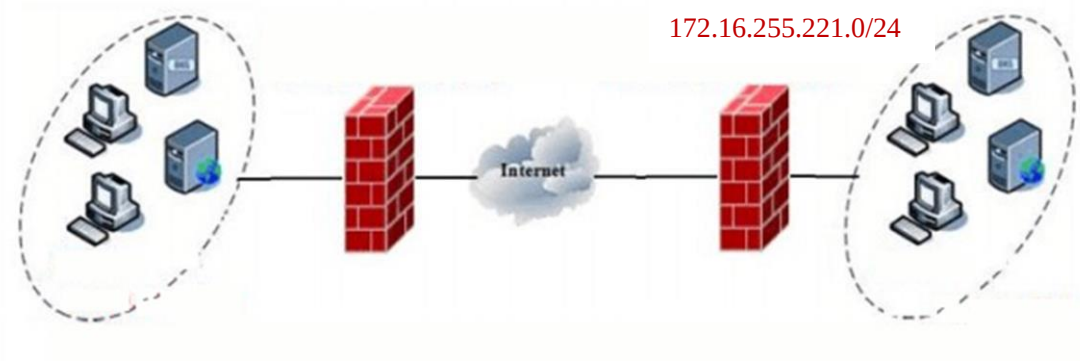
用户场景

中心端华为防火墙做了一对一 nat　114.118.75.x　221.122.75.x 划分了多个子网

分支设备需要访问中心子网(10.143.76.100、10.143.76.101、10.143.92.114、10.143.92.50、10.143.92.51、10.143.92.200)

中心用华为设备

分支用启博设备，作为出口网关，网段 172.16.255.221/24



华为设备 ipsec 配置


高级
IKE参数
IKE版本
v1
v2
使用v1发起和接受协商。
协商模式
自动
主模式
野蛮模式
加密算法
AES256
AES192
AES128
3DES
DES
认证算法
SHA2-512
SHA2-384
SHA2-256
SHA1
MD5
DH组
16
15
14
5
2
1
SA超时时间
3600
<60-604800>秒


IPSec参数
封装模式
自动
传输模式
隧道模式
安全协议
ESP
AH
AH-ESP
ESP加密算法
AES256
AES192
AES128
3DES
DES
ESP认证算法
SHA2-512
SHA2-384
SHA2-256
SHA1
MD5
PFS
NONE
16
15
14
5
2
1
SA超时
基于时间
28800
<300-604800>秒
基于流量
0
<0 , 8000-200000000>KB
DPD（对端状态检测）
检测方式
周期性发送
需要时才发送
检测时间间隔
10
<10-3600>秒
重传时间间隔
5
<2-60>秒
NAT穿越

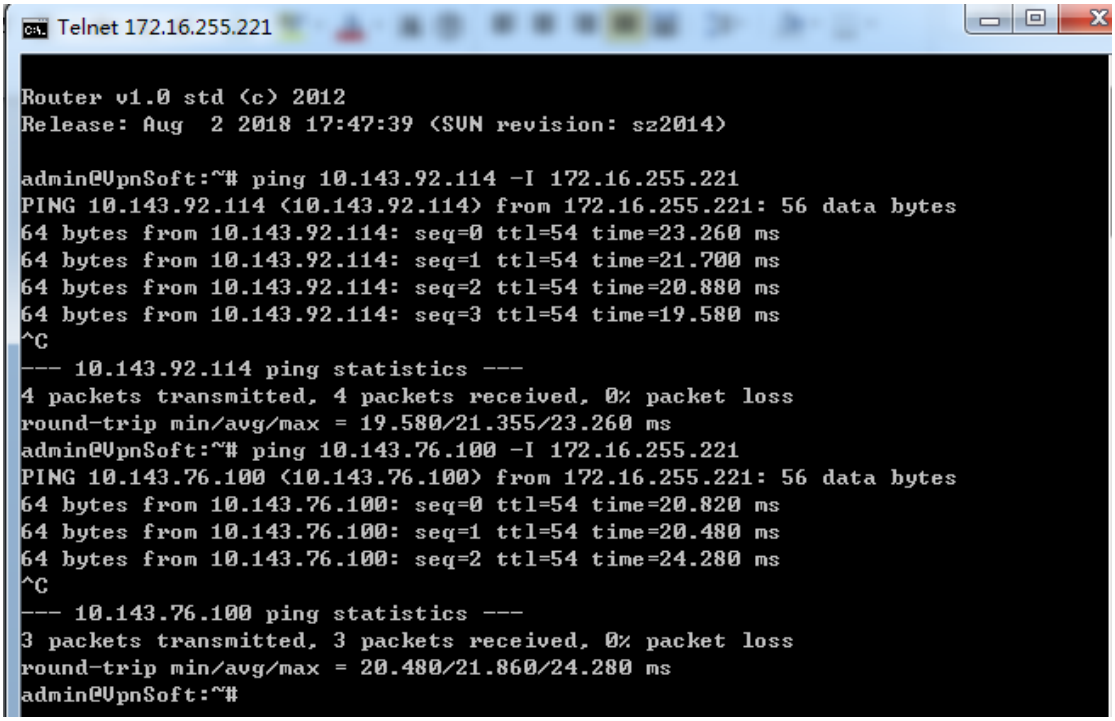
启博 VPN 设备配置

1、修改设备网段

2、设置第三方互联 ipsec 参数

4、ipsec vpn 隧道建立

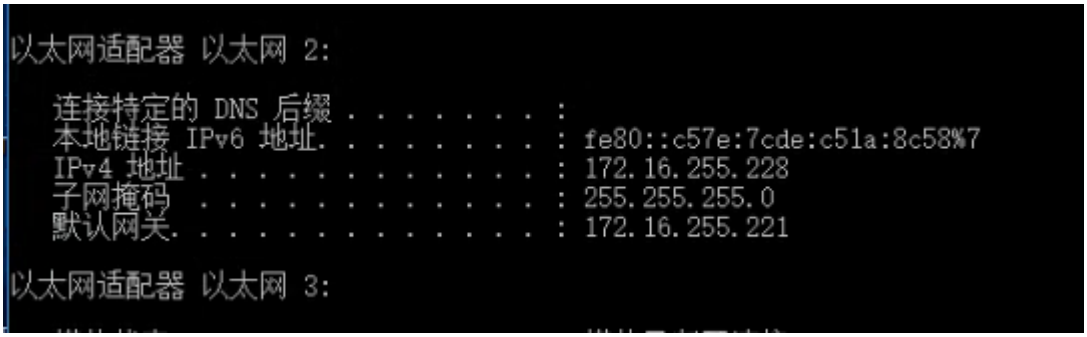
5、telnet 到 VPN 设备加源地址 ping 需要访问的 ip

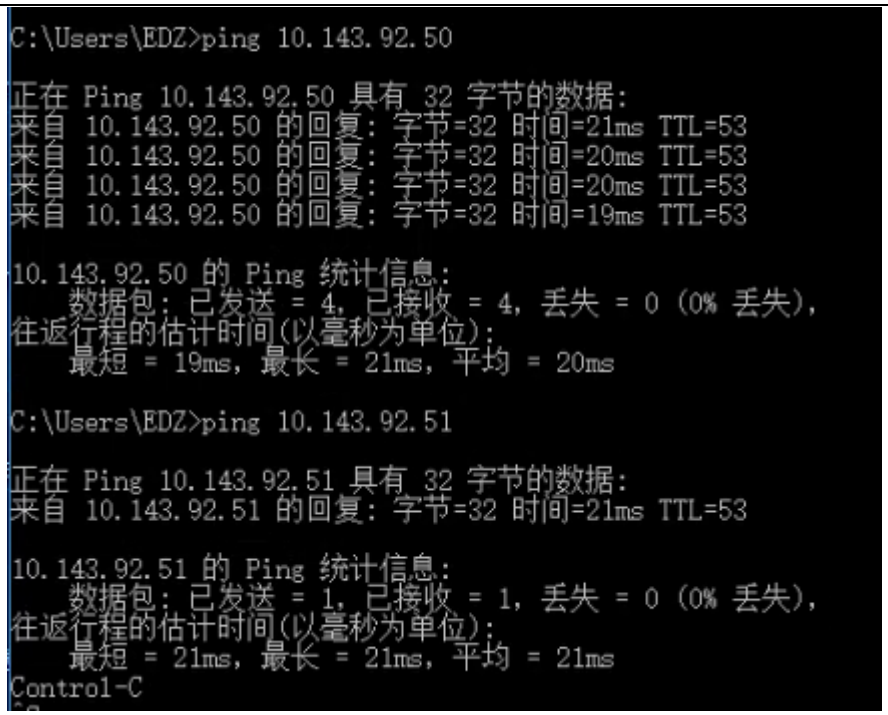


6、VPN 防火墙开机执行 nat 命令

```
iptables -t nat -A POSTROUTING -o ipsec0 -j SNAT --to 172.16.255.221
```

7、测试 VPN 下面的 pc 访问 10.143.76.100、10.143.76.101、10.143.92.114、10.143.92.50、10.143.92.51、10.143.92.200)




C:\Users\EDZ>ping 10.143.92.50
正在 Ping 10.143.92.50 具有 32 字节的数据:
来自 10.143.92.50 的回复: 字节=32 时间=21ms TTL=53
来自 10.143.92.50 的回复: 字节=32 时间=20ms TTL=53
来自 10.143.92.50 的回复: 字节=32 时间=20ms TTL=53
来自 10.143.92.50 的回复: 字节=32 时间=19ms TTL=53
10.143.92.50 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 19ms, 最长 = 21ms, 平均 = 20ms
C:\Users\EDZ>ping 10.143.92.51
正在 Ping 10.143.92.51 具有 32 字节的数据:
来自 10.143.92.51 的回复: 字节=32 时间=21ms TTL=53
10.143.92.51 的 Ping 统计信息:
数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 21ms, 最长 = 21ms, 平均 = 21ms
Control-C