在安全訪問和Azure/AWS中託管的C8000Vs之間的IPSec通道翻動

目錄

問題

在C8000V/Cisco IOS-XE路由器和us-east-2區域的Cisco安全訪問網路之間的IPsec網路隧道正在搖擺。

所有隧道組都受到影響，導致內部路由器與思科安全訪問網路之間的隧道關閉。

環境

- 技術：解決方案支援（SSPT — 需要合約）
- 子技術：安全訪問 — 網路隧道（IPSEC、站點到站點、專用資源）
- 產品系列：SECACCS
- 路由器：C8000V/Cisco IOS-XE路由器（內部部署）
- 遠端終端：思科安全訪問網路（美國東部–2地區）
- 軟體版本：未指定
- 觀察到錯誤消息、日誌和調試
- 在中斷期間沒有終端使用者受到影響

解析

從CNHE Splunk日誌

埠= 1409

sourceIpAddr = x.x.x.x

埠= 1408

sourceIpAddr = x.x.x.x

1. 檢測到遠端終結點更改（埠已更新）
2. 皮層在此更新時觸發子項重新生成鍵
3. 使用新埠進行重新金鑰時客戶端沒有響應，因此cortex會耗盡重試並終止隧道
4. 使用通道啟動的新連線埠重新發起使用者端後不久

來自CSA Splunk日誌。

2026-02-02T16:36:02.188+00:00觸發使用本地IP的ike更新的子金鑰重新生成金鑰： x.x.x.x，

ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00重新傳輸1個請求，帶消息ID 0

2026-02-02T16:36:08.207+00:00重新傳輸2個請求，帶消息ID 0

2026-02-02T16:36:16.207+00:00重新傳輸3個請求，帶消息ID 0

2026-02-02T16:36:32.207+00:00重新傳輸4個請求，帶消息ID 0

2026-02-02T16:37:04.207+00:00重新傳輸5個請求，帶消息ID 0

2026-02-02T16:38:08.208+00:00在5次重新傳輸後放棄

2026-02-02T16:38:08.208+00:00終止IKE，子SA重新生成金鑰失敗

在調試日誌1769305781091_vJY_CENTRAL_R2.log中:

無效SPI錯誤 — 非常頻繁：

*Jan 24 07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI:decaps: rec'd IPSEC資料包對於 destaddr=x.x.x.x prot=50,spi=,srcaddr=x.x.x.x，input interface=Tunnel12具有無效的spi

*Jan 24 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI:decaps: rec'd IPSEC資料包對於 destaddr=x.x.x.x、prot=50、spi=、srcaddr=x.x.x.x、input interface=Tunnel11具有無效的spi

通道擺動 — 通道關閉/啟動的多個例項：

*1月24日08:33:12.069: %LINEPROTO-5-UPDOWN：介面隧道上的線路協定12，狀態更改為關閉

*1月24日08:33:14.459: %LINEPROTO-5-UPDOWN：介面Tunnel11上的線路協定，狀態更改為關閉

*1月24日08:33:15.275: %LINEPROTO-5-UPDOWN：介面Tunnel11上的線路協定，狀態更改為up

原因

如果客戶端的埠在抖動，這似乎是一個不穩定的客戶端問題。

在Azure中進行更改後，抖動目前似乎很穩定。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。