

知 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。

```
)=0018-82ec-d73c;DstIPAddr(1007)=172.16.253.37;DstPort(1008)=8000;MatchCount(1069)=6;Event(1048)=Perm
%Sep 8 09:53:44:563 2023 DWDC-HLW-EX-F1010-2 IPSEC/6/IPSEC_SA_ESTABLISH: IPsec SA was established.
SA information:
Role: responder
Local address: 172.16.253.37
Remote address: 172.16.253.37
Sour addr: 172.16.253.37
Dest addr: 172.16.253.37
Inside VPN instance:
Outside VPN instance:
Inbound AH SPI: 0
Outbound AH SPI: 0
Inbound ESP SPI: 2599368899
Outbound ESP SPI: 198810808
ACL number: 3000
%Sep 8 09:53:44:820 2023 DWDC-HLW-EX-F1010-2 IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was delet
ACL number: 3000
%Sep 8 09:53:44:820 2023 DWDC-HLW-EX-F1010-2 IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted.
Reason: An IPsec SA deletion message was received from peer.
SA information:
Role: responder
Local address: 172.16.253.37
Remote address: 172.16.253.37
Sour addr: 172.16.253.37
Dest addr: 172.16.253.37
Inside VPN instance:
Outside VPN instance:
Inbound AH SPI: 0
Outbound AH SPI: 0
Inbound ESP SPI: 2599368899
Outbound ESP SPI: 198810808
Initiator Cookie: 8a358e500b6174
Responder Cookie: 422f86d8cccd9195
Message ID: 0x61b4fcb1
Connection ID: 57970797
Tunnel ID: 28
```

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。

2.1.17 ike invalid-spi-recovery enable

ike invalid-spi-recovery enable命令用来开启针对无效IPsec SPI的IKE SA恢复功能。
undo ike invalid-spi-recovery enable命令用来关闭针对无效IPsec SPI的IKE SA恢复功能。

【命令】

```
ike invalid-spi-recovery enable
undo ike invalid-spi-recovery enable
```

【缺省情况】

针对无效IPsec SPI的IKE SA恢复功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【使用指导】

当IPsec隧道一端的安全网关出现问题（例如安全网关重启）导致本端IPsec SA丢失时，会造成IPsec流量黑洞现象：一端（接收端）的IPsec SA已经完全丢失，而另一端（发送端）还持有对应的IPsec SA且不断地向对端发送报文。当接收端收到发送端使用此IPsec SA封装的IPsec报文时，就会因为找不到对应的SA而丢弃该报文，形成流量黑洞。该现象造成IPsec隧道链路长时间得不到恢复（只有等到发送端旧的IPsec SA生命周期超时，并重建IPsec SA后，两端IPsec流量才能得以恢复），因此需要采取有效的IPsec SA恢复手段来快速恢复中断的IPsec通信。

SA由SPI唯一标识，接收方根据IPsec报文中的SPI在SA数据库中查找对应的IPsec SA，若接收方找不到处理该报文的IPsec SA，则认为此报文的SPI无效。如果接收端当前存在IKE SA，则会向对端发送删除对应IPsec SA的通知消息，发送端收到此通知消息后，就会立即删除此无效SPI对应的IPsec SA。之后，当发送端需要继续向接收端发送报文时，就会转发两端重建IPsec SA。恢复中断的IPsec通信链路得以恢复；如果接收端当前不存在IKE SA，就不会转发本端向对端发送删除IPsec SA的通知消息，接收端将默认丢弃无效SPI的IPsec报文，使得链路无法恢复。后一种情况下，如果开启了IPsec无效SPI恢复IKE SA功能，就会触发本端与对端协商新的IKE SA并发送删除消息给对端，从而使链路恢复正常。

由于开启此功能后，若攻击者伪造大量源IP地址不同但目的IP地址相同的无效SPI报文发送设备，会导致设备忙于与无效SPI报文协商建立IKE SA而面临受到DoS（Denial of Service）攻击的风险，通常情况下，建议关闭针对无效IPsec SPI的IKE SA恢复功能。

【示例】

配置IPsec SA并开启IPsec SA恢复功能。

```
%Sep 8 04:19:49:955 2023 DWDC-HLW-EX-F1010-2 IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted.
Reason: An IPsec SA deletion message was received from peer.
SA information:
Role: responder
Local address:
Remote address:
Sour addr:
Dest addr:
Inside VPN instance:
Outside VPN instance:
Inbound AH SPI: 0
Outbound AH SPI: 0
Inbound ESP SPI:
Outbound ESP SPI:
Initiator Cookie:
Responder Cookie:
Message ID: 0x
Connection ID:
Tunnel ID: 26
%Sep 8 04:19:49:955 2023 DWDC-HLW-EX-F1010-2 IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted.
Reason: An IKE SA deletion message was received.
SA information:
Role: responder
Local address:
Remote address:
Sour addr:
Dest addr:
Inside VPN instance:
Outside VPN instance:
Inbound AH SPI: 0
Outbound AH SPI: 0
Inbound ESP SPI: 3154023267
Outbound ESP SPI: 195595737
```

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.

```

1Sep 8 10:11:28:297 2023 DWDC-HLW-EX-F1010-2 IKE/6/IPSEC_ES_SA_TERMINATE: The IKE phase 2 SA was deleted.
Reason: An IPsec SA deletion message was received from peer.
SA information:
Role: responder
Local address: 720...138
Remote address: 11...20
...
当ipsec VPN无法正常建立时:
① 排查阶段一 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。
...
1Sep 8 10:11:28:298 2023 DWDC-HLW-EX-F1010-2 IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted.

```

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

```

IPSec参数

封装模式 自动 传输模式 隧道模式

安全协议 ESP AH AH-ESP

ESP加密算法 SM4 GCM256 GCM192 GCM128 GMAC256 GMAC192 GMAC128 AES-256 AES-192 AES-128 3DES DES

ESP认证算法 SM3 SHA2-512 SHA2-384 SHA2-256 SHA1 MD5

PFOS NONE 24 21 20 19 18 16 15 14 5 2 1

SA超时 基于时间 基于流量

基于时间: 3600 <30-604800>秒

基于流量: 5242880 <0, 256-200000000>KB

两端算法修改一致后ipsec建立正常, 故障消失。

