构建不同类型的VPN

1、GRE模式

环境：centos7.4虚拟机2台，关闭防火墙，SELinux，配置好yum源，清空iptables规则

规划：client eth1 201.0.1.1

Proxy eth0 192.168.4.2

Eth1 201.0.1.2

[root@client ~]# lsmod | grep ip\_gre

[root@client ~]# modprobe ip\_gre

[root@client ~]# lsmod | grep ip\_gre

ip\_gre 22707 0

ip\_tunnel 25163 1 ip\_gre

gre

[root@client ~]# ip tunnel add tun0 mode gre remote 201.0.1.2 local 201.0.1.1

[root@client ~]# ip link show | grep tun0

6: tun0@NONE: <POINTOPOINT,NOARP> mtu 1476 qdisc noqueue state DOWN mode DEFAULT qlen 1

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

[root@client ~]# ip link show | grep tun0

6: tun0@NONE: <POINTOPOINT,NOARP,UP,LOWER\_UP> mtu 1476 qdisc noqueue state UNKNOWN mode DEFAULT qlen 1

[root@client ~]# ip addr add 10.10.10.10/24 peer 10.10.10.5/24 dev tun0

[root@client ~]# ip a s | grep 10.10

inet 10.10.10.10 peer 10.10.10.5/24 scope global tun0

[root@proxy ~]# lsmod | grep ip\_gre

[root@proxy ~]# modprobe ip\_gre

[root@proxy ~]# lsmod | grep ip\_gre

ip\_gre 22707 0

ip\_tunnel 25163 1 ip\_gre

gre 13144 1 ip\_gre

[root@proxy ~]# ip tunnel add tun0 mode gre remote 201.0.1.1 local 201.

0.1.2

[root@proxy ~]# ip link show | grep tun0

6: tun0@NONE: <POINTOPOINT,NOARP> mtu 1476 qdisc noop state DOWN mode DEFAULT qlen 1

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

[root@proxy ~]# ip link show | grep tun0

6: tun0@NONE: <POINTOPOINT,NOARP,UP,LOWER\_UP> mtu 1476 qdisc noqueue state UNKNOWN mode DEFAULT qlen 1

[root@proxy ~]# ip addr add 10.10.10.5/24 peer 10.10.10.10/24 dev tun0

[root@proxy ~]# ip a s | grep 10.10

inet 10.10.10.5 peer 10.10.10.10/24 scope global tun0

[root@proxy ~]# cat /proc/sys/net/ipv4/ip\_forward

0

[root@proxy ~]# vim /etc/sysctl.conf

[root@proxy ~]# tail -1 /etc/sysctl.conf

net.ipv4.ip\_forward=1

[root@proxy ~]# sysctl -p

net.ipv4.ip\_forward = 1

[root@proxy ~]# cat /proc/sys/net/ipv4/ip\_forward

1

[root@proxy ~]#

[root@client ~]# ping -c 2 10.10.10.10

PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.

64 bytes from 10.10.10.10: icmp\_seq=1 ttl=64 time=0.038 ms

64 bytes from 10.10.10.10: icmp\_seq=2 ttl=64 time=0.028 ms

--- 10.10.10.10 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 999ms

rtt min/avg/max/mdev = 0.028/0.033/0.038/0.005 ms

[root@client ~]# ping -c 2 10.10.10.5

PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.

64 bytes from 10.10.10.5: icmp\_seq=1 ttl=64 time=0.425 ms

64 bytes from 10.10.10.5: icmp\_seq=2 ttl=64 time=0.557 ms

2、PPTP模式

环境：centos7.4虚拟机一台，windows虚拟机一台，

规划：Linux eth0 192.168.4.2

Eth1 201.0.1.2

Windows eth0 201.0.1.5

[root@proxy ~]# ls

pptpd-1.4.0-2.el7.x86\_64.rpm

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

[root@proxy ~]# vim /etc/pptpd.conf

[root@proxy ~]# cat /etc/pptpd.conf | grep -v "^$" | grep -v "^#"

option /etc/ppp/options.pptpd

logwtmp

localip 201.0.1.2

remoteip 192.168.3.1-50

[root@proxy ~]#

[root@proxy ~]# vim /etc/ppp/options.pptpd

[root@proxy ~]# sed -rn "40p;67p" /etc/ppp/options.pptpd

require-mppe-128

ms-dns 8.8.8.8

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

[root@proxy ~]# tail -2 /etc/ppp/chap-secrets

#用户名 任何服务器 用户密码 用户地址

mark \* 123456 \*

[root@proxy ~]# systemctl start pptpd

[root@proxy ~]# netstat -anptu | grep pptp

tcp 0 0 0.0.0.0:1723 0.0.0.0:\* LISTEN 1619/pptpd

[root@proxy ~]# iptables -nL

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

[root@proxy ~]# iptables -t nat -nL

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -j SNAT --to-source 201.0.1.2

[root@proxy ~]# iptables -t nat -nL

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

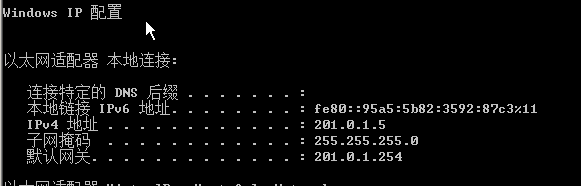
Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

SNAT all -- 192.168.3.0/24 0.0.0.0/0 to:201.0.1.2

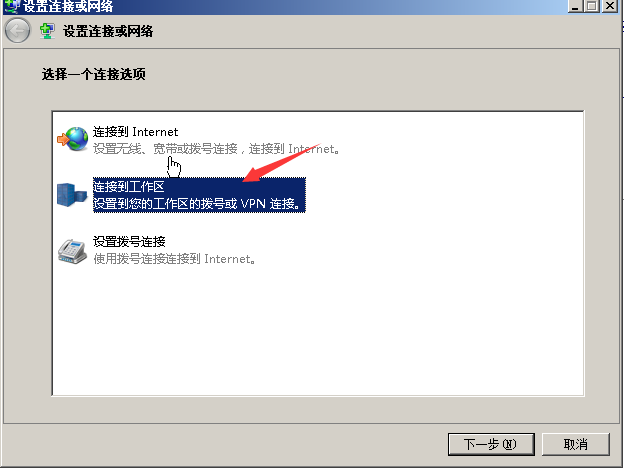
[root@proxy ~]# cat /proc/sys/net/ipv4/ip\_forward

1

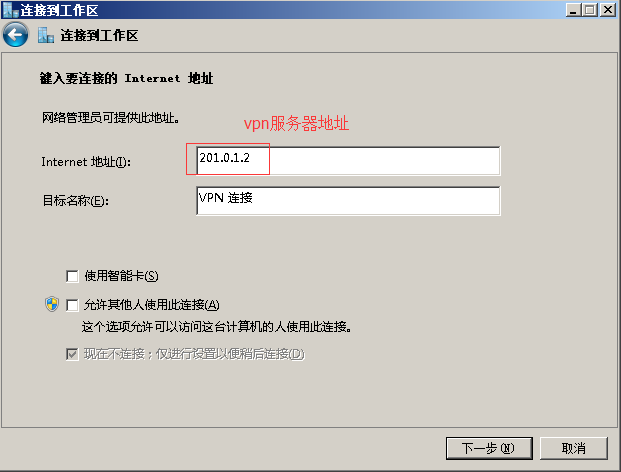


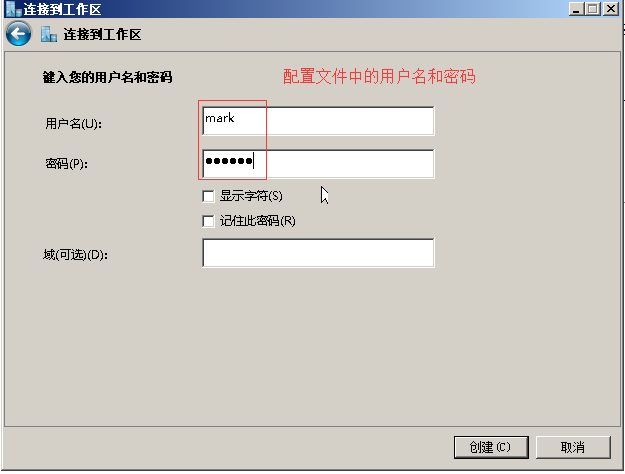


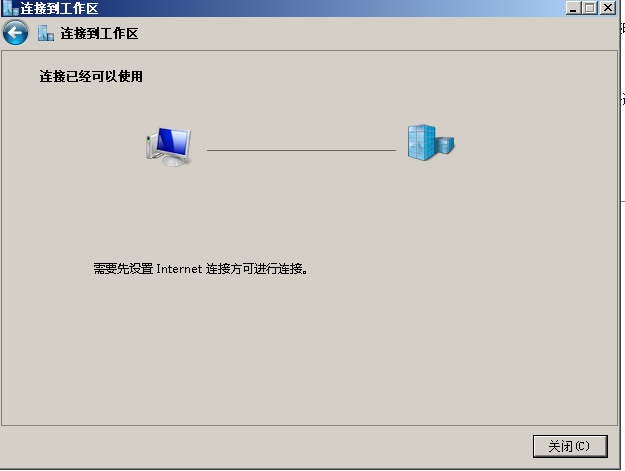










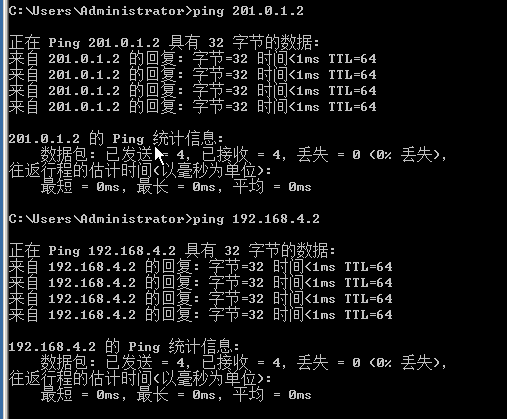












3、L2TP+IPSec

环境：centos7.4虚拟机一台，windows虚拟机一台，

规划：Linux eth0 192.168.4.2

Eth1 201.0.1.2

Windows eth0 201.0.1.5

[root@proxy ~]# yum -y install libreswan.x86\_64

[root@proxy ~]# tail -1 /etc/ipsec.conf

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

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

[root@proxy ~]# cat /etc/ipsec.d/myipsec.conf

conn IDC-PSK-NAT

rightsubnet=vhost:%priv

also=IDC-PSK-noNAT

conn IDC-PSK-noNAT

authby=secret

ike=3des-sha1;modp1024

phase2alg=aes256-sha1;modp2048

pfs=no

auto=add

keyingtries=3

rekey=no

ikelifetime=8h

keylife=3h

type=transport

left=201.0.1.2

leftprotoport=17/1701

right=%any

rightprotoport=17/%any

[root@proxy ~]# tail -1 /etc/ipsec.secrets

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

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

[root@proxy ~]# cat /etc/ipsec.d/mypass.secrets

201.0.1.2 %any: PSK "randpass"

[root@proxy ~]# systemctl start ipsec.service

[root@proxy ~]# netstat -anptu | grep pluto

udp 0 0 127.0.0.1:4500 0.0.0.0:\* 2230/pluto

udp 0 0 192.168.4.2:4500 0.0.0.0:\* 2230/pluto

udp 0 0 201.0.1.2:4500 0.0.0.0:\* 2230/pluto

udp 0 0 10.10.10.5:4500 0.0.0.0:\* 2230/pluto

udp 0 0 127.0.0.1:500 0.0.0.0:\* 2230/pluto

udp 0 0 192.168.4.2:500 0.0.0.0:\* 2230/pluto

udp 0 0 201.0.1.2:500 0.0.0.0:\* 2230/pluto

udp 0 0 10.10.10.5:500 0.0.0.0:\* 2230/pluto

udp6 0 0 ::1:500 :::\* 2230/pluto

[root@proxy ~]#

[root@proxy ~]# yum -y install ./xl2tpd-1.3.8-2.el7.x86\_64.rpm

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

[root@proxy ~]# sed -rn "31,33p" /etc/xl2tpd/xl2tpd.conf

[lns default]

ip range = 192.168.5.128-192.168.5.200

local ip = 201.0.1.2

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

[root@proxy ~]# sed -rn "10p;16p;21p" /etc/ppp/options.xl2tpd

#crtscts

#lock

require-mschap-v2

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

[root@proxy ~]# tail -1 /etc/ppp/chap-secrets

mark \* 123456 \*

[root@proxy ~]# systemctl restart xl2tpd.service

[root@proxy ~]# netstat -antpu | grep xl2tpd

udp 0 0 0.0.0.0:1701 0.0.0.0:\* 2554/xl2tpd

[root@proxy ~]#

[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.5.0/24 -j SNAT --to-source 201.0.1.2

[root@proxy ~]# iptables -t nat -nL

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

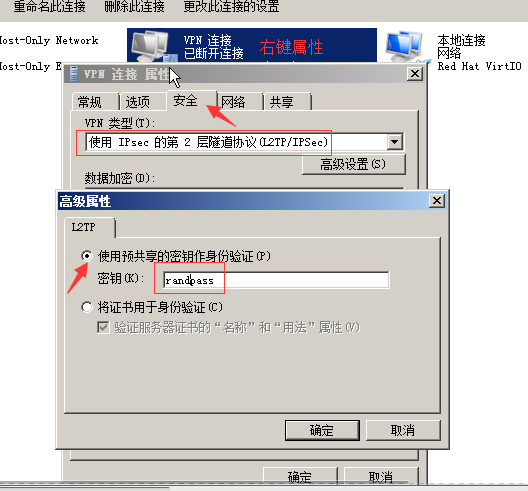
SNAT all -- 192.168.3.0/24 0.0.0.0/0 to:201.0.1.2

SNAT all -- 192.168.5.0/24 0.0.0.0/0 to:201.0.1.2

[root@proxy ~]# cat /proc/sys/net/ipv4/ip\_forward

1

[root@proxy ~]#



#修改注册表



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





