L2tp/Ipsec

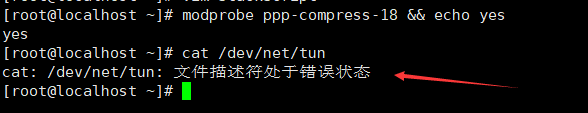
    很多时候，我们不主要是用于翻墙，而是企业内部个人用户使用，使得个人用户能使用公司网络，访问公司私有资源等。比如，一台云服务器，只允许公司网络登陆，那么通过这个vpn，就可以在家连上vpn后，使用公司网络登陆云服务器。好了，废话不多说，现在记录一下 l2tp/ipsec VPN的搭建。

1.  先看看你的主机是否支持pptp，返回结果为yes就表示通过

modprobe ppp-compress-18 && echo yes

1. 是否开启了TUN，有的虚拟机主机需要开启，返回结果为cat: /dev/net/tun: File descriptor in bad state。就表示通过。

cat /dev/net/tun



3 安装EPEL源（CentOS7官方源中已经去掉了xl2tpd）

yum install -y epel-release

4 安装xl2tpd和libreswan(openswan已经停止维护)

yum install -y xl2tpd libreswan lsof

5 编辑xl2tpd配置文件

vim /etc/xl2tpd/xl2tpd.conf

[lns default]

ip range = 10.0.0.10-10.0.0.90

local ip = 10.0.0.99

require chap = yes

refuse pap = yes

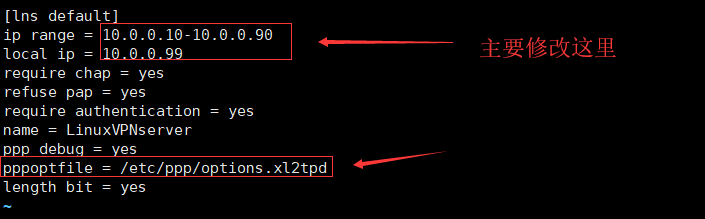
require authentication = yes

name = LinuxVPNserver

ppp debug = yes

pppoptfile = /etc/ppp/options.xl2tpd

length bit = yes



6 编辑pppoptfile文件

vim /etc/ppp/options.xl2tpd

ipcp-accept-local

ipcp-accept-remote

ms-dns 114.114.114.114

ms-dns 8.8.8.8

# ms-dns 192.168.1.1

# ms-dns 192.168.1.3

# ms-wins 192.168.1.2

# ms-wins 192.168.1.4

noccp

auth

crtscts

idle 1800

mtu 1410

mru 1410

nodefaultroute

debug

lock

proxyarp

connect-delay 5000

require-mschap-v2

persist

logfile /var/log/xl2tpd.log



7 编辑ipsec配置文件

vim /etc/ipsec.conf

config setup

protostack=netkey

dumpdir=/var/run/pluto/

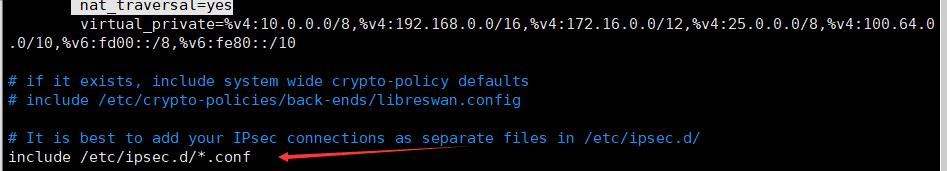
nat\_traversal=yes

virtual\_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12,%v4:25.0.0.0/8,%v4:100.64.0.0/10,%v6:fd00::/8,%v6:fe80::/10

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



8 编辑include的conf文件



vim /etc/ipsec.d/l2tp\_psk.conf # 新建如下配置文文件，直接复制的话，前面是很多空格，在启动的时候会报错，需要将空格删除，换成tab的距离，距离相同。不能用空格！

---------------------------------------------------------------------------------

conn L2TP-PSK-NAT

(tab距离)rightsubnet=0.0.0.0/0

        dpddelay=10

        dpdtimeout=20

        dpdaction=clear

        forceencaps=yes

        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=192.168.9.87    # 这个是网卡的内网IP，后面通过NAT转发

        leftprotoport=17/1701    # 端口，默认1701，不用改

        right=%any

        rightprotoport=17/%any

conn L2TP-PSK-NAT

rightsubnet=vhost:%priv

also=L2TP-PSK-noNAT

conn L2TP-PSK-noNAT

authby=secret

pfs=no

auto=add

keyingtries=3

dpddelay=30

dpdtimeout=120

dpdaction=clear

rekey=no

ikelifetime=8h

keylife=1h

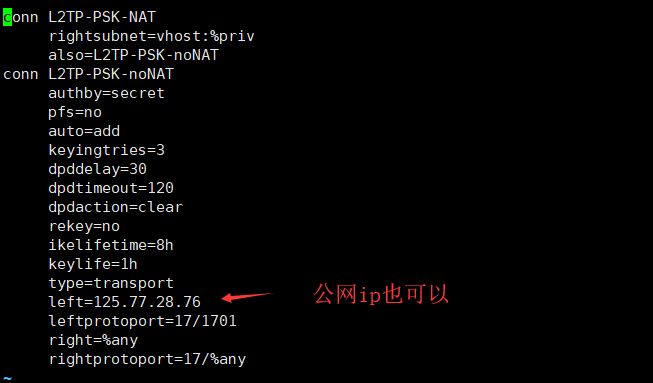
type=transport

left=125.77.28.76

leftprotoport=17/1701

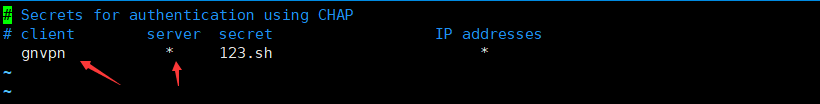
right=%any

rightprotoport=17/%any



9 设置用户名密码

vim /etc/ppp/chap-secrets



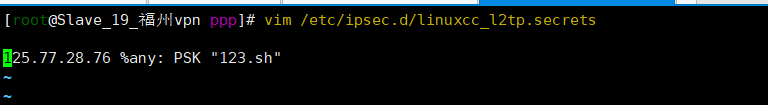
***# 格式为： 用户名  类型  密码  允许访问的ip***

***# 这个配置文件，也是pptpd的用户密码配置文件，直接类型上用\*表示所有。因为这里我们只搭建l2tp/ipsec***

10 设置预共享密钥PSK

vim /etc/ipsec.d/linuxcc\_l2tp.secrets *新建如下文件*

*125.77.28.76 %any: PSK "123.sh"*



11 CentOS7 防火墙设置

firewall-cmd --permanent --add-service=ipsec      # 放行ipsec服务，安装时会自定生成此服务

firewall-cmd --permanent --add-port=1701/udp      # xl2tp 的端口，默认1701.

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

firewall-cmd --permanent --add-masquerade      # 启用NAT转发功能。必须启用此功能

firewall-cmd --reload      # 重载配置

Iptables 配置

iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE

iptables -A INPUT -p udp -m multiport --dports 17,25,53,1701 -j ACCEPT

iptables -A INPUT -p udp -m multiport --sports 17,25,53,1701 -j ACCEPT

12 修改内核参数

vim /etc/sysctl.conf

vm.swappiness = 0

net.ipv4.neigh.default.gc\_stale\_time = 120

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

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

net.ipv4.conf.default.arp\_announce = 2

net.ipv4.conf.all.arp\_announce = 2

net.ipv4.tcp\_max\_tw\_buckets = 5000

net.ipv4.tcp\_syncookies = 1

net.ipv4.tcp\_max\_syn\_backlog = 1024

net.ipv4.tcp\_synack\_retries = 2

net.ipv4.conf.lo.arp\_announce = 2

net.ipv4.ip\_forward = 1

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

net.ipv4.conf.default.send\_red

sysctl -p

13 启动ipsec

systemctl enable ipsec     *# 设为开机启动*

systemctl restart ipsec

14 检查配置

ipsec verify     # 检查命令

# 可能会出现类似如下情况：

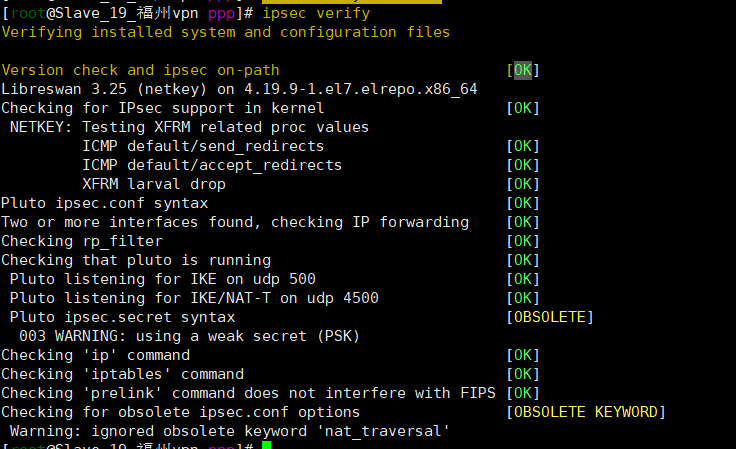
Checking rp\_filter                                  [ENABLED]

 /proc/sys/net/ipv4/conf/ens160/rp\_filter           [ENABLED]

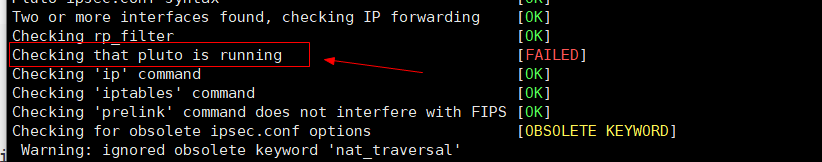
 /proc/sys/net/ipv4/conf/ens192/rp\_filter           [ENABLED]

# 这是内核参数没有生效，直接依次手动打开这些文件，将 1 改为 0

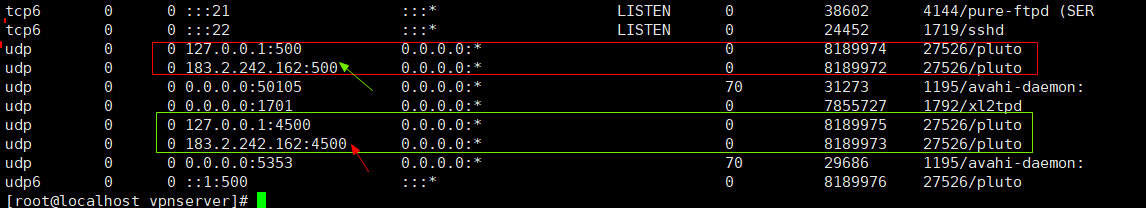
# 然后重新执行检查，输出如下内容则OK：



报这个错误，



后面发现是因为500 和4500 这两个端口被vpnserver占用了，后面把vpnserver停掉，再把ipsec重启，就可以了



15 启动xl2tp

systemctl enable xl2tpd      *# 设为开机启动*

systemctl start xl2tpd      *# 启动xl2tp*

到此，服务端的搭建已经完成，然后就是使用客户端进行连接，win10可以使用自带的vpn客户端进行连接，不需要安装任何东西。这里记录如果使用win10进行连接，如果是mac或linux系统，会有别的vpn客户端，这里暂不介绍，有兴趣的百度以下即可。

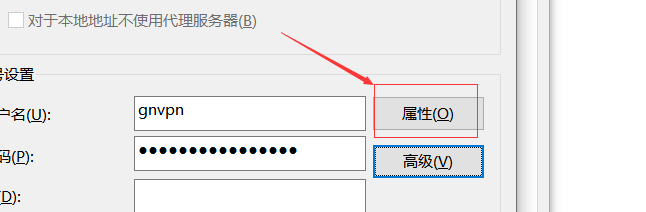
然后，使用上面自定义的用户名密码，点击连接，会很久都连接不上，然后报如下错误： L2TP连接尝试失败，因为安全层在初始化与远程计算机的协商时遇到了一个处理错误

    这是由于win10本身的问题，解决办法如下：

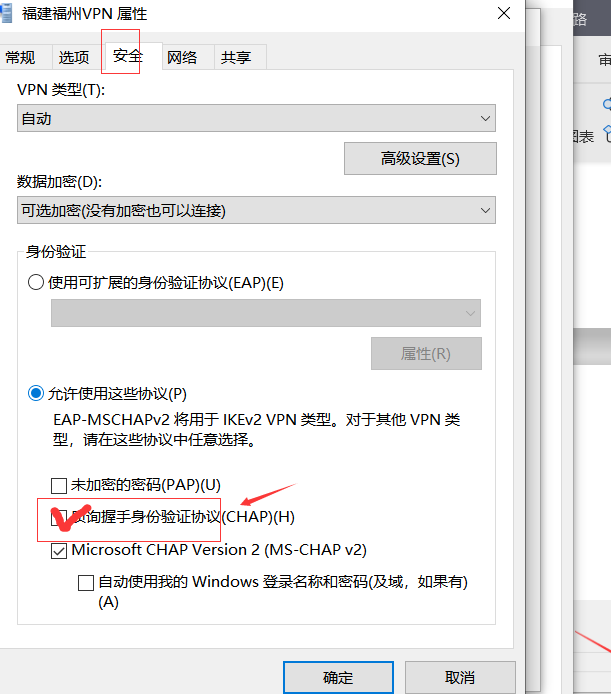
1. 首先，打开网络适配器，修改VPN连接的属性



然后点击这里



把下面指定的地方勾上



2. 查看服务状态，确保开启并设备为开机启动

windows+r 运行 输入 services.msc，查找ipsec policy agent

找到如菜单: HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

点击编辑，添加ProhibitIpSec，类型为 DWORD(32位), 必须是32位，64位不行，注意。 vlan为1

修改AllowL2TPWeakCrypto， vlan为 1.



    保存退出，重启计算机即可。然后再次连接vpn，就会发现连上了。然后试试访问内网资源，或者直接百度搜索IP，会发现自己的ip地址变成的服务端的ip地址。即可以使用此网络进行访问。