GRE VPN

搭建GRE VPN环境启动内核模块 ip\_gre

创建一个虚拟VPN（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可以查看内核模块信息

lsmod 显示模块列表

modprobe ip\_gre 加载模块ip\_gre

lsmod | grep ip\_gre 查看 是否加载了gre模块

modinfo ip\_gre 查看模块信息

主机创建VPN隧道

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）

mode 设置隧道使用gre模式

remote后面是其他主机建立隧道的对方IP地址

没启动前

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

启动该隧道（类型与设置网卡UP）

ip link show 查看

ip link set tun0 up 设置UP

启动后

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

为VPN配置隧道IP地址

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（10.10.10.10/24）

隧道对面的主机IP的隧道IP为（10.10.10.5/24）

ip a s 查看IP地址

开启路由转发

echo 1 > /proc/sys/net/ipv4/ip\_forward

里面数直1是开0是关闭

测试是否可以连接通性

ping 10.10.10.10

ping 10.10.10.5

创建PPTP VPN

使用PPTP协议创建一个可以支持身份验证的隧道连接

使用MPPE对数据进行加密

安装软件包

yum -y install pptpd-1.4.0-2.el7.x86\_64.rpm

查看所有的路径

rpm -qc pphtd

修改配置文件

vim /etc/pptpd.conf

localip 201.1.2.5 服务器本机IP

remoteip 192.168.3.1-50 分配给客户端的IP池

修改配置文件

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

修改配置文件

vim /etc/ppp/chap-secretc

lisi \* 123456 \*

用户名 服务器标记 密码 客户端

echo 1 > /proc/sys/net/ipv4/ip\_forward //开启路由转发

启动服务

systemctl start pptpd

systemctl enable pptpd

关闭防火墙

firewall-cmd --set-default-zone=trusted

翻墙设置

iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \

> -j SNAT --to-source 201.1.2.5