用户的三层流量封装在传输层之上（传输层可用tcp也可用udp）

**外网**是指不属于用户内部网络的网络，是用来承载用户内部网络流量并打通用户不同站点之间的通信（用于承载用户要走隧道的流量）

**第一章、L2TP VPN**

在

**第二章、ipsec（strongswan）**

在epel源里有strongswan的安装包

# cat /etc/yum.repos.d/epel.repo

[epel]

name=Extra Packages for Enterprise Linux 7 - $basearch

#baseurl=http://download.fedoraproject.org/pub/epel/7/$basearch

metalink=https://mirrors.fedoraproject.org/metalink?repo=epel-7&arch=$basearch

failovermethod=priority

enabled=1

gpgcheck=1

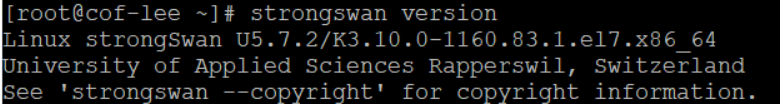
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7

# yum install epel-release #安装epel的yum源

# yum install strongswan #安装strongswan

#依赖trousers包

# strongswan version #查看安装的版本



# vi /etc/strongswan/ipsec.conf #主配置文件

config setup

uniqueids=never #关闭ID唯一性，即允许多个客户端使用同一个证书，多设备同时在线

conn %default #默认配置项，其他conn配置项都会调用此默认项

authby=psk #默认使用预共享密钥认证方式

type=tunnel

conn to-west

left=x.x.x.x #本vpn服务器的公网IP地址，如果与对端vpn服务器之间不经过nat设备，则直接写本vpn服务器的内网ip

leftid=x.x.x.x #本地网关设备的标识，本vpn服务器的内网ip

leftsubnet=192.168.0.0/24 #本vpn服务器这一侧的网段，本地端网络，0.0.0.0/0为通配，表示所有IP网段

right=y.y.y.y #对端vpn服务器的公网IP地址，不经过公网则直接写内网ip

rightid=y.y.y.y #对端VPN网关的标识，对端vpn服务器的内网ip

rightsubnet=192.168.100.0/24 #对端vpn服务器那一侧的网段

dpdaction=clear #dpd表示Dead Peer Detection，对端失效检测，clear表示对端失效时关闭连接

keyexchange=ikev1 # IPsec连接使用的IKE版本

auto=route

ike=aes128-sha256-modp2048 # IKE协议的加密算法-认证算法-DH分组

ikelifetime=86400s # IKE协议的SA生命周期

esp=aes128-sha256-modp2048 # IPsec协议的加密算法-认证算法-DH分组

lifetime=86400s #IPsec协议的SA生命周期

type=tunnel

fragmentation=yes #允许分片

**★ike及esp加密认证算法还可为：（多个值之间用逗号隔开）**

aes128-sha1-modp1024,aes128-sha1-modp2048,aes128-sha256-modp1024,aes128-sha256-modp2048,aes256-sha256-modp1024,aes256-sha256-modp2048,aes256-sha256-modp4096,aes128gcm12-aes128gcm16-aes256gcm12-aes256gcm16-modp2048-modp4096-modp1024

**★使用ssl证书认证：**

leftauth=pubkey #本地端使用公钥验证

leftcert= x.x.x.x.cert.pem #指定本地端证书

rightauth=pubkey #远程端使用公钥验证

rightcert= y.y.y.y.cert.pem #指定远程端证书

# vi /etc/strongswan/ipsec.secrets

x.x.x.x y.y.y.y : PSK passxx123

# x.x.x.x为leftid，y.y.y.y为rightid

# passxx123为IPsec连接的预共享密钥，2端的vpn服务器预共享密钥要求一致

# vi /etc/strongswan/strongswan.d/charon.conf

max\_ikev1\_exchanges = 50 #取消前面的#注释，并修改为允许建立的最大连接数，默认为最大只允许建立3条连接

**★开启系统ipv4路由转发**

# vi /etc/sysctl.conf

net.ipv4.ip\_forward=1

# echo 1 > /proc/sys/net/ipv4/ip\_forward

**★防火墙放通端口及协议报文入站**

firewall-cmd --add-port=500/udp

firewall-cmd --add-port=4500/udp

firewall-cmd --add-rich-rule='rule protocol value="esp" accept'

firewall-cmd --add-rich-rule='rule protocol value="ah" accept'

firewall-cmd --runtime-to-permanent

★启动服务

# systemctl enable strongswan

# systemctl start strongswan

# strongswan status #查看服务状态

# strongswan listcacerts #查看加载的CA证书

**第三章、OpenVPN**

在