配置流量收集器的忽略清單功能

目錄

簡介

本文檔介紹如何使用「忽略清單」將SNA流量收集器配置為拒絕來自特定匯出器的傳入的netflow。

背景資訊

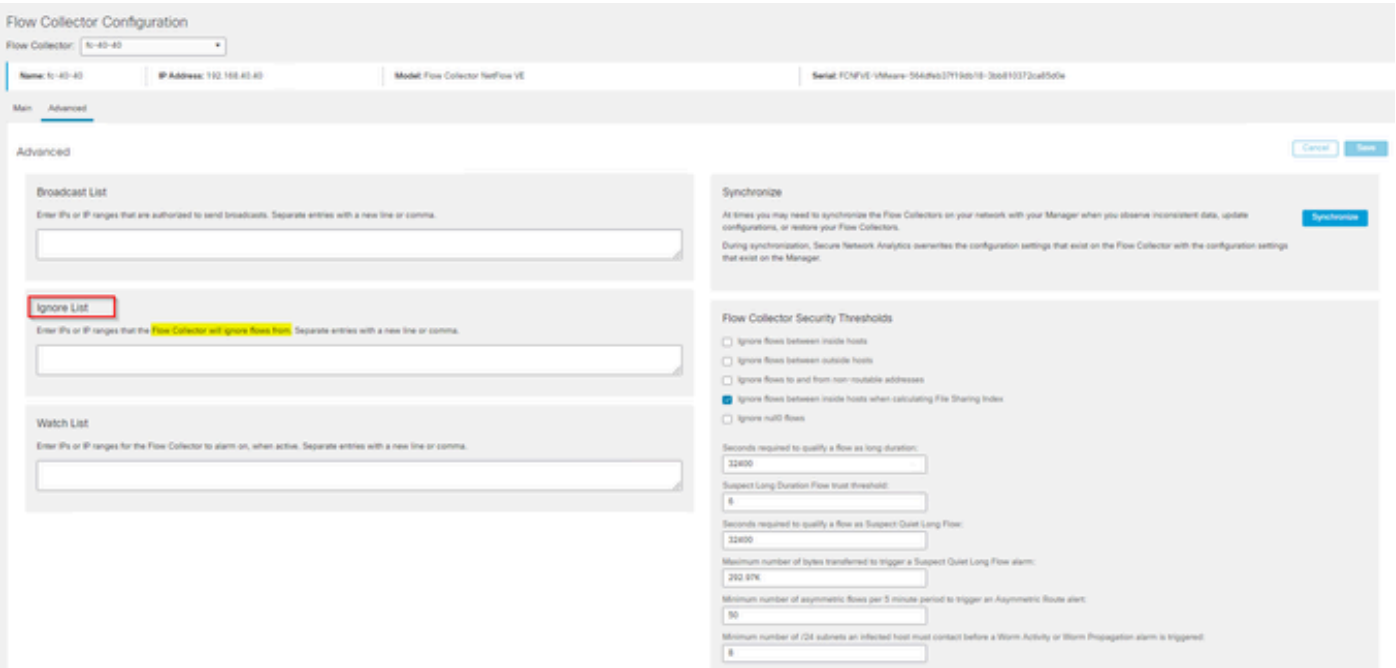
通常，會出現以下問題：「是否有任何方法通知我的SNA流量收集器拒絕來自特定匯出器的傳入網路流？」

答案是肯定的，這是通過使用流量收集器「忽略清單」功能完成的。

設定

忽略清單功能特定於流量收集器。 在SNA 7.x的更高版本中，此功能可在SNA Manager Web UI上的流量收集器配置頁面內使用。

使用此頁可指定流收集器為其設定的、不限數量的主機或子網。 如果Flow Collector看到屬於這些IP地址的任何流量，它將從任何圖形或表中排除該流量。 請確定您可以信任所有往返於主機的流量。Secure Network Analytics不會分析此流量，也不會分析偽裝為包含任何這些主機的流量。如果網路上發起的攻擊涉及這些主機/子網之一，Flow Collector無法報告該攻擊。



常見問題

對於智慧許可，忽略清單對每秒流量(FPS)計算有何影響？

答：將主機IP地址或範圍新增到忽略清單可有效防止任何流量根據計算得出的FPS速率進行計數，該速率最高傳送到SMC並用於智慧許可證報告。 在SMC控制面板上顯示的流趨勢圖中，不再顯示/計算流。

當客戶端處於拆分隧道模式時，處理NVM流時，如何使用忽略清單功能？

客戶可以配置AnyConnect向我們傳送網路上和網路外流量（也稱為拆分隧道）。網外流量使用可能包含重疊IP的終端本地IP地址。SNA不支援重疊的IP， t因此建議使用Ignore list功能來避免分割通道問題，從而保留基於NVM的流量進行檢測的優點。

在此使用情形中，我們配置「忽略清單」以防止離網的NVM流從流快取→ flow_stats、流搜尋、自定義安全事件

1. 將IP地址和網路掩碼(例如，新增192.168.1.0/24、127.0.0.1/24)新增到忽略清單中
2. 驗證nvm_flows是否仍使用NVM流填充
3. 如果src或dst IP在Ignore List中，請驗證flow_stats是否沒有NVM流

是否可以使用ignore list忽略來自整個匯出器的流？ 否，因為忽略清單基於流資料而不是匯出器資料，所以將匯出器IP地址新增到忽略清單將有效地忽略匯出器IP作為流的源或目標列出的流資料，而不是忽略來自該特定匯出器的所有流記錄

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）。