**Morning：**

1. VPN概述

VPN（Virtual Private Network）：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

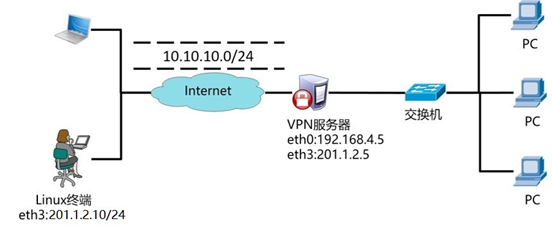
-连接完成后，各个地区的子公司可以像局域网一样通讯

-偶尔可以用于翻墙

-主流VPN技术（GRE，PPTP，L2TP+IPSec，客户端不需装软件）

1. 配置GRE VPN

**-实验拓扑+原理**



原理： tun0 --- eth3 -------------> eth3 --- tun0（将封装的包在公网传输）

**步骤1：Client主机启动GRE模块**

1）查看计算机当前加载的模块

[root@client ~]# lsmod #显示所有模块列表

[root@client ~]# lsmod | grep ip\_gre #查看gre是否加载

2）加载ip\_gre

[root@client ~]# modprobe ip\_gre

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

#所有模块的路径：/lib/modules/3.10.0-693.el7.x86\_64/kernel/，包括驱动及各种内核模块

**步骤2：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

#创建隧道名称为tun0，使用gre模式，对方IP 2.5，本机IP 2.10

2）启用该隧道，为VPN配置隧道IP地址

[root@client ~]# ip link set tun0 up #启动tun0

[root@client ~]# ip link show

[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，对面的主机IP为10.5

[root@client ~]# ip a s #查看IP地址

1. 关闭防火墙

**步骤3：Proxy主机创建VPN隧道**

1～5）重复步骤1、步骤2（IP地址相反）

6）开启路由转发、关闭防火墙（默认已设置）

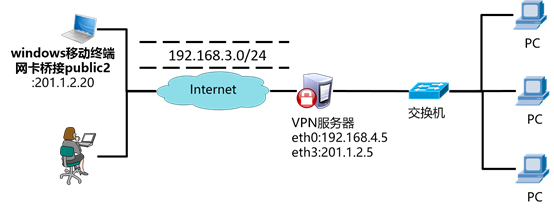
[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip\_forward

7）测试连通性

[root@proxy ~]# ping 10.10.10.10

3、创建PPTP VPN

**-实验拓扑**



**步骤1：部署VPN服务器**

1）安装软件包

[root@proxy vpn]# yum -y install pptpd-1.4.0-2.el7.x86\_64.rpm

#软件包放在lnmp\_soft/vpn/里

[root@proxy ~]# rpm -qc pptpd #-c只显示配置文件

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 #分配给客户端的隧道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 #账户配置文件

jacob \* 123456 \*

#用户名 服务器标记(在./options.pptpd指出) 密码 客户端

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

#默认已设置

1. 启动服务

[root@proxy ~]# systemctl start pptpd

[root@proxy ~]# systemctl enable pptpd

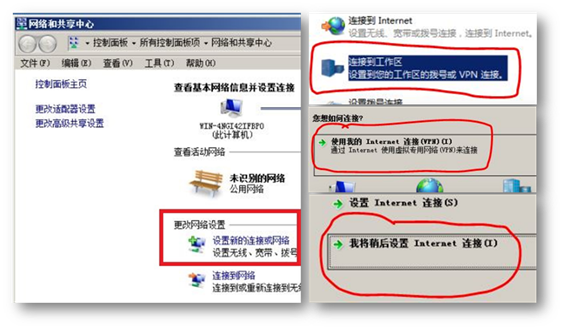
4）翻墙设置（非必需操作）

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

#让私网IP变成公网IP（NAT）

**步骤2：客户端设置**

1）在Windows主机设置新的Internet连接



2）输入服务器地址，用户名及密码



1. 打开“更改适配器配置”，完成拨号
2. 进行网络连通测试

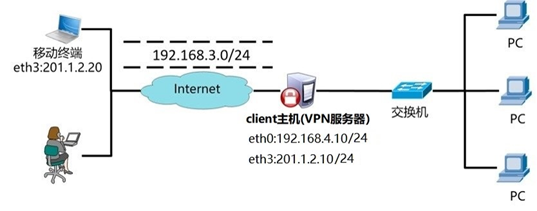
ping 201.1.2.5

ping 192.168.4.5

**Afternoon：**

1、创建L2TP+IPSec VPN

**-实验拓扑**



**步骤1：部署IPSec服务（数据加密）**

1）安装软件包（默认已装）

[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 ~]# cp lnmp/vpn/myi..conf /etc/ipsec.d/myipsec.conf

#从lnmp包中拷贝IPSec密钥验证配置文件

authby=secret #加密认证

ike=3des-sha1;modp1024 #算法

phase2alg=aes256-sha1;modp2048 #算法

left=201.1.2.10 #重要，服务器本机的外网IP

3）创建IPSec预定义共享密钥

[root@client ~]# cat /etc/ipsec.secrets #仅查看，不需修改

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

[root@client ~]# vim /etc/ipsec.d/mypass.secrets

201.1.2.10 %any: PSK "randpass"

#定义VPN服务器的IP，PSK定义预共享密钥，any允许所有用户

4）启动IPSec服务

[root@client ~]# systemctl start ipsec

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

**步骤2：部署XL2TP服务（VPN隧道）**

1. 安装软件包

[root@client vpn]# yum -y install xl2tpd-1.3.8-2.el7.x86\_64.rpm

2）修改xl2tp配置文件

[root@client ~]# vim /etc/xl2tpd/xl2tpd.conf

ip range = 192.168.3.128-192.168.3.254 #客户端IP池

local ip = 201.1.2.10 #VPN服务器IP

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

require-mschap-v2 #取消注释，强制要求认证

#crtscts #注释该行，否则影响Windows拨号

#lock #注释该行，否则影响Windows拨号

[root@client ~]# vim /etc/ppp/chap-secrets

gjq \* 123456 \*

#账户名称 服务器标记 密码 客户端IP

1. 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

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

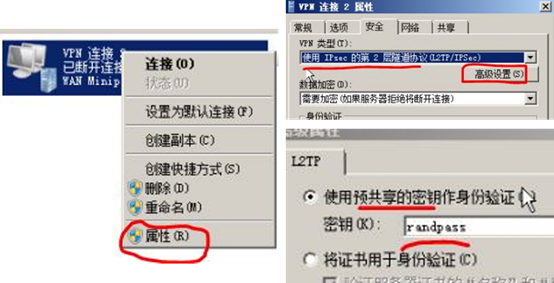
#让私网IP变成公网IP（NAT）

**步骤3：客户端设置**

1. 新建网络连接

参考：Morning --> 3、创建PPTP VPN --> 步骤2：客户端设置

2）选择VPN类型（Win10不需要）



3）设置Windows注册表（否则报789错误）

-Win+R，输入”regedit”；

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

-右击新建>“DWORD值”

-名称改为”ProhibitIpSec”，数值数据改为1

-退出注册表编辑器，重启计算机

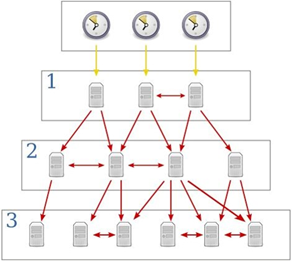
4）拨号连接VPN，测试网络连通性

**-查看VPN服务器日志**

[root@client ~]# tailf /var/log/messages

2、搭建NTP时间同步

**-NTP(网络时间协议)的分层设计**



Stratum层的总数规定不超过15层

**步骤1：部署NTP服务**

1. 安装软件包chrony
2. 修改主配置文件

[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IP或网络访问NTP

#deny 192.168.4.1 #拒绝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、开机自启
2. 设置防火墙

**步骤2：配置客户端**

1. 装包、配置、起服务

参考：阶段1 --> 1.ADMIN --> Day05 --> Page3

1. 测试时间同步

[root@client ~]# date -s "2000-01-01 11:11:11" #修改时间

[root@client ~]# systemctl restart chronyd #重启服务

[root@client ~]# date #时间同步

1. 注意：闰秒前必须把NTP关掉。

3、pssh远程套件工具

**步骤1：准备工作**

1）安装软件包

[root@proxy lnmp\_soft]# 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 #不写用户名默认为root

host3

**步骤2：使用密码并发远程其他主机**

1. pssh语法格式

[root@proxy ~]# man 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（一次连接数）

-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 将ssh支持的参数传递给pssh

2）使用密码远程多台主机执行命令，屏幕显示输出信息

[root@proxy ~]# pssh -i -A -H 'host1 host2 host3' -x '-o StrictHostKeyChecking=no' echo hello

#只有首次连接需要-x ‘-o StrictHostKeyChecking=no’

3）通过读取host.txt读取主机信息

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

**步骤3：使用密钥并发远程其他主机**

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

#非交互式生成密钥文件

[root@proxy ~]# for i in host1 host2 host3; do ssh-copy-id $i; done

2）使用密钥远程其他主机

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

3）将标准输出写入到/tmp目录

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

#自动将输出文件命名为主机列表名

**步骤4：并发拷贝数据到其他主机**

1. pscp.pssh语法格式

[root@proxy ~]# man pscp.pssh

#提供并发拷贝文件功能，选项基本与pssh一致

-r 递归拷贝目录

1. 拷贝本地文件到远程主机目录/下

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

1. 递归将本地目录拷贝到远程主机目录/tmp

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

**步骤5：并发从其他主机下载数据到本机**

1）pslurp语法格式

[root@proxy ~]# man pslurp

#提供远程下载功能，选项与pscp.pssh基本一致

1. 将远程主机的文件，拷贝到当前目录下，改名为pass

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

#自动在当前按主机列表名创建目录，并把拷贝文件分别放在里面

3）将远程主机的/etc/passwd目录，拷贝到media下

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

**步骤6：并发杀死其他主机的进程**

1）pnuke语法格式

[root@proxy ~]# man 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

4）将远程主机上的test.sh脚本杀死

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