F1000防火墙 ipsec丢包

IPSec VPN 卢鹏 2024-06-30 发表

问题描述

现场F1000防火墙与对端f100建立ipsec
F100侧pingf1000侧ping不通，一二阶段隧道sa都有，协商没有问题，但是数据不通
Debug看被ipsec给丢了
*Jun 25 07:55:21:004 2024 HRB-H3F100C-VPNA IPFW/7/IPFW_INFO: -COntext=1;
MBUF was intercepted! Phase Num is 9(post routing beforefrag), Service ID is 28(ipsec), Bitmap is 800000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is GigabitEthernet1/0/1,
s= 10.8.6.2, d= 10.3.10.10, protocol= 1, pktid = 56622
VsysID = 1.

过程分析

查看现场配置，包括策略模板和策略，都不能使用相同的感兴趣流

```
ipsec policy-template 1 1
transform-set GE1/0/1_IPv4_1
 security acl 3001
 local-address 1.1.1.1
remote-address 2.2.2.2
ike-profile GE1/0/1_IPv4_1
#
ipsec policy-template 2 1
transform-set GE1/0/1_IPv4_1
 security acl 3001
 local-address 1.1.1.1
remote-address 3.3.3.3
ike-profile GE1/0/1_IPv4_2
#
```

感兴趣流不能deny ip

```
acl advanced 3001
rule 1 permit ip source 10.1.0.0 0.0.255.255 destination 10.2.0.0 0.0.255.255
rule 100 deny ip
```

解决方法

去掉冲突/重叠的acl，acl去掉deny后正常