在FMC中使用Packet Tracer工具重新運行資料包

目錄

簡介

本檔案介紹如何使用FMC GUI Packet Tracer工具在FTD裝置上重新執行封包。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower技術知識
- 瞭解透過防火牆的資料包流

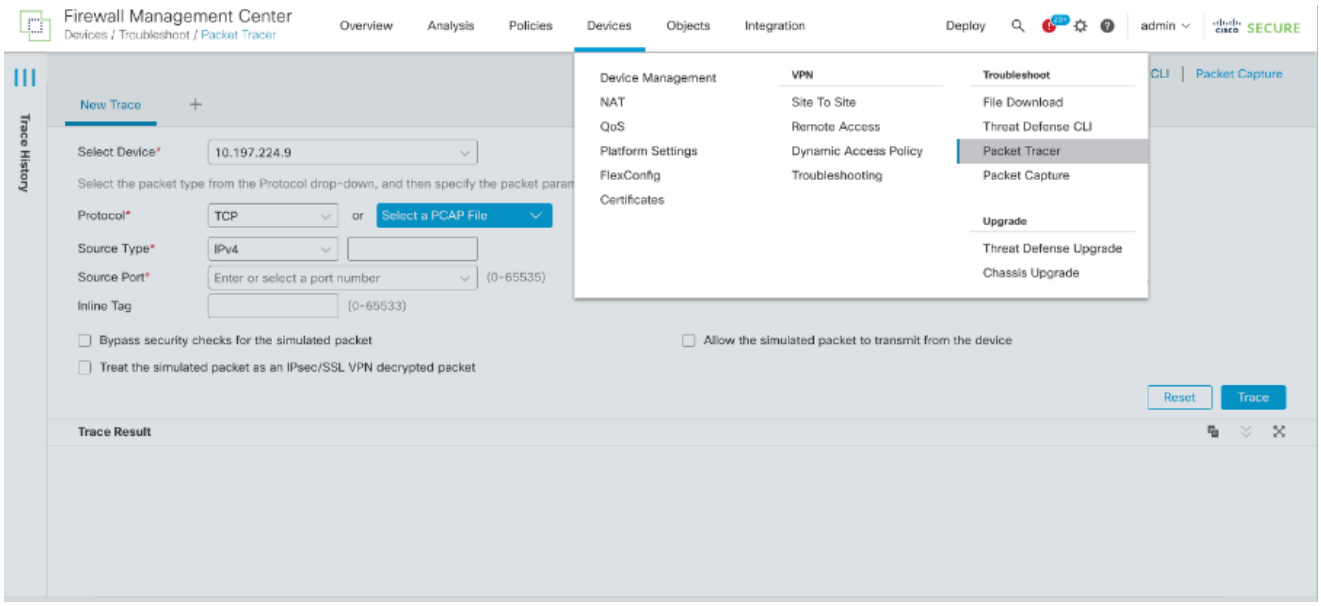
採用元件

- Cisco Secure Firewall Management Center (FMC)和Cisco Firewall Threat Defense (FTD) 7.1或更高版本。
- PCAP格式的資料包捕獲檔案

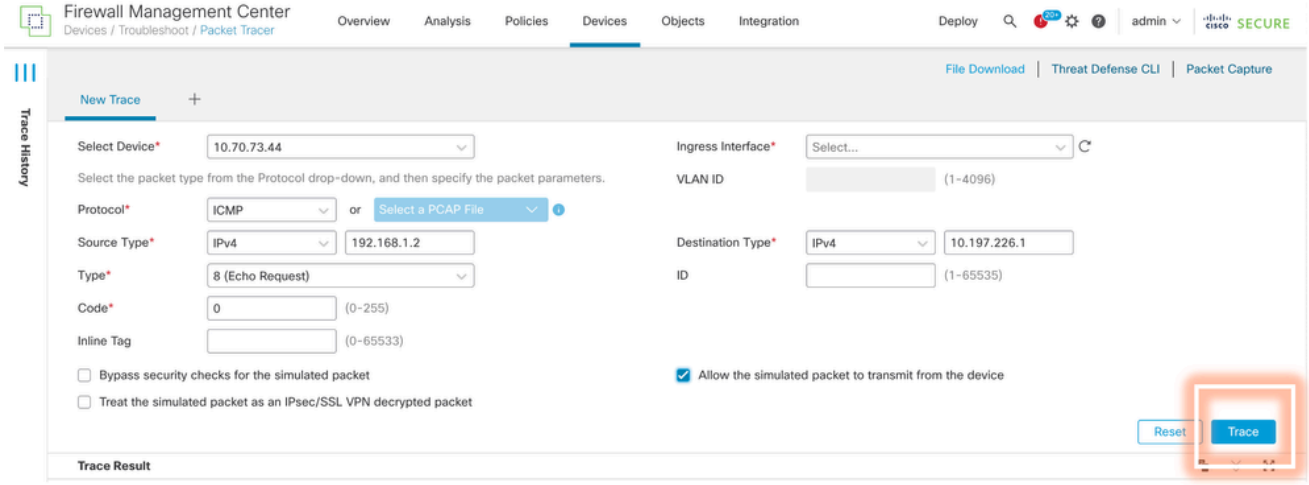
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

使用FMC中提供的Packet Tracer工具重新運行資料包

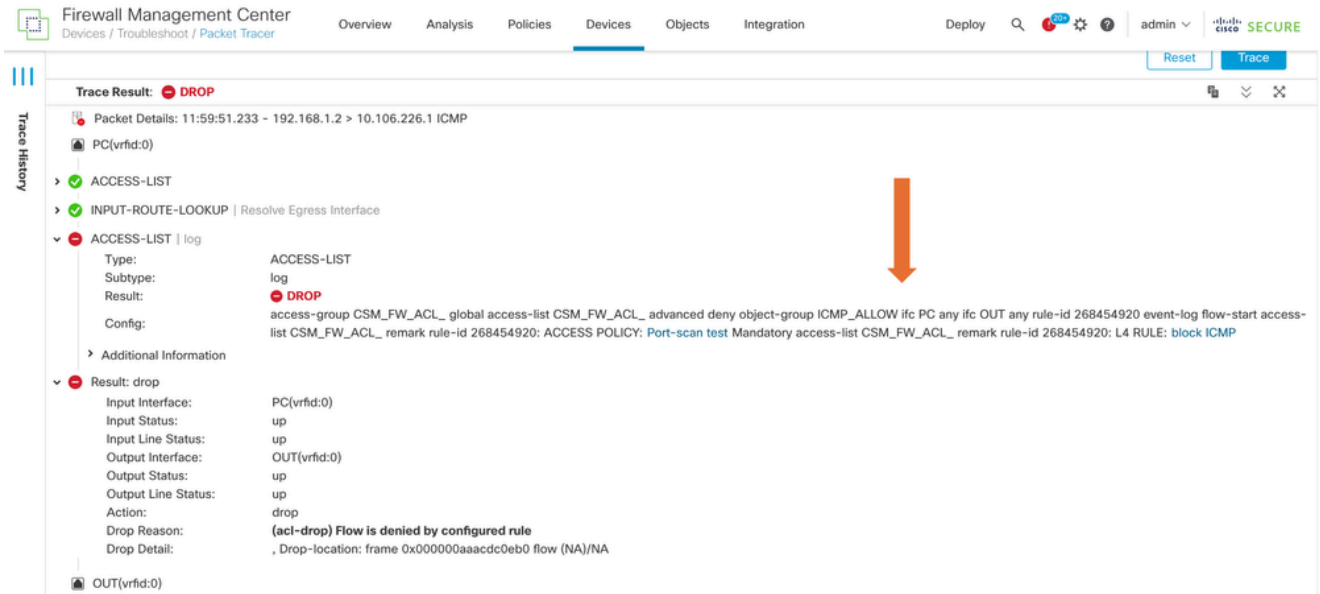
1. 登入FMC GUI。轉至Devices > Troubleshoot > Packet Tracer。



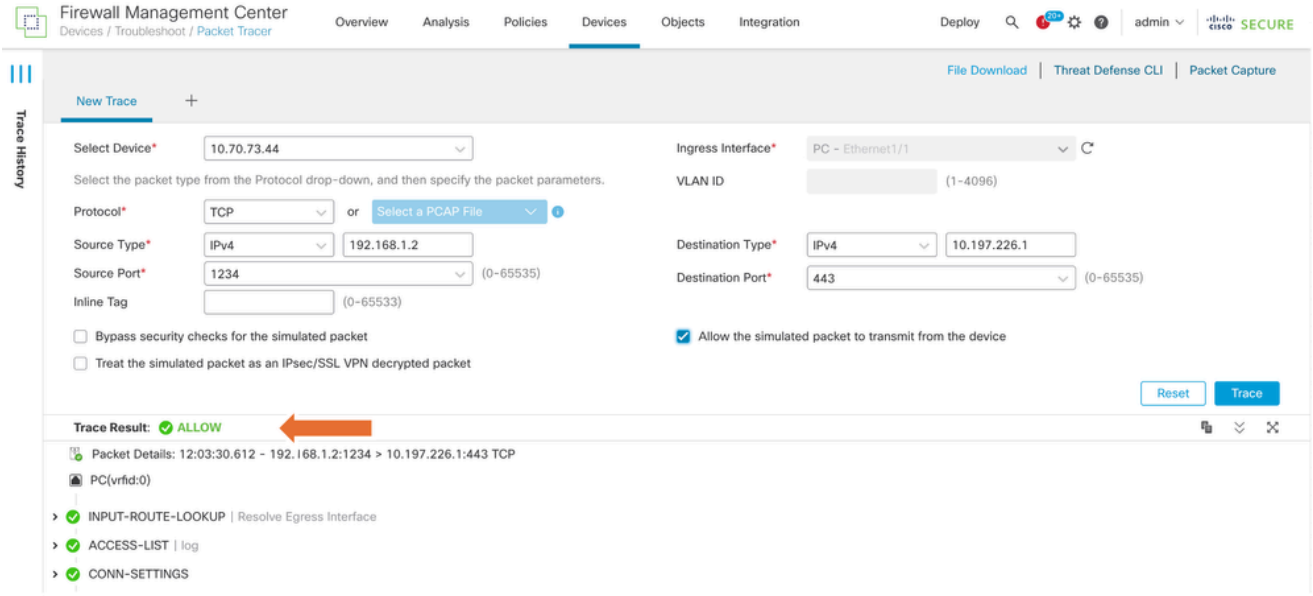
2. 提供源、目標、協定、入口介面的詳細資訊。按一下「追蹤」。



3. 使用Allow the simulated packet to transmit from the device選項，從裝置重新執行此資料包。
4. 請注意，資料包被丟棄，因為訪問控制策略中有已配置的丟棄ICMP資料包的規則。

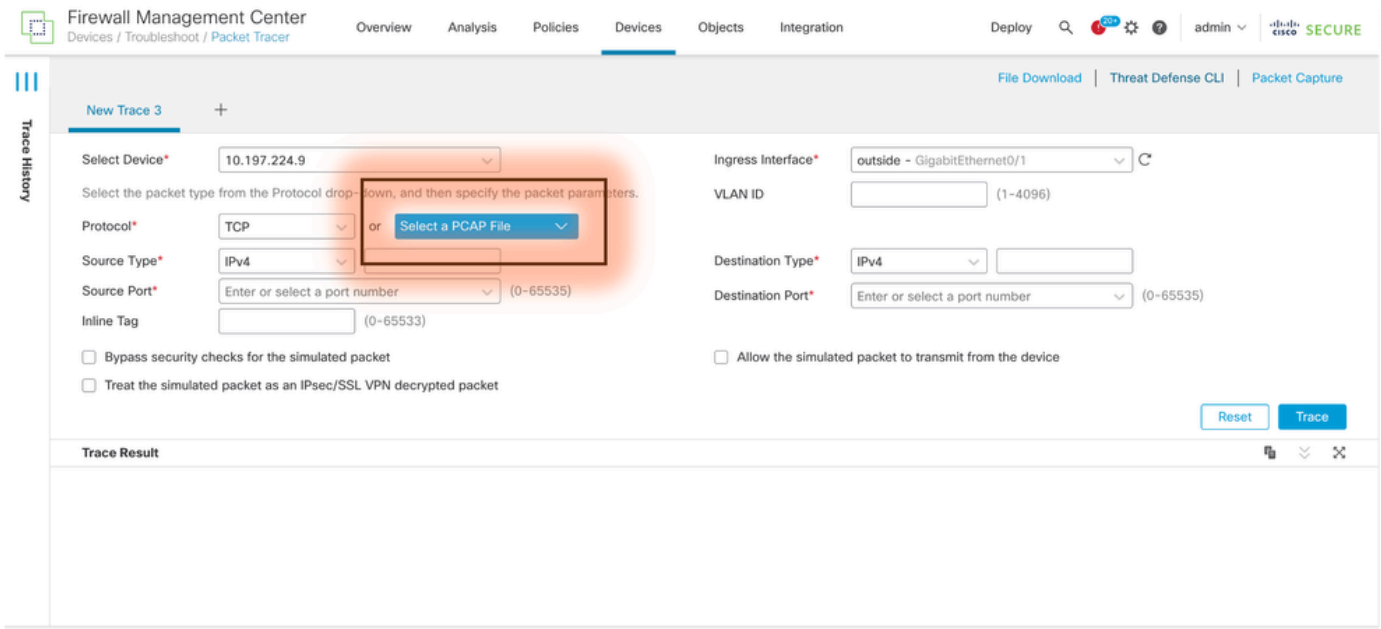


5. 使用TCP資料包的此Packet Tracer將獲得跟蹤的最終結果（如圖所示）。



使用PCAP檔案重新執行封包

您可以使用「選取PCAP檔案」按鈕來上傳pcap檔案。然後選擇Ingress介面並按一下Trace。

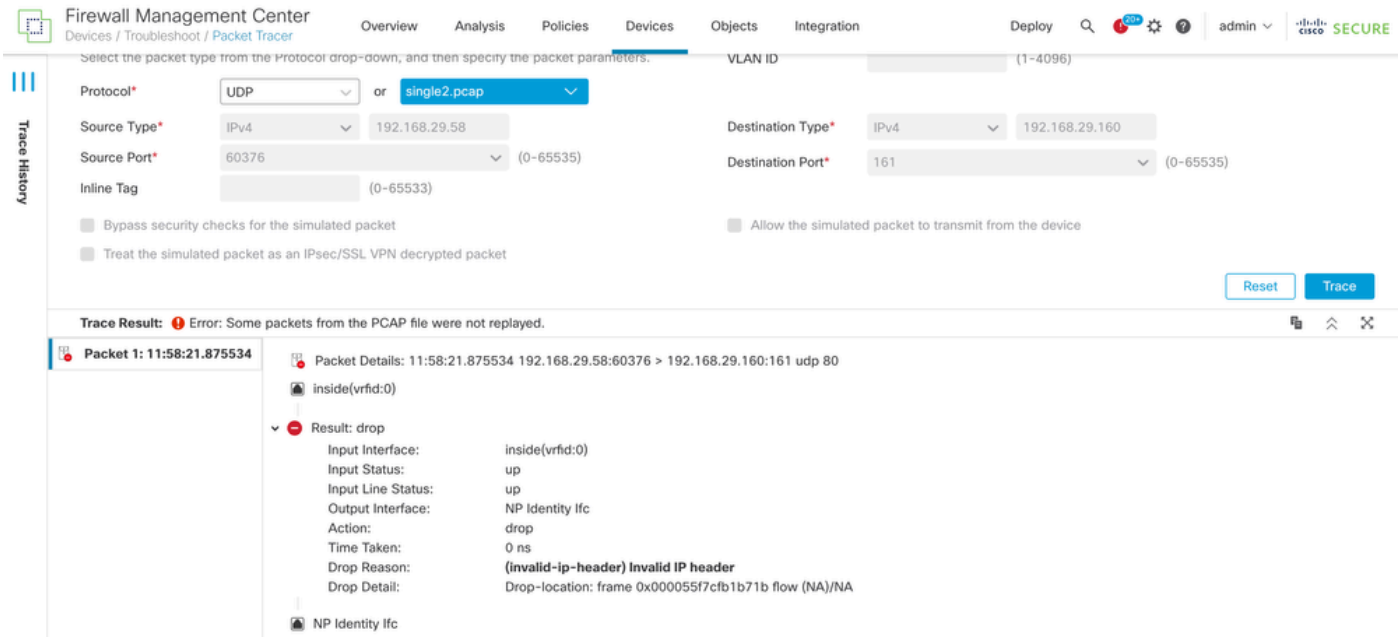


使用此選項的限制

1. 我們只能模擬TCP/UDP資料包。
2. PCAP檔案中支援的最大資料包數為100。
3. Pcap檔案大小必須小於1 MB。

4. PCAP檔案名稱不得超過64個字元（包括副檔名），且只能包含英數字元、特殊字元(「。」、「-」、「_」)或同時包含兩者。
5. 目前僅支援單一流量封包。

跟蹤3將丟棄原因顯示為無效IP報頭



相關檔案

有關資料包捕獲和跟蹤器的詳細資訊，請參閱Cisco Live文檔。

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）。