在IKE重新生成金鑰事件期間，安全訪問網路隧道組與Azure VPN網關間歇性擺動

目錄

問題

在Cisco安全訪問和Azure VPN網關之間新配置的網路隧道組在IKE重新生成金鑰事件期間大約每4小時發生一次間歇性隧道抖動。

觀察到以下特定錯誤消息和症狀：

- BGP對等關閉，保留計時器已過期
- 警報：失敗的IKE重新金鑰
- IKE隧道已斷開

隧道擺動會導致週期性中斷、IKE金鑰錯誤、完整性檢查失敗、隧道斷開和BGP對等丟棄，影響到Azure資源的穩定連線。在重新生成金鑰協商期間觀察到身份驗證失敗。

環境

- 配置到Azure VPN網關的Cisco安全訪問(CSA)網路隧道組
- 使用IKEv2的IPsec站點到站點VPN隧道
- 在主模式(MM)策略中配置AES-GCM-256加密的Azure VPN網關
- 使用埠4500在兩端啟用NAT-T（NAT穿越）
- 在端點之間配置BGP對等
- 預設IKE SA生存時間為4小時(28800秒)
- 初始IPsec SA生存期配置，稍後修改到10800秒

- 未在Azure端啟用PFS（完全向前保密）

解析

根據Azure VPN網關中的錯誤識別，通過更改配置來避免主模式策略中的AES-GCM密碼來解決此問題。

步驟 1:Azure VPN網關調試分析

從Azure VPN網關端收集了IKE調試，在重新生成金鑰嘗試期間顯示此行為：

```
SESSION_ID :{} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

步驟 2:根本原因識別

Azure支援調查了重新生成金鑰失敗。Azure分析發現，當Azure使用AES-GCM-256啟動MM-REKEY時，重新金鑰資料包的格式不正確。本地裝置不響應格式錯誤的重新生成金鑰請求，從而導致隧道斷開。

步驟 3:配置因應措施實施

根據Azure的建議，實施了此緩解：

- 從網路隧道組配置中的主模式(MM)策略中刪除AES-GCM密碼。
- 配置不使用GCM模式的備用加密方法。

請參閱https://securitydocs.cisco.com/docs/csa/olh/121327.dita中的步驟17。

步驟 4:替代緩解選項

Azure還提供了可以考慮的額外緩解策略：

- 將本地MM生存期配置為大於28800秒，以便Azure始終啟動重新生成金鑰。
- 將Azure VPN網關設定為僅響應方模式，本地SA生存時間小於Azure生存時間。

原因

根本原因是Azure VPN網關中的一個錯誤，該錯誤影響AES-GCM重新生成金鑰操作。當Azure使用AES-GCM-256啟動MM-REKEY時，重新金鑰資料包的格式不正確，導致本地思科安全訪問裝置無法響應格式錯誤的重新金鑰請求。這會導致IKE重新生成金鑰失敗、身份驗證錯誤和隨後的隧道斷開。

Azure已將此錯誤確認為現有錯誤，並記錄了在未來網關版本（定於2026年中發佈）中計畫進行的修復。

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）。