VPN

vpn:虚拟专用网络(VPN)的功能是：在[公用网络](https://baike.baidu.com/item/%E5%85%AC%E7%94%A8%E7%BD%91%E7%BB%9C/12752077" \t "/home/student/文档\\x/_blank)上建立[专用网络](https://baike.baidu.com/item/%E4%B8%93%E7%94%A8%E7%BD%91%E7%BB%9C/795899" \t "/home/student/文档\\x/_blank)，进行[加密](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86/752748" \t "/home/student/文档\\x/_blank)通讯。

在[企业网络](https://baike.baidu.com/item/%E4%BC%81%E4%B8%9A%E7%BD%91%E7%BB%9C/2119389" \t "/home/student/文档\\x/_blank)中有广泛应用。[VPN](https://baike.baidu.com/item/VPN" \t "/home/student/文档\\x/_blank)网关通过对[数据包](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85/489739" \t "/home/student/文档\\x/_blank)的加密和数据包目标地址的转换

实现[远程访问](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E8%AE%BF%E9%97%AE/3326708" \t "/home/student/文档\\x/_blank)。VPN可通过[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571" \t "/home/student/文档\\x/_blank)、硬件、软件等多种方式实现

案例1:配置GRE VPN

1.1问题

本案例要求搭建一个GRE VPN环境,并测试该VPN网络是否能正常通讯,要不如下:

\*启用内核模块ip\_gre

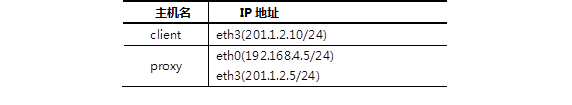
\*创建一个虚拟VPN隧道

\*实现两台主机点到点的隧道通讯

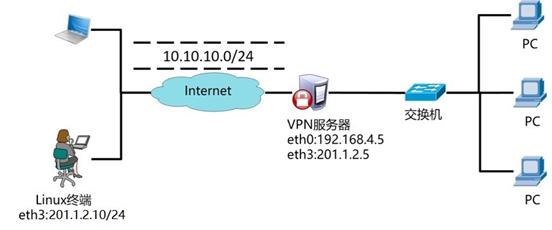
1.2方案

使用lsmod查看当前计算机已经加载的模块,使用modprdobe加载Linux内核模块,使用modinfo可以查看内核模块的信息

准备实验所需的虚拟机环境,实验环境所需要的主机及对应的IP设置列表如下,正确配置IP地址,主句名称,并且为每台主句配置yum源



实验拓扑如图所示



1.3步骤

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]加载模块信息

[root@client ~]# modinfo ip\_gre

filename: /lib/modules/3.10.0-693.el7.x86\_64/kernel/net/ipv4/ip\_gre.ko.xz

alias: netdev-gretap0

alias: netdev-gre0

alias: rtnl-link-gretap

alias: rtnl-link-gre

license: GPL

rhelversion: 7.4

srcversion: F37A2BF90692F86E3A8BD15

depends: ip\_tunnel,gre

intree: Y

vermagic: 3.10.0-693.el7.x86\_64 SMP mod\_unload modversions

signer: CentOS Linux kernel signing key

sig\_key: DA:18:7D:CA:7D:BE:53:AB:05:BD:13:BD:0C:4E:21:F4:22:B6:A4:9C

sig\_hashalgo: sha256

parm: log\_ecn\_error:Log packets received with corrupted ECN (bool)

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]启用盖隧道(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

]#lsmod

]#lsmod |grep ip\_gre

[2]加载模块ip\_gre

]#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

[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

[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward //开启路由转发功能[必须用重定向编辑]

[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

案例2:创建PPTP VPN

2.1问题

本案例要求搭建一个PPTP VPN环境，并测试该VPN网络是否能够正常通讯，要求如下:

使用PPTP协议创建一个支持身份验证的隧道连接

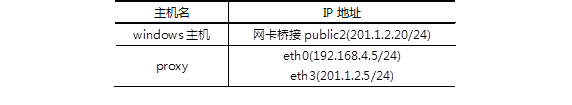
使用MPPE对数据进行加密

为客户端分配192.168.3.0/24的地址池

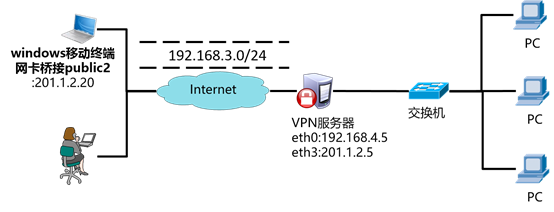
客户端连接的用户名为jacob，密码为123456

2.2方案

准备实验所需的虚拟机环境，实验环境所需要的主机及对应的IP设置列表如表-2所示，正确配置IP地址、主机名称，并且为每台主机配置YUM源.



实验拓扑图



2.3步骤

实现此案例需要按照如下步骤进行

步骤一:部署VPN服务器

[1]安装软件(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(非必要操作)

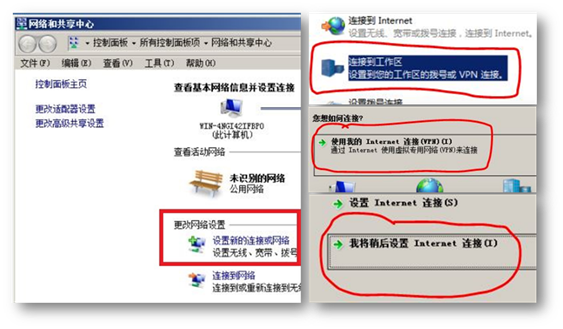
[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \

> -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）。





C:/Users/Jacob>ping 201.1.2.5

C:/Users/Jacob>ping 192.168.4.5

案例3创建L2TP+IPSecVPN

3.1问题

本案例要求搭建一个L2TP+IPSec VPN环境，并测试该VPN网络是否能够正常通讯，具体要求如下：

使用L2TP协议创建一个支持身份验证与加密的隧道连接

使用IPSec对数据进行加密

为客户端分配192.168.3.0/24的地址池

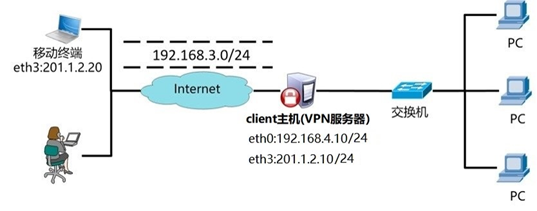
客户端连接的用户名为：jacob，密码为：123456

预共享密钥为：randpass

3.2方案

准备实验所需的虚拟机环境，实验环境所需要的主机及对应的IP设置列表如表-3所示，正确配置IP地址、主机名称，并且为每台主机配置YUM源。





3.3步骤

步骤一:部署IPSec服务

[1]安装软件包

]#yum -y install libreswan

[2]新建IPSec秘钥验证配置文件

[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](mailto:root@client) ~]# vim /etc/ipsec.d/myipsec.conf

//新建该文件，参考lnmp\_soft/vpn/myipsec.conf

conn IDC-PSK-NAT

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

also=IDC-PSK-noNAT

conn IDC-PSK-noNAT

authby=secret                                    //加密认证

ike=3des-sha1;modp1024                        //算法

phase2alg=aes256-sha1;modp2048                //算法

pfs=no

auto=add

keyingtries=3

rekey=no

ikelifetime=8h

keylife=3h

type=transport

left=201.1.2.10                                //重要，服务器本机的外网IP

leftprotoport=17/1701

right=%any                                    //允许任何客户端连接

rightprotoport=17/%any

[3]创建IPSec预定义共享秘钥

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

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

[[root@client](mailto: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IPSce服务

[root@client ~]# systemctl start ipsec

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

udp 0 0 127.0.0.1:4500 0.0.0.0:\* 3148/pluto

udp 0 0 192.168.4.10:4500 0.0.0.0:\* 3148/pluto

udp 0 0 201.1.2.10:4500 0.0.0.0:\* 3148/pluto

udp 0 0 127.0.0.1:500 0.0.0.0:\* 3148/pluto

udp 0 0 192.168.4.10:500 0.0.0.0:\* 3148/pluto

udp 0 0 201.1.2.10:500 0.0.0.0:\* 3148/pluto

udp6 0 0 ::1:500 :::\* 3148/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

]#systemctl start xl2tpd

]#netstat -nutpl | 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

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

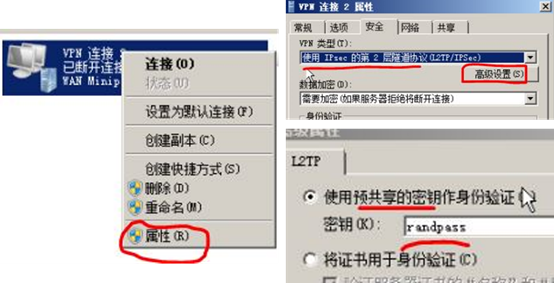
> -j SNAT --to-source 201.1.2.10

步骤三: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。

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

\*连接VPN并测试网络连通性（参考案例2）。

案例4:NTP时间同步

4.1问题

本案例要求搭建一个NTP服务器，为整个网络环境中的所有主机提供时间校准服务，具体要求如下：

部署一台NTP时间服务器

设置时间服务器上层与0.centos.pool.ntp.org同步

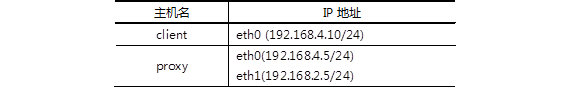
设置本地服务器层级数量为10

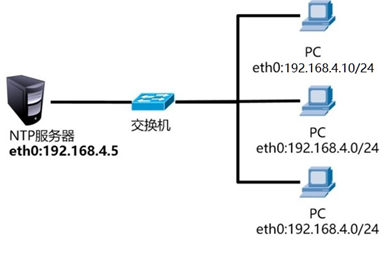
许192.168.4.0/24网络的主机同步时间

客户端验证时间是否同步

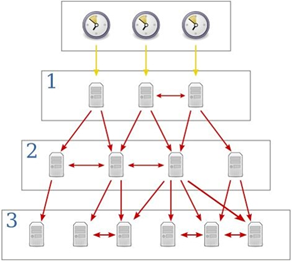
4.2方案

准备实验所需的虚拟机环境，实验环境所需要的主机及对应的IP设置列表如表-4所示，正确配置IP地址、主机名称，并且为每台主机配置YUM源。





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（包括15）。



4.3步骤

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

/etc/chrony.conf

/etc/chrony.keys

.. ..

[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

.. ..

[3]启动服务

[root@proxy ~]# systemctl restart chronyd

[root@proxy ~]# systemctl enable chronyd

[4]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