**6\_Operation07VPN和NTP**

**一 VNP**

**1.1 VPN**:Virtual Private Network

1.1.1**在公共网络的基础上建立专用私有网络,进行加密通讯**

多用于为集团公司的各地子公司建立连接

连接完成后,各个地区的子公司可以想局域网一样通讯

在企业网络中有广泛的应用

偶尔可以用于翻墙

1.1.2目前主流的VPN技术:GRE,PPTP,L2TP+IPSec,SSL

搭建难度从左到右依次增加,安全性从左到右依次增加

lsmod 查看内核激活的功能

lsmod | wc -l 统计内核激活的程序数

modprobe ip\_gre 内核激活ip\_gre

rmmod 程序名 关闭激活的程序

lsmod | grep pre

modinfo ip\_gre

**1.2案例：配置GRE VPN**

要求:

搭建一个GRE VPN环境，并测试该VPN网络是否能够正常通讯，要求如下：

启用内核模块ip\_gre

创建一个虚拟VPN隧道(10.10.10.0/24)

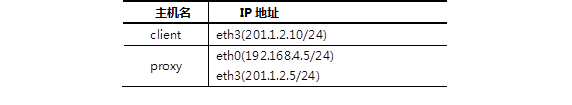
实现两台主机点到点的隧道通讯

方案:

使用lsmod查看当前计算机已经加载的模块，使用modprobe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设置列表如表-1所示，正确配置IP地址、主机名称，并且为每台主机配置YUM源。

表－1 主机列表



实验拓扑如图-1所示。

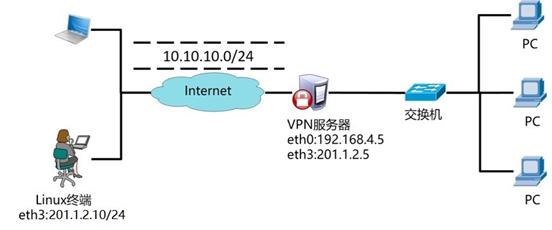


图-1

**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

client ~]# **lsmod** #示模块列表

client ~]# **lsmod | grep ip\_gre** #确定是否加载了gre模块

2)加载模块ip\_gre

client ~]# **modprobe ip\_gre**

3）查看模块信息

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**

**ip 命令帮助**

**ip help;ip tunnel help;等**

1）创建隧道

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后为本机的IP地址，remote后为与本机建立隧道的对方主机的IP地址

2）启用该隧道（类似与设置网卡up）

client ~]# ip link show

client ~]# **ip link set tun0 up** #启用隧道tun0

client ~]# **ip link show(ip a s)**

3）为VPN配置隧道IP地址

client ~]# **ip addr add 10.10.10.10/24 peer 10.10.10.5/24 \**

**> dev tun0**

#为隧道tun0设置本机隧道IP地址为:10.10.10.10/24

#为隧道tun0对面主机隧道IP地址为:10.10.10.5/24

client ~]# ip a s #查看IP地址

4）关闭防火墙

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

client ~]# **lsmod**  #显示模块列表

client ~]# **lsmod | grep ip\_gre** #确定是否加载了gre模块

2)加载模块ip\_gre

client ~]# **modprobe ip\_gre**

3）创建隧道

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后为本机的IP地址，remote后为与本机建立隧道的对方主机的IP地址

4）启用该隧道（类似与设置网卡up）

proxy ~]# ip link show

proxy ~]# **ip link set tun0 up**         #启用隧道tun0

proxy ~]# **ip link show**

5）为VPN配置隧道IP地址

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

proxy ~]# ip a s #查看IP地址

6）开启路由转发、关闭防火墙

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

**#只能用重echo+重定向修改值为0或1;中继的主机必须开启此设置,作为软路由,连接公网,并在软路由上设置网络地址转换(NAT)[实验中proxy为中继的主机]**

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

7)测试连通性

client ~]# ping 10.10.10.5

proxy ~]# ping 10.10.10.10

**1.3 案例：创建PPTP VPN**

1.3.1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

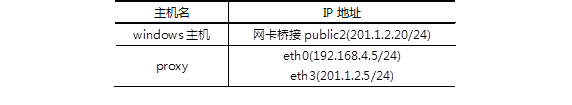
为客户端分配192.168.3.0/24的地址池

客户端连接的用户名为jacob，密码为123456

1.3.2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-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。

表－2 主机列表



实验拓扑如图-2所示。

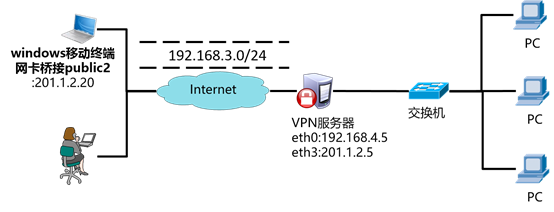


图-2

1.3.3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）安装软件包（软件包参考lnmp\_soft）**

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

proxy ~]# rpm -qc pptpd

**/etc/ppp/options.pptpd**

**/etc/pptpd.conf**

/etc/sysconfig/pptpd

**2)修改配置文件(设置 IP地址池\加密和DNS)**

proxy ~]# vim **/etc/pptpd.conf #设置IP地址池**

**最后2行,解除注释并修改**

localip 201.1.2.5 #服务器本地IP

remoteip 192.168.3.1-50,192.168.3.100-150

#分配给客户端的IP池(VPN的IP地址池),多段ip用,号分隔

proxy ~]# vim **/etc/ppp/options.pptpd #设置加密和DNS**

require-mppe-128 #使用MPPE加密数据

ms-dns 8.8.8.8 #设置DNS服务器,给客户机域名解析使用

proxy ~]# vim **/etc/ppp/chap-secrets** **#修改配置文件设置账户和密码**

jacob \* 123456 \*

用户名 服务器标记 密码 客户端

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

#开启路由转发

**3）启动服务**

proxy ~]# systemctl start **pptpd**

proxy ~]# systemctl enable pptpd

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

**4）翻墙设置（非必需操作）**

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）。

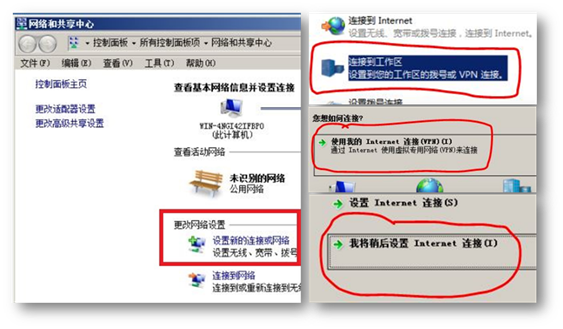


图-3



图-4

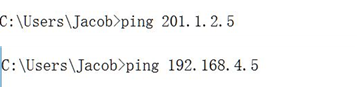


图-5

**1.4案例:创建L2TP+IPSec VPN**

1.4.1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 PSK:PRE SHARED KEY

1.4.2 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-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。

表－3 主机列表



实验拓扑如图-6所示。

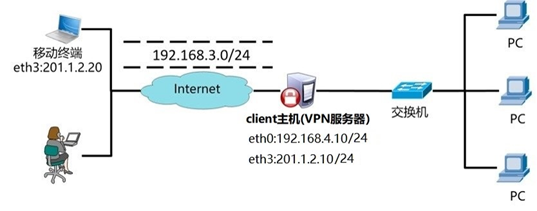


图-6

**1.4.3步骤**

**步骤一：部署IPSec服务**

**1）安装软件包**

client ~]# yum -y install libreswan

**2)新建IPSec密钥验证配置文件**(lnmp/php内myipsec.conf)

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**

**#新建该文件并修改，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预定义共享密钥**

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

include **/etc/ipsec.d/\*.secrets #预共享秘钥的存放路径和命名方式**

[[root@client](mailto:root@client) ~]# **vim /etc/ipsec.d/mypass.secrets**

**#创建预定义共享密钥并修改**

**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**

client ~]# systemctl start ipsec

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/php）**

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）**

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**

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** **#修改用户和密码文件**

jacob \* 123456 \*

#账户名称 服务器标记 密码 客户端IP

**3）启动服务**

client ~]# systemctl start xl2tpd

client ~]# netstat -ntulp |grep xl2tpd

udp 0 0 0.0.0.0:1701 0.0.0.0:\* 3580/xl2tpd

**4）设置路由转发，防火墙**

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

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

**5）翻墙设置（非必需操作）**

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。

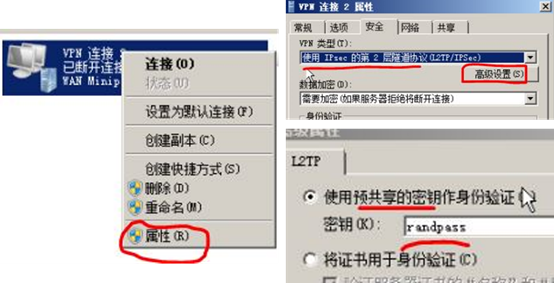


图-7

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）。

**二 案例：NTP时间同步**

**2.1 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

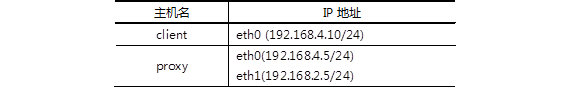
允许192.168.4.0/24网络的主机同步时间

客户端验证时间是否同步

**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-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。

表－4 主机列表



实验拓扑如图-8所示。

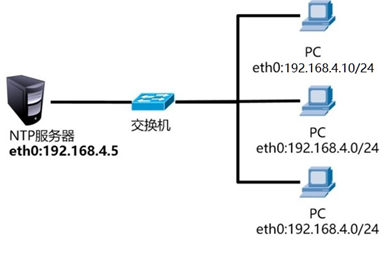
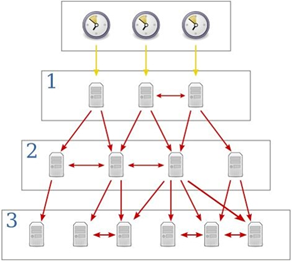


图-8

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）**。

图-9

**2.3 步骤**

**步骤一：部署NTP服务**

**1）安装软件包**

proxy ~]# **yum -y install chrony**

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**

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**

**#解除注释,激活本机为时间服务器;允许哪个IP或网络访问NTP**

**#deny 192.168.4.1 #拒绝哪个IP或网络访问NTP**

**local stratum 10 #解除注释;设置NTP服务器的层数量**

.. ..

**3)启动NTP服务**

proxy ~]# systemctl restart chronyd

proxy ~]# systemctl enable chronyd

**4)设置防火墙**

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

**步骤二：配置客户端**

**1）安装软件包**

client ~]# **yum -y install chrony**

**2) 修改配置文件**

client ~]# vim **/etc/chrony.conf**

**server 192.168.4.5**

#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**

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

client ~]# date #查看修改后的时间

**4) 重启chrony与服务器同步时间**

client ~]# systemctl restart chronyd

**5) 确认时间是否已经同步**

client ~]# date #多执行几次查看结果