FMC關聯策略允許清單事件要求啟用網路發現策略

目錄

問題

在Cisco Secure Firewall Management Center(FMC)上使用允許清單配置關聯策略時，請務必注意，除非為目標網路IP配置了網路發現策略，否則不會生成允許清單事件和允許清單違規。如果沒有此配置，則在Analysis > Correlation > Allow List Events和Analysis > Correlation > Allow List Violations下不會顯示任何事件。

在實驗室檢測過程中，發現了以下行為：

- 為配置的目標網路正確生成關聯事件。
- 目標網路主機不符合時，不會生成允許清單事件或允許清單違規。

環境

- 由安全防火牆管理中心(FMC)管理的Cisco Firepower威脅防禦(FTD)
- 使用允許列錶針對特定IP地址配置的關聯策略
- 允許配置為允許特定Web應用程式、應用程式或協定的清單

解析

經過大量的實驗室測試並與開發團隊協商，確認必須啟用網路發現策略，才能生成允許清單事件和允許清單違規。

決議案涉及以下步驟：

步驟 1:啟用網路發現策略

在FMC介面中導航到Policies > Network Discovery，然後建立規則（如果不存在規則）。

步驟 2:配置網路發現規則

使用適當的源網路設定配置網路發現規則：

- 將源網路指定為內部網路範圍。
- 或者，如果監控所有流量源，請使用所有網路(0.0.0.0/0)。
- 確保規則涵蓋預期從中產生Allow List Events的網路。

步驟 3:啟用關聯策略規則

驗證關聯策略規則是否處於活動狀態且未處於禁用狀態。

步驟 4:驗證允許清單事件生成

啟用網路發現並啟用關聯策略規則後：

1. — 使用瀏覽器從已配置的目標網路訪問網站（使主機不符合要求）。

2. — 監視分析>關聯>允許清單事件和分析>關聯>允許清單違規事件生成。

3. — 驗證主機不符合要求時是否填充了事件。

實驗室測試確認，一旦啟用網路發現，將為非合規主機成功生成Allow List Events和Allow List

Violations。

原因

根本原因是網路發現策略是在FMC關聯策略中生成允許清單事件的必備條件。如果沒有活動的網路發現策略，系統無法根據配置的Allow List正確評估主機合規性，從而導致目標網路主機變得不合規時不會生成Allow List Events。

相關內容

- Cisco FMC相關合規性清單檔案
- 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）。