使用IKEv2对vEdge上的服务隧道的IPsec问题进行故障排除

目录

简介

本文档介绍如何对配置了Internet密钥交换版本2(IKEv2)的第三方设备的Internet协议安全(IPsec)隧道的最常见问题进行故障排除。Cisco SD-WAN文档中最常被称为服务/传输隧道。本文档还说明如何启用和读取IKE调试并将其关联到数据包交换，以了解IPsec协商的故障点。

先决条件

要求

Cisco 建议您了解以下主题：

- IKEv2
- IPsec协商
- 思科SD-WAN

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

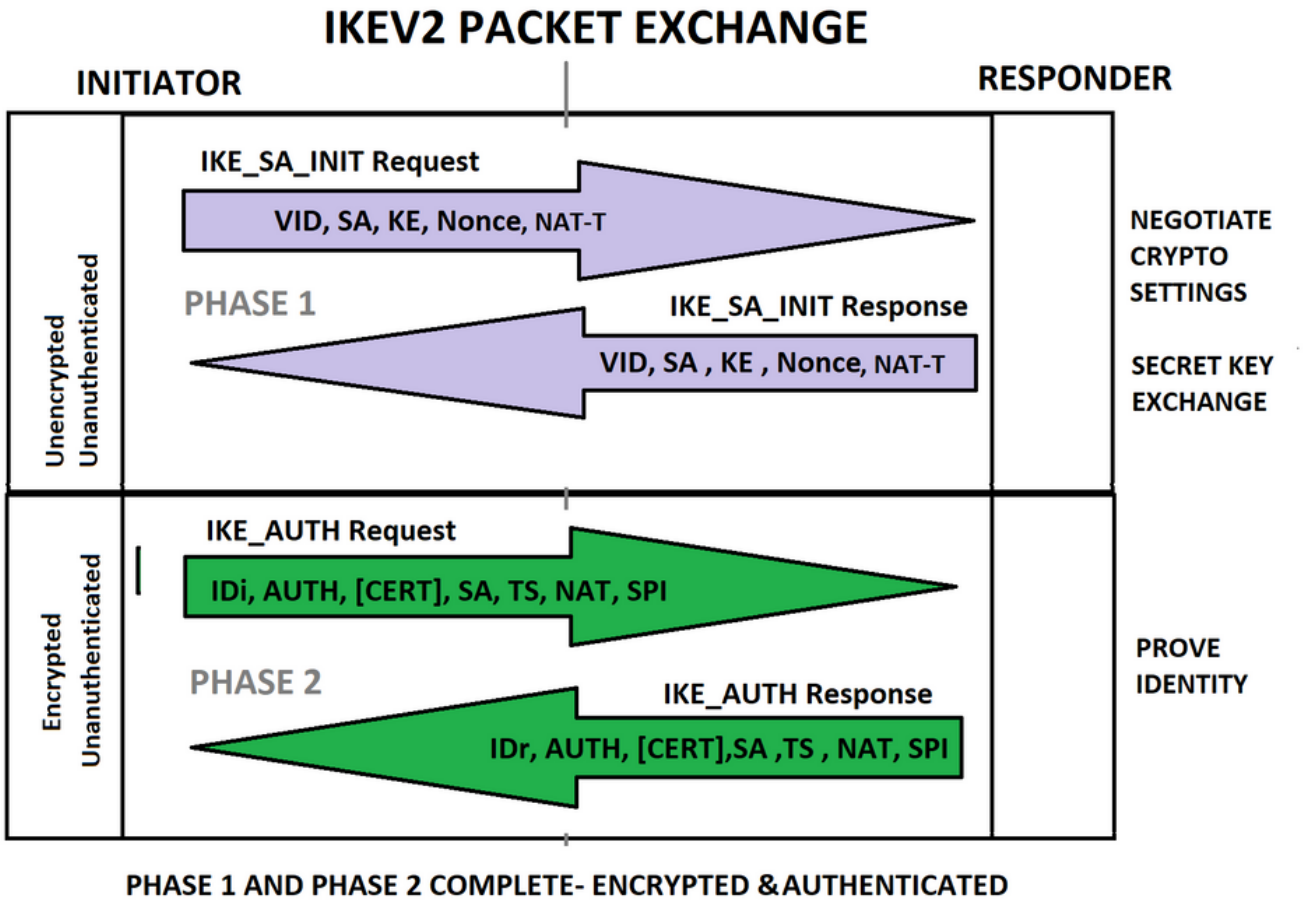
背景信息

IKE词汇表

- **互联网协议安全(IPsec)** 是IP网络中2个通信点之间的一套标准协议，提供数据身份验证、完整性和机密性。
- **Internet密钥交换版本2(IKEv2)是用于在IPsec协议簇中设置安全关联(SA)的协议。**
- 安**全关**联(**SA**)是在两个网络实体之间建立共享安全属性以支持安全通信。SA可以包括密码算法和模式等属性；流量加密密钥；以及要通过连接传递的网络数据的参数。
- 供**应商ID**(**VID**)用于识别具有相同供应商实施的对等设备以支持供应商特定功能。
- **nonce**:在交换中创建的随机值，以添加随机性并防止重播攻击。
- **密钥交换(KE)信**息，用于Diffie-Hellman(DH)安全密钥交换过程。
- **身份发起方/响应方(IDi/IDr.)**用于向对等体发送身份验证信息。此信息在公共共享密钥的保护下传输。
- IPSec共享密钥可通过再次使用DH来获得，以确保完**全前向保**密(PFS)，或通过刷新从原始DH交换获得的共享密钥来获得。
- **Diffie-Hellman(DH)密钥交换是一种通过公共信道进行加密算法安全交换的方法。**
- **流量选择器(TS)**是在IPsec协商中交换的通过加密隧道的代理身份或流量。

IKEv2数据包交换

每个IKE数据包都包含隧道建立的负载信息。IKE术语表解释了此映像上显示的缩写，作为数据包交换负载内容的一部分。

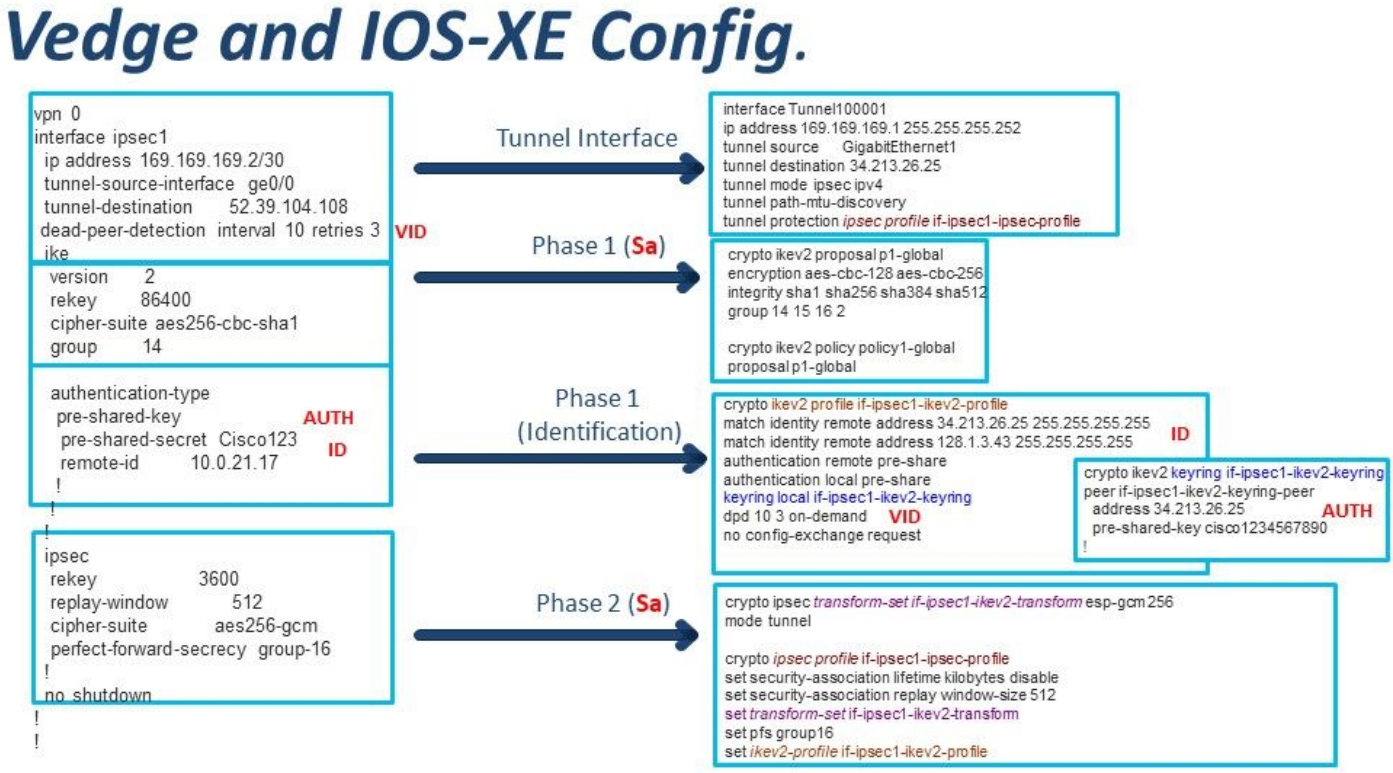


IKEV2-Exchange

注意：必须验证IPsec隧道在IKE协商的数据包交换中无法快速分析为有效解决问题而涉及的配置。

注意：本文档不详细描述IKEv2数据包交换。有关更多参考，请导航至IKEv2数据包交换和协议级别调试

需要将vEdge配置与Cisco IOS® XE配置关联。此外，如图所示，将IPsec概念与IKEv2数据包交换的负载内容进行匹配也很有用。



注意：配置的每个部分修改IKE协商交换的一个方面。将命令与IPsec的协议协商关联起来非常重要。

故障排除

启用IKE调试

在vEdge上，调试链接启用调试级别信息IKEv1或IKEv2。

```
debug iked misc high
debug iked event high
```

可以显示vshell中的当前调试信息并运行命令tail **-f <debug path>**。

```
vshell
tail -f /var/log/message
```

在CLI中，还可以显示指定路径的当前日志/调试信息。

```
monitor start /var/log/messages
```

启动IPsec问题故障排除过程的提示

可以分隔三种不同的IPsec方案。这是确定症状的一个很好的参考点，以便能够更好地了解如何开始。

1. IPsec隧道未建立。
2. IPsec隧道关闭，并自行重新建立。（拍摄）
3. IPsec隧道关闭，并保持关闭状态。

由于IPsec隧道未建立故障症状，需要实时调试以验证IKE协商上的当前行为。

对于IPsec隧道关闭并根据其自身的症状重新建立隧道，最常称为隧道Flapped，需要根本原因分析(RCA)。了解隧道关闭时的时间戳或查看调试的估计时间是必不可少的。

由于IPsec隧道关闭，并且它处于关闭状态症状，这意味着隧道以前工作过，但由于任何原因，隧道已关闭，我们需要了解拆除原因以及阻止隧道再次成功建立的当前行为。

在故障排除开始之前，请确定以下要点：

1. IPsec隧道（编号），包含问题和配置。
2. 隧道关闭时的时间戳（如果适用）。
3. IPsec对等IP地址（隧道目标）。

所有调试和日志都保存在/var/log/messages文件中，对于当前日志，它们保存在消息文件中，但是对于此特定症状，在问题发生后的数小时/数天内可以识别出抖动，最可能与调试相关的是消息1、2、3.....等。了解查看正确消息文件并分析与IPsec隧道相关的IKE协商的调试（字符）的时间戳非常重要。

大多数调试不会打印IPsec隧道的编号。识别协商和数据包的最常用方法是使用远程对等体的IP地址和隧道源于网桥的IP地址。打印的IKE调试的一些示例：

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_IPsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
```

IKE INIT协商的调试显示IPsec隧道编号，但是，数据包交换的后续信息仅使用IPsec隧道IP地址。

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_ipsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jun 18 00:31:22 vedge01 charon: 16[NET] sending packet: from 10.132.3.92[500] to 10.10.10.1[500]
(464 bytes)
Jun 18 00:31:22 vedge01 charon: 12[NET] received packet: from 10.10.10.1[500] to
10.132.3.92[500] (468 bytes)
Jun 18 00:31:22 vedge01 charon: 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(HTTP_CERT_LOOK) N(FRAG_SUP) V ]
Jun 18 00:31:22 vedge01 charon: 12[ENC] received unknown vendor ID:
4f:85:58:17:1d:21:a0:8d:69:cb:5f:60:9b:3c:06:00
Jun 18 00:31:22 vedge01 charon: 12[IKE] local host is behind NAT, sending keep alives
```

IPsec隧道配置：

```
interface ipsec2 ip address 192.168.1.9/30 tunnel-source 10.132.3.92 tunnel-destination
10.10.10.1 dead-peer-detection interval 30 ike version 2 rekey 86400 cipher-suite aes256-cbc-
sha1 group 14 authentication-type pre-shared-key pre-shared-secret
$8$wgrs/Cw6tX0na34yF4Fga0B62mGBpHFdOzFaRmoYfnBioWVO3s3efFPBbkaZqvoN ! ! ! ipsec rekey 3600
replay-window 512 cipher-suite aes256-gcm perfect-forward-secrecy group-14 !
```

症状 1. IPsec隧道未建立

由于问题可能是隧道的第一个实现，因此它尚未启动，IKE调试是最佳选项。

症状 2. IPsec隧道关闭，并自行重新建立

如前所述，通常，此症状旨在了解隧道断开的根本原因。根本原因分析已知，有时网络管理员会阻止进一步的问题。

在故障排除开始之前，请确定以下要点：

1. IPsec隧道（编号），包含问题和配置。
2. 隧道关闭时的时间戳。
3. IPsec对等IP地址（隧道目标）

DPD重传

在本例中，隧道于6月18日00:31:17关闭。

```
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec2
DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

> **注意**：IPsec隧道关闭的日志不是已标记调试的一部分，它们是*FTMD*日志。因此，不会打*印IKE*和Charon。

> **注意**：相关日志通常不会一起打印，它们之间会有与同一进程无关的更多信息。

步骤1.确定时间戳并将时间和日志关联后，开始从下到上查看日志。

```
Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits

Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
```

上次成功的DPD数据包交换描述为请求号542。

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 13.51.17.190[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]
```

步骤2.将所有信息按正确顺序排列：

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
10.132.3.92[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 Lvedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec2 DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"LONDSR01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

对于所述示例，由于vEdge01未收到来自10.10.10.1的DPD数据包，隧道关闭。在3 DPD重新传输后，IPsec对等体应设置为“丢失”，隧道关闭。此行为有多种原因，通常与ISP有关，在ISP中，数据包在路径中丢失或丢弃。如果问题发生一次，则无法跟踪丢失的流量，但是，如果问题仍然存在，则可以使用vEdge、远程IPSec对等体和ISP上的捕获来跟踪数据包。

症状3. IPsec隧道关闭，并保持关闭状态

如前所述，隧道以前工作正常，但由于任何原因，隧道已关闭，无法再次成功建立。在此场景中，会影响网络。

在故障排除开始之前确定要点：

1. IPsec隧道（编号），包含问题和配置。
2. 隧道关闭时的时间戳。
3. IPsec对等IP地址（隧道目标）

PFS不匹配

在本例中，故障排除不以隧道关闭时的时间戳开始。当问题持续存在时，IKE调试是最佳选项。

```
interface ipsec1 description VWAN_VPN ip address 192.168.0.101/30 tunnel-source-interface ge0/0
tunnel-destination 10.10.10.1 ike version 2 rekey 28800 cipher-suite aes256-cbc-sha1 group 2
authentication-type pre-shared-key pre-shared-secret
"$8$njK2pLLjgKWNQu0KecNtY3+fo3hbTs0/7iJy6unNtersmCGjGB38kIPjsoqqXZdVmtizLu79\naQdjt2POM242Yw=="
! ! ! ipsec rekey 3600 replay-window 512 cipher-suite aes256-cbc-sha1 perfect-forward-secrecy
group-16 ! mtu 1400 no shutdown
```

已启用调试标记并显示协商。

```
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (508 bytes)
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] parsed CREATE_CHILD_SA request 557 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] failed to establish CHILD_SA, keeping
IKE_SA
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] generating CREATE_CHILD_SA response 557 [
N(NO_PROP) ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)

daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (76 bytes)
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] parsed INFORMATIONAL request 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] generating INFORMATIONAL response 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (396 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[ENC] parsed CREATE_CHILD_SA request 559 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 Avedge01 charon: 07[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[IKE] failed to establish CHILD_SA, keeping
IKE_SA
```

> **注意：** CREATE_CHILD_SA数据包会针对每个密钥或新SA交换。有关更多参考，请导航至[了解IKEv2数据包交换]

IKE调试显示相同的行为，并且它不断重复，因此可以提取一部分信息并对其进行分析：

CREATE_CHILD_SA表示重新生成密钥，用于在IPsec终端之间生成和交换新SPI。

- Vedge从10.10.10.1接收CREATE_CHILD_SA请求数据包。
- Vedge处理请求并验证对等体10.10.10.1发送的建议(SA)
- Vedge将对等体发送的已接收建议与其配置的建议进行比较。
- 交换的CREATE_CHILD_SA失败，“未找到可接受的提议”。

目前的问题是：**如果之前隧道工作且未进行任何更改，为什么配置不匹配？**

深度分析时，已配置的提议上会有一个额外的字段，对等体不发送。

已配置建议：ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

收到的建议：
ESP:AES_GCM_16_256/NO_EXT_SEQ，
ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ，
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ，
ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ，
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ，
ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ

MODP_4096是DH组16，它为第2阶段（IPsec部分）上的PFS（完全前向保密）配置了vedges。

PFS是唯一不匹配的配置，在此配置中，隧道可以根据IKE协商中的发起方或响应方的身份成功建立或不成功建立。但是，当密钥重新启动时，隧道无法继续，并且可能出现或与此相关的症状。

vEdge IPSec/Ikev2隧道因DELETE事件被拆除后无法重新启动

有关此行为的详细信息，请参阅Cisco Bug ID CSCvx86427。

由于问题持续存在，IKE调试是最佳选项。但是，对于此特定Bug（如果调试已启用），终端和消息文件均不显示任何信息。

要缩小此问题范围并验证vEdge是否命中Cisco Bug ID CSCvx86427，需要查找隧道关闭的时刻。

在故障排除开始之前确定要点：

1. IPsec隧道（编号），包含问题和配置。
2. 隧道关闭时的时间戳。
3. IPsec对等IP地址（隧道目标）

确定时间戳并关联时间和日志后，在隧道关闭之前查看日志。

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] received DELETE for IKE_SA ipsec1_1[217]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[ENC] generating INFORMATIONAL response 4586 [ ]
Apr 13 22:05:21 vedge01 charon: 12[NET] sending packet: from 10.16.0.5[4500] to 10.10.10.1[4500]
(80 bytes)
Apr 13 22:05:21 vedge01 charon: 12[KNL] Deleting SAD entry with SPI 00000e77
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec1 DOWN
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-ftmd-6-INFO-1400002: Notification:
```

```
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.1.0.1 vpn-id:1 if-name:"ipsec1" new-state:down
```

注意： 在IPsec协商中有多个DELETES数据包，而CHILD_SA的DELETE是REKEY进程的预期DELETE，在没有任何特定IPsec协商的情况下收到纯IKE_SA DELETE数据包时，会出现此问题。该DELETE删除所有IPsec/IKE隧道。

相关信息

- KEv2数据包交换和协议级调试
- 互联网密钥交换(IKE)- RFC 2409
- IKEv2 - RFC 7296
- vEdge和Cisco IOS之间的站点到站点LAN到LAN IPSec
- 技术支持和文档 - Cisco Systems