Secure Network Analytics Virtual Appliance網路介面配置限制

目錄

問題

正在評估具有非資料儲存的安全網路分析(SNA)的部署方案，其中流量收集器通過虛擬化平台分配了多個網路介面。

產生的具體問題是：

- 虛擬流量收集器是否可以使用兩個NIC運行 — 一個用於SNA內部通訊，另一個用於NetFlow接收
- 當內部通訊網段無法訪問網際網路時，是否可以使用多個NIC配置Virtual Manager裝置以獲取威脅源

環境

- Secure Network Analytics(Stealthwatch)版本，最高為7.6.0
- 所有SNA元件的虛擬裝置版本（管理器、流量收集器）
- 具有分離的內部通訊和NetFlow接收段的網路架構

解析

Cisco Secure Network Analytics(SNA)Flow Collector可與兩個NIC介面一起部署，並且此行為已在實驗室環境中經過驗證：

1.兩個介面 — 管理訪問和NetFlow接收

- 流量收集器可以配置一個用於管理訪問的介面和一個專用於接收NetFlow的第二介面。
- 但是，管理訪問仍然可以通過任一介面（管理或NetFlow）訪問。 當前沒有選項嚴格限制介面用於其預期目的。

2.兩個介面 — NetFlow接收和威脅源接收

- 使用從流量收集器的Internet訪問檢索威脅源更新。
- 如果管理介面IP沒有直接的Internet訪問，則可以配置流量收集器上可用的proxy選項以滿足此要求，而第二個介面繼續接收NetFlow。

關於範圍的重要說明
這兩種方案都僅在實驗室設定中驗證，未記錄在SNA設計手冊中。因此，它們必須被視為觀察到的行為，而不是正式發佈的設計建議。我們鼓勵計畫進行此類部署的客戶首先在自己的測試環境中進行驗證。

原因

此行為由安全網路分析流量收集器裝置架構中的設計所導致。裝置支援分配額外的NIC，當主介面用於管理時，可以在輔助介面上接收遙測(NetFlow)。但是，裝置軟體運行其管理服務（裝置管理UI、SSH和SNA裝置間通訊）繫結到所有已配置和定址的介面，並且不公開任何逐個介面的服務繫結或訪問控制選項。因此，管理訪問仍然可以從任一網絡卡訪問，並且不能限制到為此目的指定的介面。

同樣，威脅源檢索不與特定NIC關聯。更新過程只是根據裝置路由表啟動出站連線，因此具有到Internet的有效路徑的任何介面都會為請求提供服務。如果管理介面無法直接訪問網際網路，則裝置管理中的代理配置選項會通過已批准的代理伺服器轉發出站請求，從而允許威脅源在不更改介面角色的情況下成功更新。

由於多NIC流量收集器部署和介面角色分離未在《安全網路分析設計手冊》中介紹，因此此行為未記錄而非不受支援，並且發現結果僅基於實驗室驗證。

相關內容

- Secure Network Analytics Virtual Edition裝置安裝指南

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）。