F1010防火墙对接第三方设备做ipsec VPN，ipsec sa反复删除重建

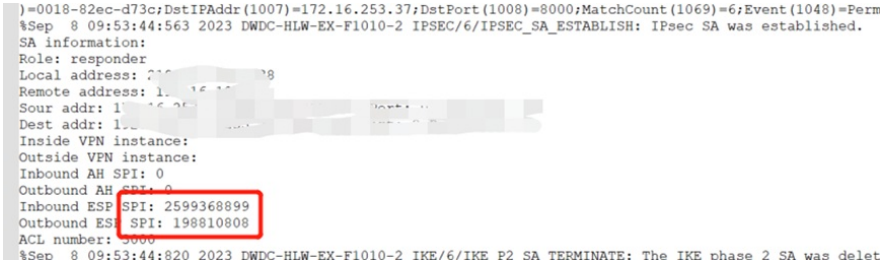
IPSec VPN　杨森A　2023-10-08 发表

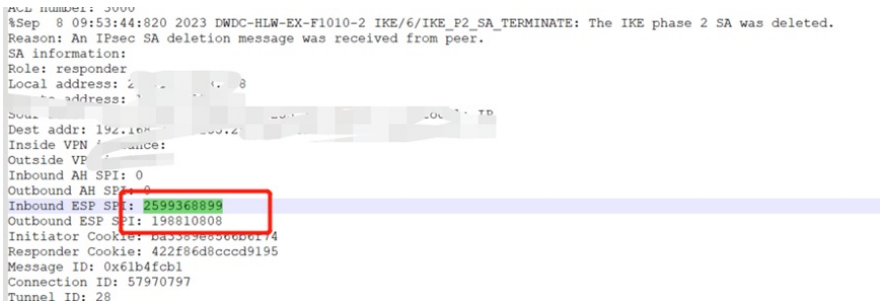
问题描述

现场F1010设备对接第三方设备做ipsec VPN，野蛮模式，本端做总部，建立ipsec以后隧道在反复断开重建。

过程分析

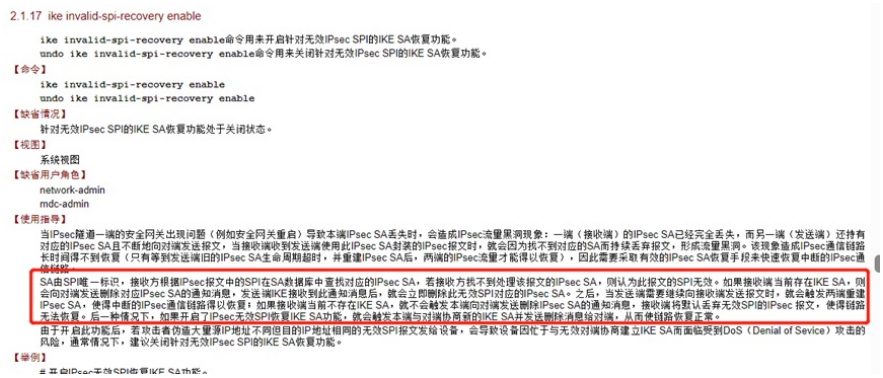
首先，看ipsec VPN建立的两个SA，ipsec SA一直在反复删除重建。

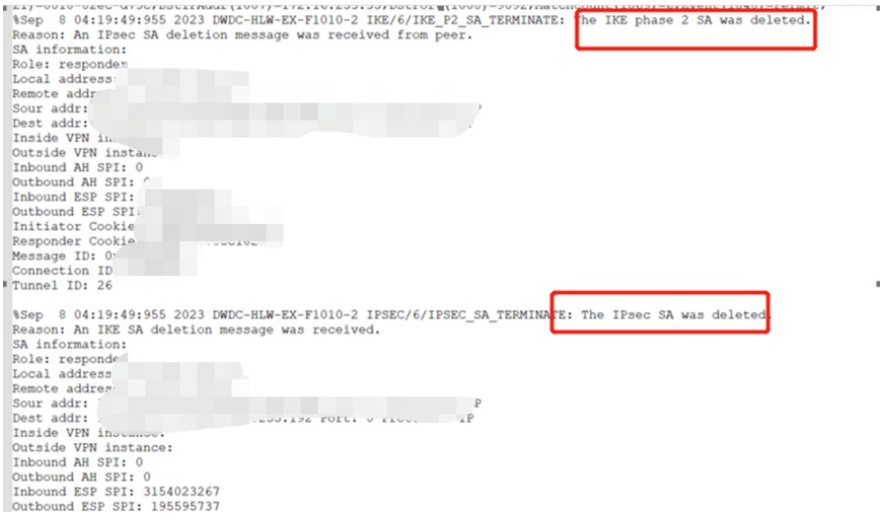




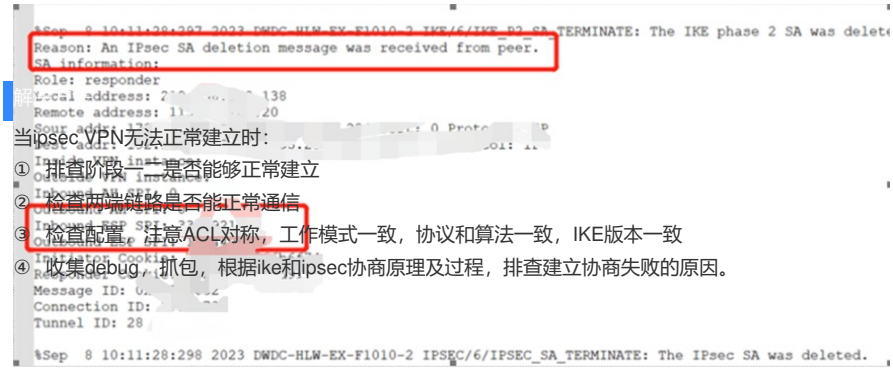
排查本端ipsec配置，发现有配置ike invalid-spi-recovery enable。

该功能是对比收到ipsec报文的SPI标识，如果在本端没有对应的ipsec SA，就通知对端删除ipsec SA，目前看报错现象隧道中断就是因为收到对端删除SA的通知，所以中断，该功能不建议开启，建议现场先关闭该功能进行测试。





两端都关闭该功能后发现ipsec sa还是在反复建立删除，排查两端配置，ACL对称，加密算法一致，继续收集debug ipsec分析，删除原因还是由于收到对端SA重置请求的报文。Reason: An IPsec SA deletion message was received from peer.



当ipsec VPN无法正常建立时：

① 排查阶段，二是否能够正常建立

② 检查两端链路是否能正常通信

③ 检查配置，注意ACL对称，工作模式一致，协议和算法一致，IKE版本一致

④ 收集debug，抓包，根据ike和ipsec协商原理及过程，排查建立协商失败的原因。

怀疑还是两端配置不一致导致，进一步检查配置，发现本端ipsec安全提议中使用的加密算法与对端不一致，ESP协议采用3des-cdc加密算法，采用md5的认证算法；而对端使用的ESP认证算法中多选择了一个sha2算法，导致两端协商不一致。

```
#
ipsec transform-set ike-profile-1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
```

两端算法修改一致后ipsec建立正常，故障消失。