

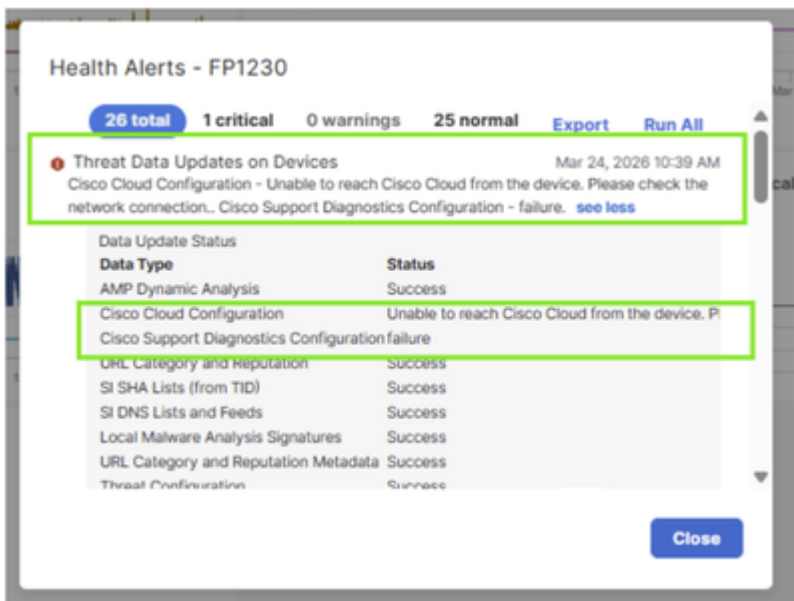
疑難排解FTD無法連線至思科雲端以取得威脅資料更新

目錄

問題

新部署的思科安全防火牆(CSF)1230裝置無法到達思科雲，阻止下載威脅防禦更新。以下錯誤消息顯示在系統中：

- 「裝置上的威脅資料更新 — 思科雲配置 — 無法從裝置訪問思科雲。請檢查網路連線。」
- "思科支援診斷配置 — 故障。"



防火牆似乎在所有其他方面都能正常工作，但雲連線故障導致裝置無法從思科基於雲的服務接收關鍵威脅情報更新。

環境

- FTD軟體版本：7.7.11.其他軟體版本也可能會受到影響。
- 硬體：CSF1230。其他平台也可能受到影響。

解析

參考 (最常見的原因)

針對FTD上的此警報對，最常見的原因包括：

- 思科雲端點的域名系統(DNS)解析失敗。
- 來自管理平面的出站連線被阻止。
- 代理是干擾因素。
- 管理介面通過NAT到達Internet，但NAT配置不正確。

在這種情況下，通過為新部署的FTD裝置設定所需的轉換規則，問題得以解決。

恢復雲連線採取了以下步驟：

步驟1.確定缺失的NAT規則

調查發現，缺少正確的NAT規則導致防火牆無法建立與Cisco雲服務的連線。這些NAT規則對於防火牆正確將流量路由到思科基於雲的威脅情報服務至關重要。

步驟2.配置轉換規則

將所需的NAT規則新增到客戶的網路配置中，以支援新防火牆的雲連線要求。這些規則使防火牆裝置能夠成功與思科雲基礎設施進行通訊，以更新威脅資料。

步驟3.驗證雲連線

實施NAT規則後，防火牆成功連線到Cisco雲。已清除以前顯示的錯誤消息，裝置開始按預期接收威脅情報更新。

解決方法是通過更改客戶網路基礎架構中的配置，而不是修改防火牆裝置本身來實現的，從而確保正確滿足新防火牆的雲連線要求。

原因

連線問題的根本原因是客戶的網路配置中缺少所需的NAT規則。

相關內容

- <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/217616-troubleshoot-cisco-cloud-configuration.html>
- <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/reference-ports.html>
- [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）。