網路中斷後的WSA上游代理運行狀況檢查問題

目錄

問題

長時間中斷網路後，配置為使用FQDN指定的上游代理的思科網路安全裝置(WSA)可能無法恢復將流量轉發到上游代理，而是直接傳送流量。此問題在WSA在網路中斷期間將上游代理標籤為「停機」時出現，但是無法識別何時上游代理重新可用（即使在網路連線恢復後）。

觀察到的具體症狀包括：

- 通過FQDN和「故障處理=直接執行」配置了上游代理的WSA
- 影響上游代理和DNS伺服器連線的長期網路中斷
- 網路恢復後，訪問日誌不顯示DEFAULT_PARENT標籤，表明流量繼續繞過上游代理
- 在一台WSA裝置上發生問題，而同一環境中的另一台裝置正常運行

環境

- 思科網路安全裝置(WSA)S系列
- AsyncOS 14.5.2-011（受影響版本）
- 硬體：S695
- 使用FQDN規範配置的上游代理
- 配置為「Go Direct」的故障處理
- 採用L2交換機基礎設施的網路環境

解析

通過將AsyncOS升級到包含CSCwi13124修復程式的版本來解決此問題。已在以下AsyncOS版本中修復此錯誤：

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

當前版本的臨時解決方法

對於無法立即升級的環境，可以通過調整用於檢查無響應的上游代理的最大空閒超時來臨時緩解：

步驟 1:訪問CLI並導航至高級代理配置：

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

步驟 2:修改最大空閒超時設定：

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

步驟 3:將預設最大值(86400秒/24小時)減小為較小的值，以減少運行狀況檢查之間的時間。

即時復原方法

如果問題當前影響流量，則下一個命令可以立即恢復上游代理功能：

步驟 1:訪問診斷選單：

```
CLI > diagnostic > PROXY > kick
```

這將重新啟動代理進程並恢復正常的上游代理操作。

驗證和測試程式

要測試問題是存在還是在升級後已解決，請檢視以下步驟：

步驟 1:建立基線監視

監控訪問日誌和代理日誌以確認WSA正在將流量傳送到上游代理。驗證流量是否到達上游代理端。

步驟 2:模擬網路中斷

確認流向上游代理的正常流量後，請斷開以下連線：

- WSA到上游代理連線
- WSA到DNS伺服器的連線

步驟 3:監控器故障檢測

檢查代理日誌和系統日誌以瞭解以下指標：

- 代理日誌可以將上游代理顯示為「……宣告為無效」
- 系統日誌可以顯示「嚴重：查詢DNS伺服器時已達到最大失敗次數……"

步驟 4:保持中斷狀態

如果不重新啟動代理進程，請保持步驟2中的disconnected狀態並繼續生成請求約10小時。

步驟 5:恢復連線

約10小時後，恢復步驟2中已斷開的連線。

步驟 6:監視恢復行為

完成步驟5後，無需重新啟動代理進程即可監控訪問日誌和代理日誌：

- 在固定系統中：流量會恢復通過上游代理，並且代理日誌顯示正常運行狀態轉換

- 在受影響的系統中：訪問日誌顯示流量繼續繞過上游代理，並且代理日誌不會顯示「……生病，現在健康」或「……健康，現在生病」消息

原因

此問題的根本原因是上游代理運行狀況檢查機制中的邏輯缺陷。當WSA確定已配置的上游代理為「宕機」（無響應）時，它實施指數回退演算法，在每次失敗後將運行狀況檢查間隔加倍。此時間間隔最多可以達到24小時(86400秒)。

當上游代理在這些擴展時間間隔之一期間再次可用時，會發生此問題。即使代理已恢復並且正常響應，WSA也不會執行運行狀況檢查，直到經過完整配置的時間間隔。這可能會導致長達24小時的連續直接流量路由，而不是恢復上游代理的使用。

此行為影響WSA配置，其中：

- 上游代理由DNS主機名/FQDN（非IP地址）指定
- 「故障處理」設定為「直接處理」
- 擴展的網路中斷會影響上游代理和DNS伺服器連線

思科錯誤 ID:CSCwi13124

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）。