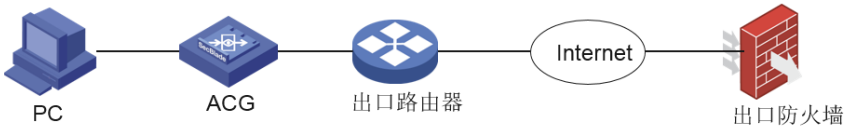
某局点ACG与防火墙建立IPSEC后无法Ping通内网网关的经验案例

SSL VPN 张腾 2018-12-12 发表

组网及说明



分支ACG与总部防火墙建立 IPSEC VPN，采用野蛮模式；ACG三层部署，终端网关在ACG上；

问题描述

IPSEC建立成功后，总部内网无法ping通分支终端网关，可以ping通分支PC;

过程分析

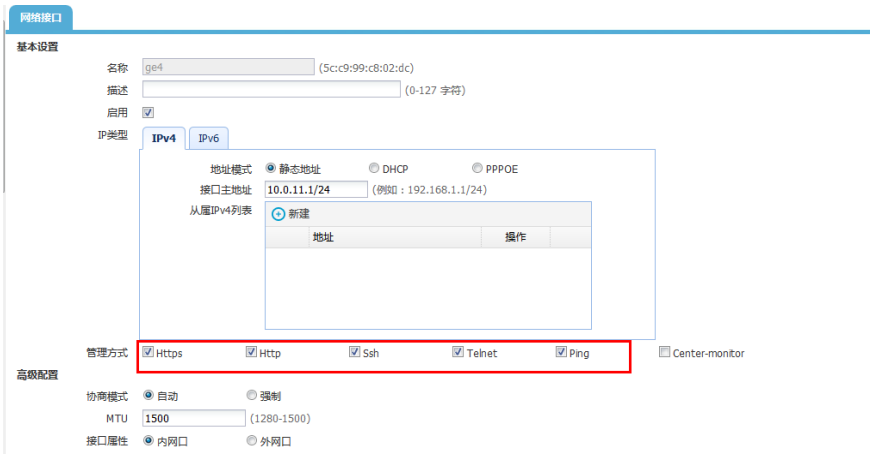
1、检测总部NAT配置

```
interface GigabitEthernet1/0/3
 port link-mode route
 ip address X.X.X.X 255.255.255.0
 nat outbound 3000
 ipsec apply policy 1
#
acl advanced 3000
 rule 11 deny ip source 10.0.0.0 0.0.0.255 destination 10.0.11.0 0.0.0.255
 rule 12 deny ip source 10.0.1.0 0.0.0.255 destination 10.0.11.0 0.0.0.255
 rule 1000 permit ip
#
```

已经调用ACL拒绝感兴趣流,目标网关地址（10.0.11.1）在此范围内 ，说明总部配置没问题；

2、总部可以访问分支PC，感兴趣流配置正确，说明IPSEC 相关配置没问题；怀疑ACG内网口禁PING；

检查ACG接口配置



内网口已经开启ping功能，现场测试分支内网PC也能够PING通此接口地址；

3、继续检查ACG配置

由于ACG建立IPSEC的实现机制与防火墙不同，需要写去对端感兴趣流的明细路由指向tunnel口，也就是说IPSEC流量需要经过tunnel口进行封装；继续检查tunnel口配置

发现tunnel口的ping功能未开启；

4、开启tunnel口ping功能后，能够正常ping通；

解决方法

开启tunnel口的ping功能；