**VPN**

**Virtual Private Natwork (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

-多用于为集团公司的各地子公司建立连接

-连接完成后 各地区的子公司可以像局域网一样通讯

-在企业中有广泛应用

-偶尔可以用于翻墙

目前主流的vpn技术（GPE PPTP L2TP+IPSec SSL）

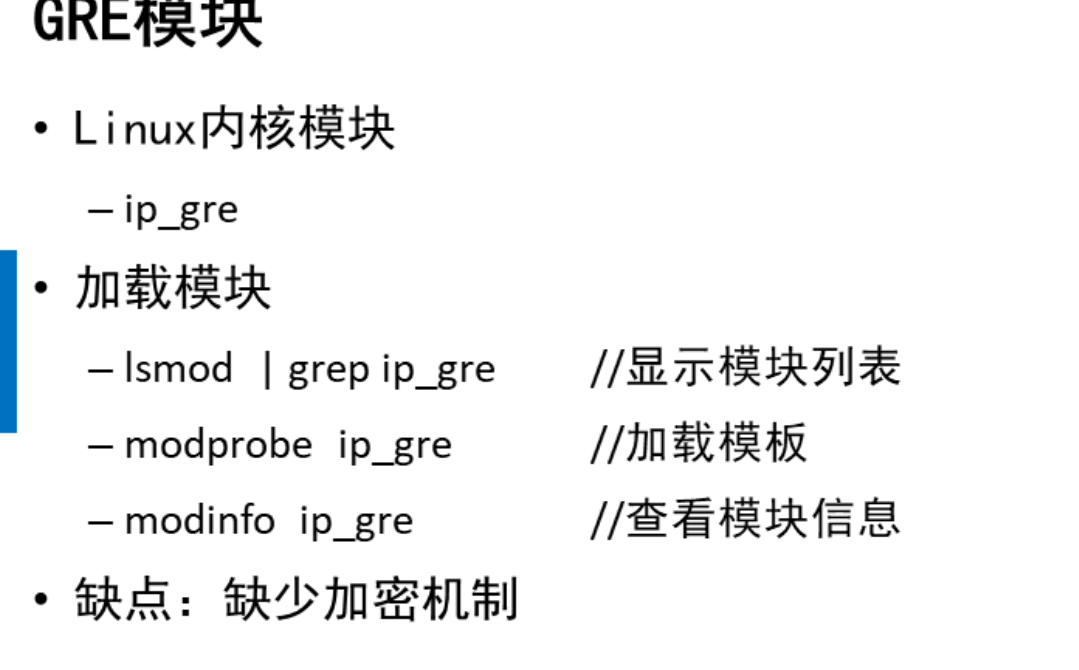
**配置GRE VPN**

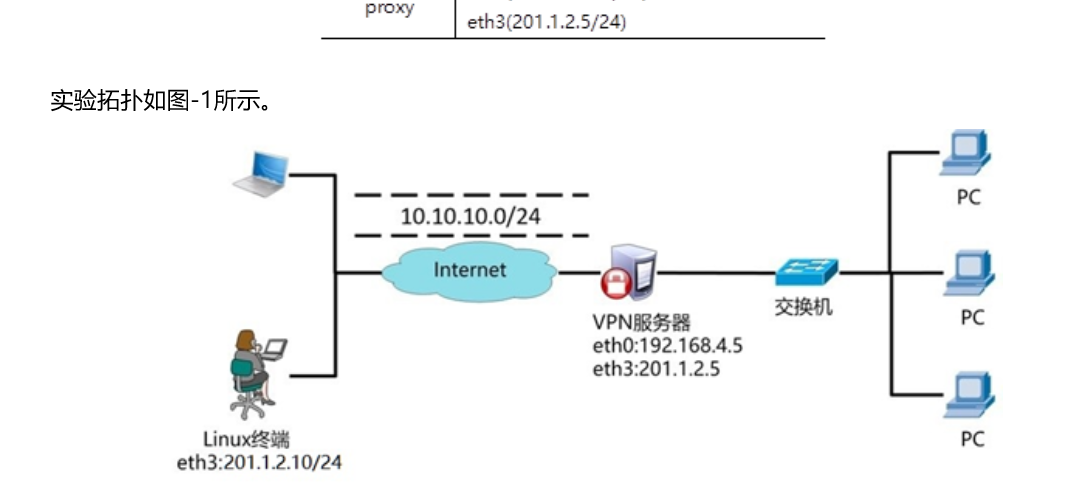
* 启用内核模块ip\_gre
* 创建一个虚拟VPN隧道(10.10.10.0/24)
* 实现两台主机点到点的隧道通讯

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。

**实现此案例需要按照如下步骤进行**





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

1. [root@client ~]# modinfo ip\_gre
2. filename: /lib/modules/3.10.0-693.el7.x86\_64/kernel/net/ipv4/ip\_gre.ko.xz
3. … …

**步骤二：Client主机创建VPN隧道**

1）创建隧道

1. [root@client ~]# ip tunnel add tun0 mode gre \
2. > 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

**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 a s

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

[root@proxy ~]# ip a s

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)测试连通性

[root@client ~]# ping 10.10.10.5

[root@proxy ~]# ping 10.10.10.10

**创建PPTP VPN**

* 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

实现此案例需要按照如下步骤进行

1）安装软件包（软件包参考lnmp\_soft/vpn/）

* [root@proxy ~]# yum install 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     服务器名称    密码     客户端IP

3）启动服务

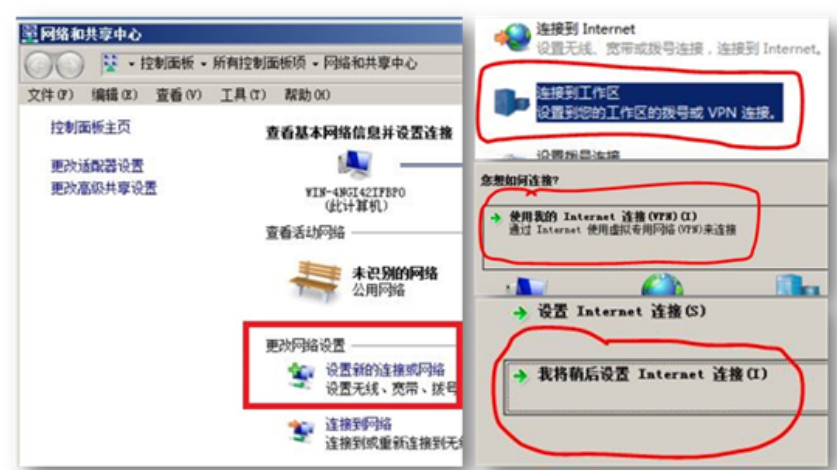
* [root@proxy ~]# systemctl start pptpd
* [root@proxy ~]# systemctl enable pptpd

4）翻墙设置（非必需操作）

1. [root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward    *//开启路由转发*
3. [root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \
4. > -j SNAT --to-source 201.1.2.5

**步骤二：客户端设置**

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**

* 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

实现此案例需要按照如下步骤进行

1）安装软件包

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

2)新建IPSec密钥验证配置文件

1. [root@client ~]# cat /etc/ipsec.conf                //仅查看一下该主配置文件
2. .. ..
3. include /etc/ipsec.d/\*.conf                    //加载该目录下的所有配置文件
5. [[root@client](mailto:root@client) ~]# vim /etc/ipsec.d/myipsec.conf
6. //新建该文件，参考lnmp\_soft/vpn/myipsec.conf
7. conn IDC-PSK-NAT
8. rightsubnet=vhost:%priv
9. also=IDC-PSK-noNAT
11. conn IDC-PSK-noNAT
12. authby=secret                                    //加密认证
13. ike=3des-sha1;modp1024                        //加密算法
14. phase2alg=aes256-sha1;modp2048                //加密算法
15. pfs=no
16. auto=add
17. keyingtries=3
18. rekey=no
19. ikelifetime=8h
20. keylife=3h
21. type=transport
22. left=201.1.2.10                                //重要，服务器本机的外网IP
23. leftprotoport=17/1701
24. right=%any                                    //允许任何客户端连接
25. rightprotoport=17/%any

3)创建IPSec预定义共享密钥

1. [root@client ~]# vim /etc/ipsec.secrets                 //修改该文件
2. include /etc/ipsec.d/\*.secrets
3. 201.1.2.10 %any: PSK "randpass"              //randpass为预共享密钥
5. //201.1.2.10是VPN服务器的IP
6. //%any:任何客户端都可以连接服务器
7. //PSK（pre share key）中文预共享密钥

4)启动IPSec服务

1. [root@client ~]# systemctl start ipsec
2. [root@client ~]# netstat -ntulp |grep 500
3. udp 0 0 127.0.0.1:4500 0.0.0.0:\* 3148/pluto
4. udp 0 0 192.168.4.10:4500 0.0.0.0:\* 3148/pluto
5. udp 0 0 201.1.2.10:4500 0.0.0.0:\* 3148/pluto
6. udp 0 0 127.0.0.1:500 0.0.0.0:\* 3148/pluto
7. udp 0 0 192.168.4.10:500 0.0.0.0:\* 3148/pluto
8. udp 0 0 201.1.2.10:500 0.0.0.0:\* 3148/pluto
9. 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/vpn/）

1. [root@client ~]# yum install 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）

1. [root@client ~]# vim /etc/xl2tpd/xl2tpd.conf                //修改主配置文件
2. [global]
3. .. ..
4. [lns default]
5. .. ..
6. ip range = 192.168.3.128-192.168.3.254                    //分配给客户端的IP池
7. local ip = 201.1.2.10                                 //VPN服务器的IP地址
9. [root@client ~]# vim /etc/ppp/options.xl2tpd            //认证配置
10. require-mschap-v2                                         //添加一行，强制要求认证
11. #crtscts                                                //注释或删除该行
12. #lock                                                //注释或删除该行
14. root@client ~]# vim /etc/ppp/chap-secrets                    //修改密码文件
15. jacob \* 123456 \*                //账户名称 服务器名称 密码 客户端IP

3）启动服务

1. [root@client ~]# systemctl start xl2tpd
2. [root@client ~]# ss -ntulp |grep xl2tpd
3. udp 0 0 0.0.0.0:1701 0.0.0.0:\* 3580/xl2tpd

4）翻墙设置（非必需操作）

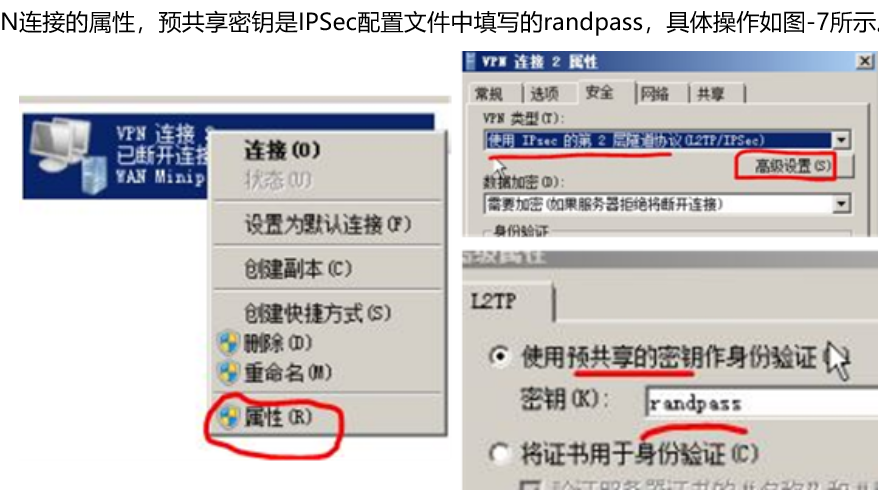
1. [root@client ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward #开启路由转发
2. [root@client ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \
3. > -j SNAT --to-source 201.1.2.10

**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）。