**VPN**

**简介：**

虚拟专用网络

在公用网络上建立专用私有网络,进行加密通讯

主流技术VPN技术(GRE,PPTP,L2TP+IPSec,SSL)

GRE只支持linux

GRE vpn **点对点连接**

两台linux主机都需要配置，ip地址相反

1.查看计算机当前加载的模块

lsmod                            //显示模块列表

lsmod | grep ip\_gre    //确定是否加载了gre模块

2.加载模块ip\_gre

modprobe ip\_gre

3.查看模块信息

modinfo ip\_gre

内核模块存放位置：/lib/modules/3.10.0-693.el7.x86\_64/kernel/net

4.创建VPN隧道

ip tunnel add tun0 mode gre remote 201.1.2.5 local 201.1.2.10

5.启动隧道

ip link set tun0 up

6.查看启动状况

ip link show | grep tun0

7.为VPN配置隧道ip地址

ip addr add 10.10.10.10/24 peer 10.10.10.5/24 dev tun0

**PPTP VPN** 多对一连接

**服务器：**

**1.安装软件包：**

yum localinstall pptpd-1.4.0-2.el7.x86\_64.rpm

rpm -qc pptpd

/etc/ppp/options.pptpd

/etc/pptpd.conf

/etc/sysconfig/pptpd

**2.修改配置文件**

vim /etc/prptpd.conf

# (must match the second field in /etc/ppp/chap-secrets entries)

name pptpd //18行

localip 201.1.2.5                                    //服务器本地IP

remoteip 192.168.3.1-50 //分配给客户端的IP池

vim /etc/ppp/chap-secrets            //修改账户配置文件

jacob         \*          123456     \*

//用户名    服务器标记    密码    客户端

echo "1" > /proc/sys/net/ipv4/ip\_forward    //开启路由转发

**3.翻墙设置**

iptables -t nat -A POSTROUTING -s 192.168.3.0/24

-j SNAT --to-source 201.1.2.5 //红色是vpn隧道ip 绿色是服务器的ip

**L2TP+IPSec**

装包 **IPSec //**预共享

yum -y install libreswan //ipsec的安装包

tar -xf lnmp\_soft.tar.gz

scp lnmp\_soft/vpn/myipsec.conf /etc/ipsec.d/

修改配置文件的服务器ip

vim /etc/ipsec.d/myipsec.conf

conn IDC-PSK-NAT

rightsubnet=vhost:%priv

also=IDC-PSK-noNAT

conn IDC-PSK-noNAT

authby=secret

ike=3des-sha1;modp1024

phase2alg=aes256-sha1;modp2048

pfs=no

auto=add

keyingtries=3

rekey=no

ikelifetime=8h

keylife=3h

type=transport

left=201.1.2.200 //修改ip，该ip为服务器的ip

leftprotoport=17/1701

right=%any

rightprotoport=17/%any

cat /etc/ipsec.secrets

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

vim /etc/ipsec.d/mypass.conf

201.1.2.200 %any: PSK "randpass"

systemctl start ipsec

ss -ntulp | grep pluto

查看4500和500端口是否起来了

**部署XL2TP服务**

安装xl2tpd包，在lnmp\_soft.tar.gz中有包

yum localinstall xl2tpd-1.3.8-2.el7.x86\_64.rpm

修改配置文件

vim /etc/xl2tpd/xl2tpd.conf //跳到最后，修改ip range和local ip

[lns default]

ip range = 192.168.1.128-192.168.1.254 //分配给客户端的IP池

local ip = 192.168.2.200 //VPN服务器的IP地址

require chap = yes

refuse pap = yes

require authentication = yes

name = LinuxVPNserver

ppp debug = yes

pppoptfile = /etc/ppp/options.xl2tpd

length bit = yes

vim /etc/ppp/options.xl2tpd

require-mschap-v2                               //添加一行，强制要求认证

#crtscts                                                //注释或删除该行

#lock                                                 //注释或删除该行

vim /etc/ppp/chap-secrets

xiao \* 123456 \* //账户名称 服务器标记 密码 客户端IP

启动服务

Systemctl start xl2tpd

Netstat -ntupl | grep xl2tpd // 查看启动端口 1701

**NTP** Network Time Protocol 网络时间协议

采用的是分层设计，如图-9所示，Stratum层的总数限制在15以内

rpm -qc chrony //查看配置文件所在路径

服务器设置

vim /etc/chrony

server 1.1.1.1 iburst //server用户客户端指向上层NTP服务器

allow 192.168.4.0/24                  //允许那个IP或网络访问我提供的NTP服务

deny 192.168.4.1                        //拒绝那个IP或网络访问NTP

local stratum 10                            //设置NTP服务器的层数量

润秒 //在润秒前需要把NTP服务器关掉

**PSSH远程连接工具**

并发ssh工具

使用密码批量、多并发远程其他主机

使用密钥批量、多并发远程其他主机

批量、多并发拷贝数据到其他主机

批量、多并发从其他主机下载数据到本机

批量、多并发杀死其他主机的进程

准备软件包，在lnmp\_soft.tar.gz中

rpm -ivh pssh-2.3.1-5.el7.noarch.rpm

修改/etc/hosts本地解析文件

cat /etc/hosts

192.168.2.100 host1

192.168.2.200 host2

192.168.4.100 host3

创建主机列表文件

cat /root/host.txt            //每行一个用户名、IP或域名

root@host1

host2

host3

使用密码批量、多并发远程其他主机

man pssh

pssh提供并发远程连接功能

-A                使用密码远程其他主机（默认使用密钥）

-i                 将输出显示在屏幕

-H                设置需要连接的主机

-h                设置主机列表文件

-p                设置并发数量

-t                 设置超时时间

-o dir            设置标准输出信息保存的目录

-e dir            设置错误输出信息保存的目录

-x                 传递参数给ssh //ssh的参数在引号里面

-r 递归拷贝,适用用与有目录的拷贝

ssh -o StrictHostKeyChecking=no hostIP //红色表示连接时不出现提示内容

pssh -i -A -H 'host1 host2 host3' -x '-o StrictHostKeyChecking=no' echo hello

//并发echo hello

ssh-keygen -N '' -f /root/.ssh/id\_rsa //非交互式生成密钥

ssh-copy-id host1

ssh-copy-id host2

ssh-copy-id host3 //发送ssh公钥给其它主机，下次连接不需要密码

pscp.pssh -h host.txt love.txt /tmp //并发批量拷贝给远程相同的文件

pscp.pssh -r -h host.txt /etc /tmp //如果拷贝内容有目录需要加”-r”,递归拷贝

pslurp -h host.txt /etc/hosts /host //将远程主机的/etc/hosts，拷贝到当前目录下， 存放在以host文件中主机命名的文件夹下

pslurp -h host.txt -L /media /etc/passwd /pass

//将远程主机的/etc/hosts目录，拷贝到media下，存放在对应主机名下的host文件

pnuke -h host.txt sleep