使用IKEv2對vEdge上的服務隧道的IPsec問題進行故障排除

目錄

簡介

本文描述如何解決連線到已配置Internet Key Exchange版本2(IKEv2)的第三方裝置的Internet協定安全(IPsec)隧道的最常見問題。通常被引用為Cisco SD-WAN文檔上的服務/傳輸隧道。本文檔還介紹了如何啟用和讀取IKE調試，並將它們與資料包交換關聯以瞭解IPsec協商上的故障點。

必要條件

需求

思科建議您瞭解以下主題：

- IKEv2
- IPsec協商
- Cisco SD-WAN

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

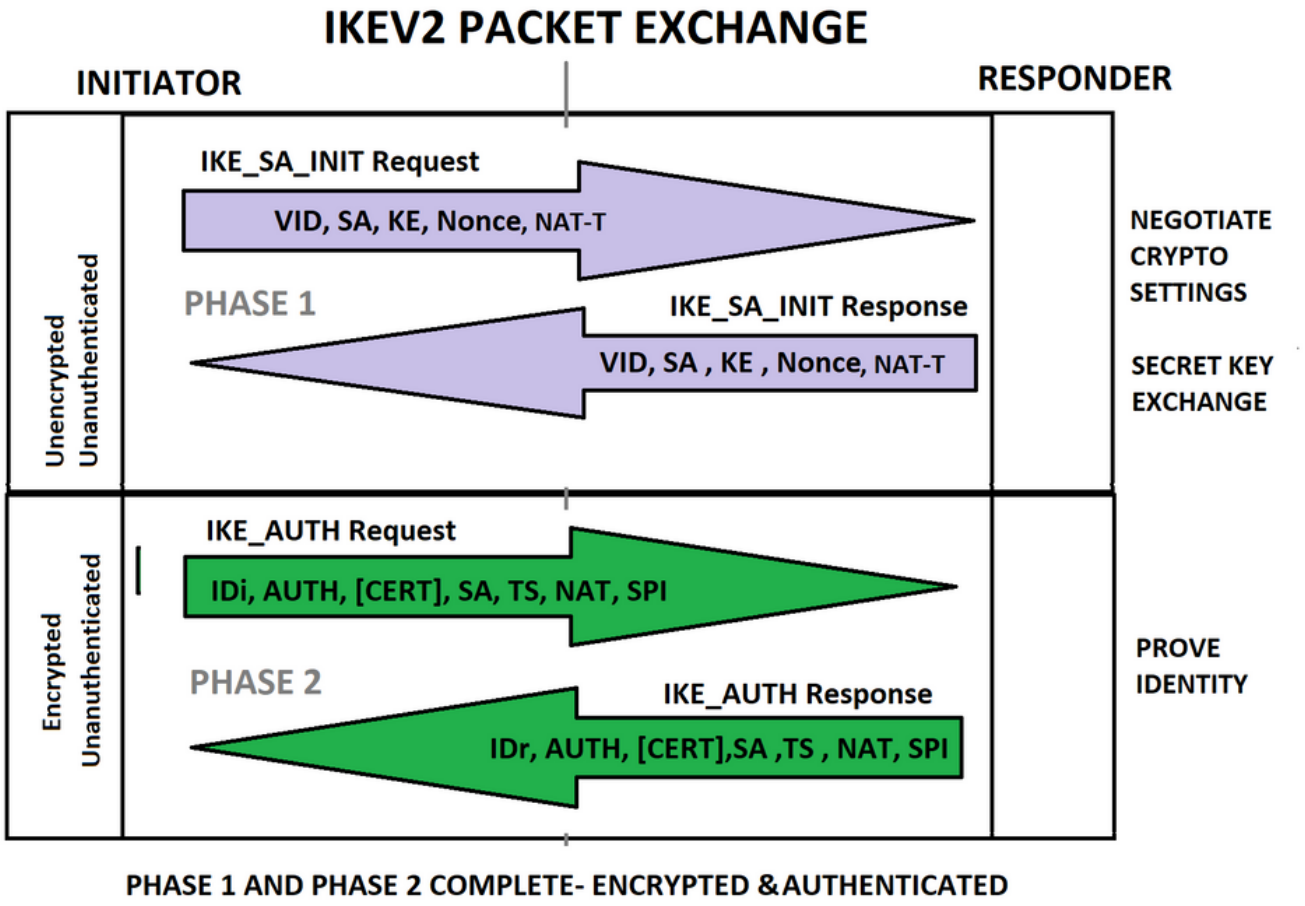
背景資訊

IKE術語表

- **網際網路通訊協定安全(IPsec)** 是跨IP網路的2個通訊點之間提供資料驗證、完整性和機密性的標準通訊協定套件。
- **Internet金鑰交換版本2(IKEv2)是用於在IPsec協定套件中設定安全關聯(SA)的協定。**
- **安全關聯**(SA)是在兩個網路實體之間建立共用安全屬性以支援安全通訊。SA可以包括加密演算法和模式等屬性；流量加密金鑰；和要通過連線的網路資料的引數。
- **供應商ID**(VID)用於標識實施相同供應商的對等裝置，以支援供應商特定功能。
- **無**:在exchange中建立的隨機值，用於新增隨機性並防止重放攻擊。
- **Diffie-hellman**(DH)安全金鑰交換進程的金鑰交換(**KE**)資訊。
- **身份發起方/響應方(IDi/IDr)**用於向對等方傳送身份驗證資訊。此資訊是在公共共用金鑰的保護下傳輸的。
- IPSec共用金鑰可以再次使用DH以確保**完全向前保密(PFS)**，也可以更新從原始DH交換中衍生的共用金鑰。
- **Diffie-hellman(DH)金鑰交換是一種通過公共通道進行安全加密演算法交換的方法。**
- **流量選擇器(TS)**是在IPsec交涉上交換的代理身分或流量，以透過通道進行加密。

IKEv2封包交換

每個IKE資料包包含用於隧道建立的負載資訊。IKE術語表說明了此影象上顯示的縮寫，作為資料包交換負載內容的一部分。

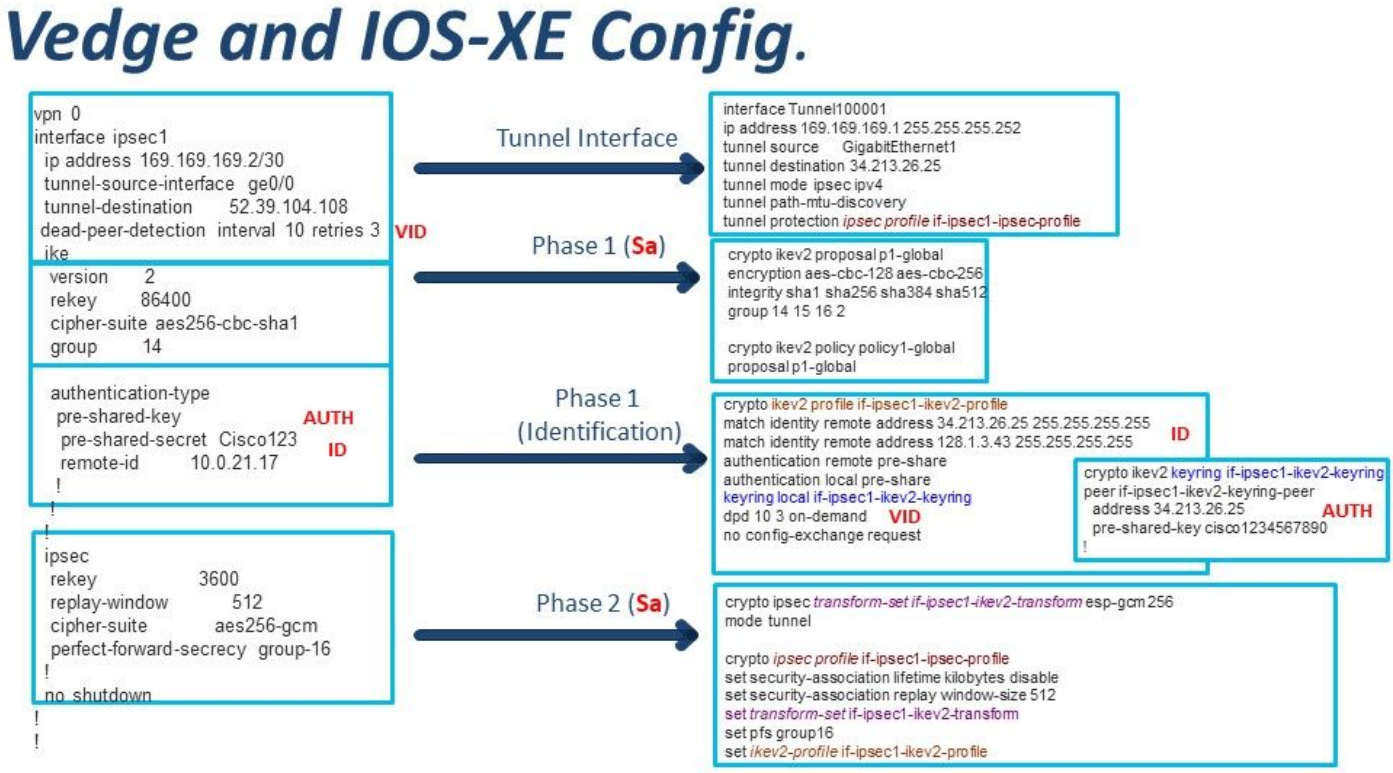


IKEV2-Exchange

附註：必須驗證IPsec隧道無法快速分析涉及到的配置以有效解決問題的IKE協商的資料包交換情況。

附註：本文檔未深入介紹IKEv2資料包交換。有關更多參考，請導航到IKEv2資料包交換和協定級別調試

需要將vEdge配置與Cisco IOS® XE配置相關聯。此外，匹配IKEv2資料包交換的IPsec概念和負載內容也非常有用，如圖所示。



附註：配置的每個部分都修改IKE協商交換的一個方面。將命令與IPsec的協定協商相關聯非常重要。

疑難排解

啟用IKE調試

在vEdge **debug iked** 上啟用IKEv1或IKEv2的調試級別資訊。

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

可以顯示**vshell**中的當前調試資訊並運行命令**tail -f** <debug path>。

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

也可以在CLI中顯示指定路徑的當前日誌/調試資訊。

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

啟動IPsec問題故障排除過程的提示

可以區分三種不同的IPsec方案。識別症狀是更好的開始方法很好的參考點。

1. IPsec隧道未建立。
2. IPsec通道發生故障，已自行重新建立。（閃爍）
3. IPsec通道已關閉，且處於關閉狀態。

由於IPsec隧道未建立症狀，因此需要即時調試以驗證IKE協商的當前行為。

若使用IPsec通道關閉，它會根據自己的症狀重新建立，通常稱為通道翻動，因此需要根本原因分析(RCA)。必須知道隧道關閉時的時間戳，或者估計時間檢視調試。

對於IPsec隧道關閉並且保持關閉狀態症狀，這意味著隧道之前曾工作過，但由於任何原因，它關閉，我們需要知道拆除原因以及當前阻止隧道再次成功建立的行為。

在故障排除開始之前確定要點：

1. IPsec通道（編號）存在問題和配置。
2. 通道關閉時的時間戳（如果適用）。
3. IPsec對等IP地址（隧道目標）。

所有調試和日誌都儲存在**/var/log/messages檔案**中，對於當前日誌，它們儲存在消息檔案中，但是對於此特定症狀，可以在問題發生後數小時/數日內確定翻動，最可能的是在messages1、2、3.等上執行相關的調試。瞭解時間戳非常重要，這樣才能檢視正確的消息檔案，並分析與IPsec隧道相關的IKE協商的調試(charon)。

大多數調試不列印IPsec隧道編號。識別協商和封包的最常見方法是使用遠端對等點的IP位址和通道源自橋接器的IP位址。列印的IKE調試的一些示例：

```
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協商的調試顯示IPsec隧道號，但是，資料包交換的後續資訊僅使用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 !
```

症狀1. 未建立IPsec通道

由於此問題可能是隧道的首次實現，因此它尚未啟動，而IKE調試是最佳選項。

症狀2. IPsec通道關閉，並且已自行重新建立

如前所述，通常解決此症狀是為了瞭解隧道關閉的根本原因。瞭解根本原因分析後，有時網路管理員可以防止進一步的問題。

在故障排除開始之前確定要點：

1. IPsec通道（編號）存在問題和配置。
2. 隧道關閉的時間戳。
3. IPsec對等IP地址（隧道目標）

DPD重新傳輸

在本例中，隧道在6月18日00:31:17關閉。

```
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
```

> **附註**：IPsec通道關閉的日誌不是索引調試的一部分，它們是*FTMD*日誌。因此，*charon*和*IKE*都不會列印。

> **附註**：相關日誌通常不是一起列印的，它們之間存在更多與同一進程不相關的資訊。

步驟1.識別出時間戳，並將時間和日誌關聯後，開始自下而上檢視日誌。

```
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)
```

上一次成功的DPD資料包交換被描述為請求# 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 [ ]
```

步驟2.按正確的順序將所有資訊放在一起：

```
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
```

例如，由於vEdge01沒有收到來自10.10.10.1的DPD資料包，通道會關閉。預計在3個DPD重新傳輸之後，IPsec對等路由器被設定為「lost」，通道會關閉。此行為的原因有多種，通常與路徑中資料包丟失或丟棄的ISP有關。如果問題出現一次，則無法跟蹤丟失的流量，但是，如果問題持續出現，則可以在vEdge、遠端IPSec對等體和ISP上使用捕獲來跟蹤資料包。

症狀3. IPsec隧道關閉且保持關閉狀態

正如在此症狀中前面提到的，隧道以前工作正常，但是由於任何原因，它關閉，隧道無法再次成功建立。在此案例中，會對網路產生影響。

在故障排除開始之前確定要點：

1. IPsec通道（編號）存在問題和配置。
2. 隧道關閉的時間戳。
3. IPsec對等IP地址（隧道目標）

PFS不匹配

在此範例中，當通道關閉時，疑難排解不會以時間戳開始。由於問題仍然存在，IKE調試是最佳選項。

```
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
```

已啟用調試連結並顯示協商。

```
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
```

> **附註：** CREATE_CHILD_SA資料包交換每個重新生成金鑰或新SA。如需更多參考，請導覽至瞭解IKEv2封包交換

IKE調試顯示相同的行為，並且它不斷重複，因此可以提取部分資訊並加以分析：

CREATE_CHILD_SA表示重新生成金鑰，目的是在IPsec端點之間生成和交換新SPIS。

- 網關收到來自10.10.10.1的CREATE_CHILD_SA請求資料包。
- vedge處理請求並驗證對等體10.10.10.1傳送的提議(SA)

- Vedge將對等體傳送的已接收建議與已配置建議進行比較。
- 交換的CREATE_CHILD_SA失敗，且「未找到可接受的提議」。

現在的問題是：**如果通道之前工作過，但未進行任何變更，為什麼會發生組態不相符？**

深入分析，對等體未傳送的已配置建議上有一個額外欄位。

配置的提議：ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

收到的建議：
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組16，該網路在第2階段（IPsec部分）上已設定為PFS（完全向前保密）。

根據IKE協商中發起者或響應者的身份，PFS是唯一可以成功建立或不成功建立隧道的不匹配配置。但是，當重新鍵入啟動時，通道將無法繼續，而且可能出現或與此症狀相關。

vEdge IPSec/Ikev2隧道在因DELETE事件而斷開後未重新啟動

有關此行為的詳細資訊，請參閱Cisco錯誤ID CSCvx86427。

隨著問題的持續，IKE調試是最佳選項。但是，如果啟用偵錯，則不會在終端或訊息檔案中顯示任何資訊。

若要縮小此問題範圍並驗證vEdge是否命中Cisco錯誤ID CSCvx86427，需要尋找通道關閉的時刻。

在故障排除開始之前確定要點：

1. IPsec通道（編號）存在問題和配置。
2. 隧道關閉的時間戳。
3. IPsec對等IP地址（隧道目標）

在識別出時間戳，並將時間和日誌關聯之後，在隧道關閉之前檢視日誌。

```
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
```

附註： IPsec交涉中有多個DELETES封包，而DELETE for CHILD_SA是REKEY流程預期的DELETE，當收到純IKE_SA DELETE封包而不進行任何特定IPsec交涉時，就會出現此問題。該DELETE刪除所有IPsec/IKE隧道。

相關資訊

- KEv2封包交換和通訊協定層級偵錯
- 網際網路金鑰交換(IKE)- RFC 2409
- IKEv2 - RFC 7296
- vEdge和Cisco IOS之間的站點到站點LAN到LAN IPSec
- 技術支援與文件 - Cisco Systems