第七天 vpn服务器和NTP时间同步 pass远程套件工具

VPN（私有网络，专有网络），可以翻墙，用于公司和子公司的连接

配置GRE VPN 不支持windos，适合于linux系统，linux系统自带，不用安装 PPTP(数据不加密) L2TP+IPSec VPN （数据加密）

1. 启用GRE模块

[root@client ~]# lsmod 显示模块列表

[root@client ~]# lsmod | grep ip\_gre //确定是否加载了gre模块，没有就加载

[root@client ~]# modprobe ip\_gre

查看模块信息 root@client ~]# modinfo ip\_gre

1. 创建VPN隧道,两端都要设置隧道

[root@client ~]# ~]# ip tunnel add tun0 mode gre remote 201.1.2.5 local 201.1.2.10

Ip tunnel add 创建隧道（隧道名称为add），可以查看ip help帮助 mode 设置隧道使用gre模式 local后面根本机的ip地址，remote后面跟其他主机的ip地址

启用该隧道

[root@client ~]# ip link show

[root@client ~]# ip link set tun0 up //设置UP

[root@client ~]# ip link show

为VPN配置隧道IP地址

[root@client ~]# ip addr add 10.10.10.10/24 peer 10.10.10.5/24 dev tun0

//为隧道tun0设置本地IP地址（10.10.10.10/24）

//隧道对面的主机IP的隧道IP为10.10.10.5/24

[root@client ~]# ip a s //查看IP地址

开启路由转发

[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward

写为1.是开启路由功能，0是关闭路由功能

测试连通性

[root@client ~]# ping 10.10.10.5

[root@proxy ~]# ping 10.10.10.10

部署VPN服务器

在windows上设置ip为201.1.2.20/24，关闭防火墙， ping通proxy

1. 安装软件包

Cd /root/lnmp\_soft/vpn

[root@proxy ~]# yum localinstall pptpd-1.4.0-2.el7.x86\_64.rpm

[root@proxy ~]# rpm -qc pptpd

1. 修改配置文件

[root@proxy ~]# vim /etc/pptpd.conf

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

[root@proxy ~]# vim /etc/ppp/options.pptpd

require-mppe-128 //使用MPPE加密数据，默认有，不用添加

ms-dns 8.8.8.8 //DNS服务器

[root@proxy ~]# vim /etc/ppp/chap-secrets //修改账户配置文件

//用户名 服务器标记 密码 客户端

jacob \* 123456 \*

3.启动服务

[root@proxy ~]# systemctl start pptpd

[root@proxy ~]# systemctl enable pptpd

4.翻墙设置（非必需操作）翻墙时必须要弄

root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -j SNAT --to-source 201.1.2.5

客户端 ：启动一台windows虚拟机，配置ip，新建网络连接。输入vpn服务账户与密码，并测试

1. 创建L2TP+IPSec VPN

必须要有lnmp包

1. 安装软件包

[root@vpn ~]# yum -y install libreswan

1. 新建IPSec密钥验证配置文件

root@vpn ~]# cat /etc/ipsec.conf //仅查看一下该主配置文件,在文件的最底行

include /etc/ipsec.d/\*.conf //加载该目录下的所有配置文件行

root@vpn ~]# vim /etc/ipsec.d/myipsec.conf //新建该文件，参考lnmp\_soft/vpn/myipsec.conf

[root@client vpn]# cp myipsec.conf /etc/ipsec.d/ 复制到/etc/ipsec.d/

root@vpn ~]# vim /etc/ipsec.d/myipsec.conf

rightsubnet=vhost:%priv //允许建立的VPN虚拟网络

authby=secret //加密认证

ike=3des-sha1;modp1024 //算法

phase2alg=aes256-sha1;modp2048 //算法

left=201.1.2.200 //重要，服务器本机的外网IP

right=%any //允许任何客户端连接

right=%any //允许任何客户端连接

1. 创建IPSec预定义共享密钥

[root@vpn ~]# cat /etc/ipsec.secrets //仅查看，不要修改该文件

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

[root@vpn ~]# vim /etc/ipsec.d/mypass.secrets //新建该文件

201.1.2.200 %any: PSK "randpass" //randpass为密钥,可随便写 //201.1.2.200是VPN服务器的IP

4)启动IPSec服务

[root@vpn ~]# systemctl start ipsec

[root@vpn ~]# netstat -ntulp |grep pluto

二部署xl2tp服务

1. 安装软件包

root@vpn ~]# yum localinstall xl2tpd-1.3.8-2.el7.x86\_64.rpm

1. 修改xl2tp配置文件（修改3个配置文件的内容）

root@vpn ~]# vim /etc/ipsec.d/myipsec.conf

ip range = 192.168.3.128-192.168.root@vpn ~]# vim /etc/ppp/chap-secrets //修改密码文件

jacob \* 123456 \* //账户名称 服务器标记 密码 客户端IP3.254//分配给客户端的IP池

local ip = 201.1.2.200 自己的ip

root@vpn ~]# 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

root@vpn ~]# vim /etc/ppp/chap-secrets //修改密码文件

jacob \* 123456 \*

//账户名称 服务器标记 密码 客户端IP

1. 启动服务

[root@vpn ~]# systemctl start xl2tpd

[root@vpn ~]# netstat -ntulp |grep xl2tpd

1. 设置路由转发

[root@vpn ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward

1. 翻墙设置（非必需操作）

[root@vpn ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -j SNAT --to-source 201.1.2.200

1. NTP时间同步

Stratum层的总数限制在15以内

1. 安装软件包

[root@proxy ~]# yum -y install chrony

2)修改配置文件

[root@proxy ~]# cat /etc/chrony.conf

server 0.centos.pool.ntp.org 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NTP

#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

1. 启动NTP服务

[root@proxy ~]# systemctl restart chronyd

[root@proxy ~]# systemctl enable chronyd

配置客户端

1. 安装软件包

[root@client ~]# yum –y install chrony

1. 修改配置文件

[root@client ~]# vim /etc/chrony.conf

server 192.168.4.5 iburst //设置与哪台服务器同步数据 //iburst参数设置重启服务后尽快同步时间

3) 将客户端时间修改为错误的时间

[root@client ~]# date -s "hour:minute" //调整时间（小时：分钟）

[root@client ~]# date //查看修改后的时间

1. 重启chrony与服务器同步时间

[root@client ~]# systemctl restart chronyd

Pass远程套件工具

1. 安装软件包

[root@proxy ~]# rpm -ivh pssh-2.3.1-5.el7.noarch.rpm

1. 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

1. 创建主机列表文件

[root@proxy ~]# cat /root/host.txt

root@host1

host2

host3

使用密码批量、多并发远程其他主机

[root@proxy ~]# man pssh //通过man帮助查看工具选项的作用

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

使用密码远程多台主机执行命令，屏幕显示标准和错误输出信息

root@proxy ~]# pssh -i -A -H 'host1 host2 host3'

-x '-o StrictHostKeyChecking=no' echo hello

使用密码远程多台主机执行命令，不显示标准和错误输出信息，通过读取host.txt读取主机信息

[root@proxy ~]# pssh -A -h host.txt

-x '-o StrictHostKeyChecking=no' echo hello

使用密钥批量、多并发远程其他主机

1. 生成密钥并发送密钥到其他主机

[root@proxy ~]# ssh-keygen -N '' -f /root/.ssh/id\_rsa //非交互生成密钥文件

[root@proxy ~]# ssh-copy-id -i /root/.ssh/id\_rsa.pub host1

[root@proxy ~]# ssh-copy-id -i /root/.ssh/id\_rsa.pub host2

[root@proxy ~]# ssh-copy-id -i /root/.ssh/id\_rsa.pub host3

1. 使用密钥远程其他主机

[root@proxy ~]# pssh -h host.txt -x '-o StrictHostKeyChecking=no' echo hello

使用密钥远程其他主机，将标准输出信息写入到/tmp目录

root@proxy ~]# pssh -h host.txt -o /tmp/ -x '-o StrictHostKeyChecking=no' echo hello

批量、多并发拷贝数据到其他主机

[root@proxy ~]# man pscp.pssh //通过man帮助查看工具选项的作用

pscp.pssh提供并发拷贝文件功能

-r 递归拷贝目录

其他选项基本与pssh一致