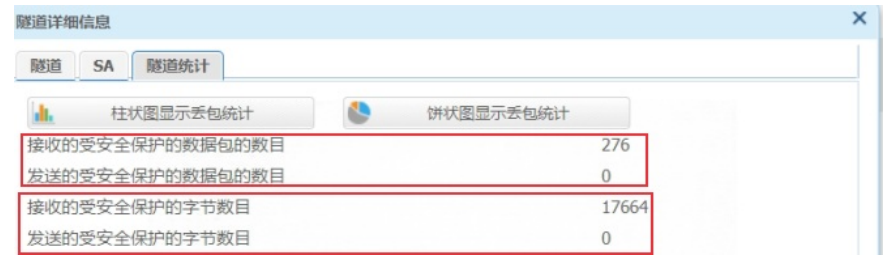
SecPath F1000-AK防火墙 IPsec VPN隧道建立不起来

IPSec VPN　付军　2022-09-29 发表

告警信息



问题描述

主模式，本端是分支，对端是总部，对接友商设备，查看有ike sa，但是没有ipsec sa，从防火墙Web页面看到IPSec VPN只有收没有发

过程分析

检查IPSec配置和对端都一致，最后检查ACL配置，发现感兴趣流从上往下匹配，匹配到了一条没有写目的地址只写了源地址的规则，而且配成了允许，导致报文走了NAT，感兴趣流在这里是需要写目的地址的。

具体可以在触发IPsec的时候，display acl看一下具体规则后面括号的匹配次数，如果次数没有增加就怀疑是不是感兴趣流没有匹配上

```
rule [illegible] permit ip source [illegible] 0.0.255.255
rule [illegible] deny ip source [illegible] 0.0.255.255 destination [illegible] 0.0.255.255
```

解决方法

删掉多余感兴趣流地址，调整deny的感兴趣流rule顺序

注意事项

修改感兴趣流ACL注意在业务空窗期进行