某局点er路由器对接V7防火墙ipsec不通

IPSec VPN　姜霁琛　2019-05-20 发表

组网及说明

本端er3260G2对接对端F1000系列防火墙做ipsec

问题描述

现场ipsec已经成功建立，但是两端私网互ping不通。检查er本端配置，无问题，路由也配置了，查看安全联盟发现隧道已经成功建立了，数据流和配置的感兴趣流也是匹配的

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
toother3	in	180.167.238.118 =>180.167.115.58	----	----	0xfce3aae9	3DES_MD5	172.17.100.0/24 =>172.17.50.0/24
toother3	out	180.167.115.58 =>180.167.238.118	----	----	0x8ef6916e	3DES_MD5	172.17.50.0/24 =>172.17.100.0/24
toother	in	180.167.238.118 =>180.167.115.58	----	----	0xfce3aaea	3DES_MD5	172.17.80.0/24 =>172.17.50.0/24
toother	out	180.167.115.58 =>180.167.238.118	----	----	0x27b8ba7	3DES_MD5	172.17.50.0/24 =>172.17.80.0/24
toother2	in	180.167.238.118 =>180.167.115.58	----	----	0xfce3aaeb	3DES_MD5	172.17.90.0/24 =>172.17.50.0/24
toother2	out	180.167.115.58 =>180.167.238.118	----	----	0xd66c87b	3DES_MD5	172.17.50.0/24 =>172.17.90.0/24

过程分析

ipsec隧道已经建立但是ping不通私网的问题，有可能和两端感兴趣流配置不是镜像流或nat配置中没有deny掉ipsec的感兴趣流，按照此思路排查，两端的感兴趣流配置无问题，再查看两端是否有配置nat，看到对端防火墙启用ipsec的接口下还配置了nat outbound，但是没有把ipsec的感兴趣流给拒绝

```
# interface GigabitEthernet1/0/6
 port link-mode route
 ip address 180.167.238.118 255.255.255.252
 nat outbound 2000
 ipsec apply policy GE1/0/6
#
acl basic 2000
  rule 5 permit
```

解决方法

在防火墙的nat的acl中最前面写一条rule，将ipsec的感兴趣流deny掉，后面再匹配其他流量走nat