**配置GRE VPN(翻墙)**

**启用内核模块ip\_gre**

**创建一个虚拟VPN隧道(10.10.10.0/24)**

**实现两台主机点到点的隧道通讯**

**步骤一：启用GRE模块（client和proxy都需要操作）**

**1）查看计算机当前加载的模块**

[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

**2)加载模块ip\_gre**

[root@client ~]# modprobe ip\_gre

**3）查看模块信息**

[root@client ~]# modinfo ip\_gre

**步骤二：Client主机创建VPN隧道**

**1）创建隧道**

[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tun0），ip tunnel help可以查看帮助

//mode设置隧道使用gre模式

//local后面跟本机的IP地址，remote后面是与其他主机建立隧道的对方IP地址

**2）启用该隧道（类似与设置网卡up）**

[root@client ~]# ip link show

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

[root@client ~]# ip link show

**3）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（10.10.10.10.10/24）

//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

**4）关闭防火墙**

[root@client ~]# firewall-cmd --set-default-zone=trusted

步骤三：Proxy主机创建VPN隧道

1）查看计算机当前加载的模块

[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

2)加载模块ip\_gre

[root@client ~]# modprobe ip\_gre

3）创建隧道

[root@proxy ~]# ~]# ip tunnel add tun0 mode gre \

> remote 201.1.2.10 local 201.1.2.5

//ip tunnel add创建隧道（隧道名称为tun0），ip tunnel help可以查看帮助

//mode设置隧道使用gre模式

//local后面跟本机的IP地址，remote后面是与其他主机建立隧道的对方IP地址

4）启用该隧道（类似与设置网卡up）

[root@proxy ~]# ip link show

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

[root@proxy ~]# ip link show

5）为VPN配置隧道IP地址

[root@proxy ~]# ip addr add 10.10.10.5/24 peer 10.10.10.10/24 \

> dev tun0

//为隧道tun0设置本地IP地址（10.10.10.10.5/24）

//隧道对面的主机IP的隧道IP为10.10.10.10/24

[root@proxy ~]# ip a s //查看IP地址

6）开启路由转发、关闭防火墙

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

[root@proxy ~]# firewall-cmd --set-default-zone=trusted

7)测试连通性

[root@client ~]# ping 10.10.10.5

[root@proxy ~]# ping 10.10.10.10

**创建PPTP VPN**

步骤一：部署VPN服务器

1）安装软件包（软件包参考lnmp\_soft）

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

[root@proxy ~]# rpm -qc pptpd

/etc/ppp/options.pptpd

/etc/pptpd.conf

/etc/sysconfig/pptpd

2)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

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

jacob \* 123456 \*

//用户名 服务器标记 密码 客户端

[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward //开启路由转发

3）启动服务

[root@proxy ~]# systemctl start pptpd

[root@proxy ~]# systemctl enable pptpd

[root@proxy ~]# firewall-cmd --set-default-zone=trusted

4）翻墙设置（非必需操作）

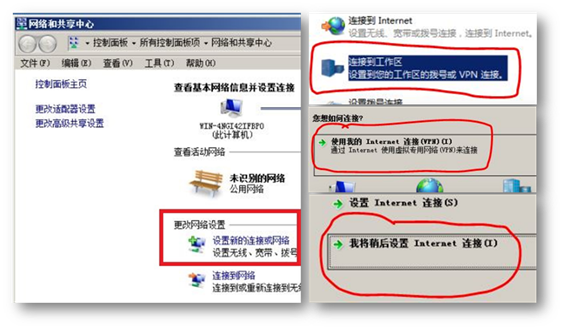
[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \

> -j SNAT --to-source 201.1.2.5

步骤二：客户端设置

启动一台Windows虚拟机，将虚拟机网卡桥接到public2，配置IP地址为201.1.2.20。

新建网络连接（具体操作如图-3所示），输入VPN服务器账户与密码（具体操作如图-4所示），连接VPN并测试网络连通性（如图-5所示）。





**创建L2TP+IPSec VPN**

步骤一：部署IPSec服务

1）安装软件包

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

2)新建IPSec密钥验证配置文件

[root@client ~]# cat /etc/ipsec.conf //仅查看一下该主配置文件

.. ..

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

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

//新建该文件，参考lnmp\_soft/vpn/myipsec.conf

[root@web1 vpn]# cp myipsec.conf /etc/ipsec.d/myipsec.conf

conn IDC-PSK-NAT

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

keyingtries=3 密钥超过三次就失败 left=201.1.2.10 //重要，服务器本机的外网IP

right=%any //允许任何客户端连接

3)创建IPSec预定义共享密钥

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

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

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

201.1.2.10 %any: PSK "randpass" #randpass为预共享密钥 #201.1.2.10是VPN服务器的IP

4)启动IPSec服务

[root@client ~]# systemctl start ipsec

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

**步骤二：部署XL2TP服务**

1）安装软件包（软件包参考lnmp\_soft）

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

2) 修改xl2tp配置文件（修改3个配置文件的内容）

[root@client ~]# vim /etc/xl2tpd/xl2tpd.conf //修改主配置文件

[global]

.. ..

[lns default]

.. ..

ip range = 192.168.3.128-192.168.3.254 //分配给客户端的IP池

local ip = 201.1.2.10 //VPN服务器的IP地址

[root@client ~]# vim /etc/ppp/options.xl2tpd //认证配置

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@client ~]# 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

3）启动服务

[root@client ~]# systemctl start xl2tpd

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

4）设置路由转发，防火墙

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

[root@client ~]# firewall-cmd --set-default-zone=trusted

5）翻墙设置（非必需操作）

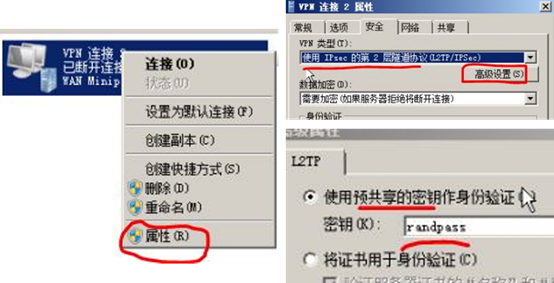
[root@client ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24

-j SNAT --to-source 201.1.2.10

步骤二：客户端设置(window10以下)

1. 新建网络连接（参考案例2），输入VPN服务器账户与密码（参考案例2）。

设置VPN连接的属性，预共享密钥是IPSec配置文件中填写的randpass，具体操作如图-7所示。



2. 设置Windows注册表（不修改注册表，连接VPN默认会报789错误），具体操作如下：

单击"开始"，单击"运行"，键入"regedit"，然后单击"确定"

找到下面的注册表子项，然后单击它：

HKEY\_LOCAL\_MACHINE\ System\CurrentControlSet\Services\Rasman\Parameters

在"编辑"菜单上，单击"新建"->"DWORD值"

在"名称"框中，键入"ProhibitIpSec"

在"数值数据"框中，键入"1"，然后单击"确定"

退出注册表编辑器，然后重新启动计算机

**NTP时间同步**

步骤一：部署NTP服务

1）安装软件包

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

[root@proxy ~]# rpm -qc chrony //查看配置文件列表

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,不能超过15层，越大校对时间越差，层数不应太大

4)启动NTP服务

[root@proxy ~]# systemctl restart chronyd

[root@proxy ~]# systemctl enable chronyd

5)设置防火墙

[root@proxy ~]# firewall-cmd --set-default-zone=trusted

步骤二：配置客户端

1）安装软件包

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

2) 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

4) 重启chrony与服务器同步时间

[root@client ~]# systemctl restart chronyd

5) 确认时间是否已经同步

[root@client ~]# date //多执行几次查看结果

**注意：时间同步机构服务器时有润妙时，一定要先关闭时间同步，否则导致服务器故障,每次重启一次chronyd就同步一次，可以做个周计划任务**

**pssh远程套件工具，批量远程控制**

**1）安装软件包，在包lnmp\_soft里面**

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

**2)修改/etc/hosts本地解析文件**

[root@proxy ~]# cat /etc/hosts

… …

192.168.2.100 host1

192.168.2.200 host2

192.168.4.10 host3

**3)创建主机列表文件**

[root@proxy ~]# cat /root/host.txt //每行一个用户名、IP或域名

… …

root@host1

host2

host3

**步骤二：使用密码批量、多并发远程其他主机**

**1）语法格式**

[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

**2)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

#另开一个终端ssh -o Str(tab) 可以出来，第一次免密，后面就不需要

**3)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 echo hello

**步骤三：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 ssh-keygen 一路回车

[root@proxy ~]# for i in 2.100 2.200 4.10

>do

>ssh-copy-id 192.168.$i

>done

#批量发送密钥到其它主机；ssh-copy-id host1 单个主机发

**2)使用密钥远程其他主机**

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

**3)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/ echo hello

**步骤四：批量、多并发拷贝数据到其他主机**

**1）语法格式**

[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

**2)将本地的/etc/hosts拷贝到远程主机的/tmp目录下**

[root@proxy ~]# pscp.pssh -h host.txt /etc/hosts / tmp

**3)递归将本地的/etc目录拷贝到远程主机的/tmp目录下**

[root@proxy ~]# pscp.pssh -r -h host.txt /etc /tmp

**步骤五：批量、多并发从其他主机下载数据到本机**

**1）语法格式**

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

#pslurp提供远程下载功能,选项与pscp.pssh基本一致

**2)将远程主机的/etc/passwd，拷贝到当前目录下，存放在对应IP下的pass文件中**

[root@proxy ~]# pslurp -h host.txt /etc/passwd /pass

**3)将远程主机的/etc/passwd目录，拷贝到media下，存放在对应IP下的pass文件**

[root@proxy ~]# pslurp -h host.txt -L /media /etc/passwd /pass

**步骤六：批量、多并发杀死其他主机的进程**

**1）语法格式**

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

#pnuke提供远程杀死进程的功能,选项与pssh基本一致

**2)将远程主机上的sleep进程杀死**

[root@proxy ~]# pnuke -h host.txt sleep

**3)将远程主机上的test相关脚本都杀死**（如：test1,testtt,test2等等）

[root@proxy ~]# pnuke -h host.txt test

**总结：建立gre VPN**

1. 加载模块 ip\_gre

modprobe ip\_gre

lsmod | grep ip\_gre #查看gre模块

modinfo ip\_gre #查看模块信息

2.创建VPN隧道

ip tunnel add tuno mode gre remote 201.1.2.5 local 201.1.2.10

#隧道名为tun0，隧道模式 gre, remote 对方ip，local 是本机ip

1. 启用该隧道

ip link set tun0 up

ip link show #显示

1. 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

#隧道tun0本机ip10.10 ; 对方隧道ip，peer 10.10.10.5

ip a s #查看IP地址；关闭防火墙

1. 建立vpn隧道对方同样加载模块

2.创建vpn隧道

ip tunnel add tun0 mode gre remote 201.1.2.10 local 201.1.2.5

#注意ip

3.启用隧道

ip link set tun0 up

4.为vpn配置ip

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

#注意ip

5.vpn服务器开启路由转发、关防火墙

echo “1” > /proc/sys/net/ipv4/ip\_forward

6.测试 看是否能ping通

**二．创建PPTP VPN,（windos）**

1）安装软件包（lnmp\_soft/vpn）

yum -y install pptpd-1.4.0-2.el7.x86\_64.rpm

1. 修改配置文件

vim /etc/pptpd.conf

localip 192.168.2.100 #服务器本地IP

remoteip 192.168.3.1-50 #分配给客户端的IP

vim /etc/ppp/options.pptpd

require-mppe-128 #使用MPPE加密数据

ms-dns 8.8.8.8 #DNS服务器

vim /etc/ppp/chap-secrets

jacob \* 123456 \*

用户名 标记 密码 客户端

1. 开启路由转发

echo “1” > /proc/net/ipv4/ip\_forward

1. 启动服务

systemctl start pptpd

systemctl enable pptpd

**客户端设置**

1. **创建L2TP+IPSec VPN**

**部署IPSec服务**

1）安装软件包

yum -y install libreswan

1. 新建IPSec密钥验证配置文件

cp myipsec.conf /etc/ipsec.d/myipsec.conf

vim /etc/ipsec.d/myipsec.conf

.......

left=201.1.2.10 #服务器本机的外网ip

right=%any #允许任何客户端连接

**3)创建IPSec预定义共享密钥**

vim /etc/ipsec.d/pass.secrets #新建改文件里面写如下内容

201.1.2.10 %any: PSK “randpass”

#randpass为预共享密钥 ip是vpn服务器的ip

**4)启动IPSec服务**

[root@client ~]# systemctl start ipsec

**步骤二：部署XL2TP服务**

1. **安装软件包（软件包参考lnmp\_soft/vpn）**

[root@client ~]# 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）

vim /etc/xl2tpd/xl2tpd.conf

ip range = 192.168.3.128-192.168.3.254 #分配给客户端的ip池

local ip = 201.1.2.10 #vpn服务器的ip

vim /etc/ppp/options.xl2tpd 认证配置

require-mschap-v2 添加一行，强制要求认证

#crtscts #lock

vim /etc/ppp/chap-secrets 修改密码文件

jacob \* 123456 \*

3）启动服务

[root@client ~]# systemctl start xl2tpd

4）设置路由转发，防火墙

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

[root@client ~]# firewall-cmd --set-default-zone=trusted

**客户端设置**