恢復主對等IP時安全訪問網路隧道組內部伺服器錯誤

目錄

問題

嘗試在Cisco Secure Access上修改網路隧道組(NTG)中的遠端對等IP時，使用者在嘗試將主隧道IP恢復為先前配置的值時，可能會在UI中遇到「Internal Server Error」（內部伺服器錯誤）。具體場景包括：

- 最初配置有主隧道IP和輔助IP的NTG，兩個隧道都成功建立。
- 為了測試目的，主隧道IP被更改為不同的IP地址，可以毫無問題地接受該地址。
- 當嘗試將主隧道IP恢復為原始值時，系統無法儲存配置並在UI中返回「Internal Server Error（內部伺服器錯誤）」。
- 此行為始終可重複，在嘗試重複使用先前配置的IP地址時出現。
- 原始IP先前工作正常，並且與輔助隧道IP沒有衝突。

環境

- 思科安全存取（前身為Cisco Umbrella for SSE）
- 專用接入的網路隧道組配置
- 具有主要和輔助對等IP的雙隧道配置
- 基於Web的管理介面

解析

此問題由後端驗證/狀態問題導致，其中原始對等IP在配置更改後仍被保留或停滯在後端系統中。必須遵循下一節中介紹的故障排除和解決步驟：

步驟 1:收集診斷資訊

收集以下資訊以進行後端驗證：

- 安全訪問組織ID
- 網路隧道組名稱
- 受影響的主隧道的隧道ID
- 為NTG選擇的區域/資料中心
- 儲存嘗試失敗的確切時間戳，包括時區
- 確認原始IP是否出現在任何其他NTG中（當前或先前）
- 失敗的儲存嘗試的瀏覽器HAR捕獲

步驟 2:捕獲瀏覽器HAR檔案

為失敗的儲存嘗試收集診斷資料：

- 開啟瀏覽器開發人員工具
- 轉到「網路」頁籤
- 啟用保留日誌
- 重現儲存失敗
- 匯出HAR檔案並將其附加到支援案例

附註：在上傳HAR檔案之前清理/刪除所有會話令牌或cookie。

步驟 3:後端驗證和清理

此問題需要後端干預，無法僅從UI解決。下列操作必須由思科技術支援執行：

- 參與Secure Access後端/SSE平台團隊
- 驗證過時的對等IP保留
- 檢查孤立的隧道對象
- 識別與特定NTG配置關聯的重複後端金鑰
- 清除原始IP的過時隧道對等體引用
- 如有必要，強制後端重新同步NTG對象
- 釋放繫結到NTG UUID的對等IP分配

步驟 4:替代解析方法

如果後端清理不能立即可用，請嘗試以下過程：

- 刪除網路隧道組主配置
- 等待5分鐘
- 使用所需的IP地址重新新增NTG

⚠注意：有可能。此處提到的詳細資訊似乎包含執行後可能會產生重大影響的過程或命令。請確保上述程式或命令已由SME或業務部門在執行或推薦之前進行評估。

步驟 5:臨時解決方法

如果NTG正在生產中且無法刪除：

- 繼續使用輔助隧道進行連線

- 從您的供應商/合作夥伴處獲取其他公共IP
- 更新NTG主裝置以使用備用IP
- 確認減少冗餘直到後端問題得到解決

原因

此問題是由思科安全訪問後端系統中的軟體錯誤導致的。當主對等IP被更改並恢復回其原始值時，後端驗證系統錯誤地將原始IP視為仍處於分配或保留狀態，即使它應該可以重複使用。這會導致後端驗證失敗，UI將其遮蔽為一般的「Internal Server Error」。 在配置更改過程中，後端系統無法正確清除或釋放IP保留，從而造成一個持久狀態問題，阻止在同一NTG中重複使用IP。

相關內容

- 排除故障並收集思科安全訪問的基本資訊
- 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）。