

在FMC中使用Packet Tracer工具重新運行資料包

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[使用FMC中提供的Packet Tracer工具重新運行資料包](#)

[使用PCAP檔案重新執行封包](#)

[使用此選項的限制](#)

[相關檔案](#)

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

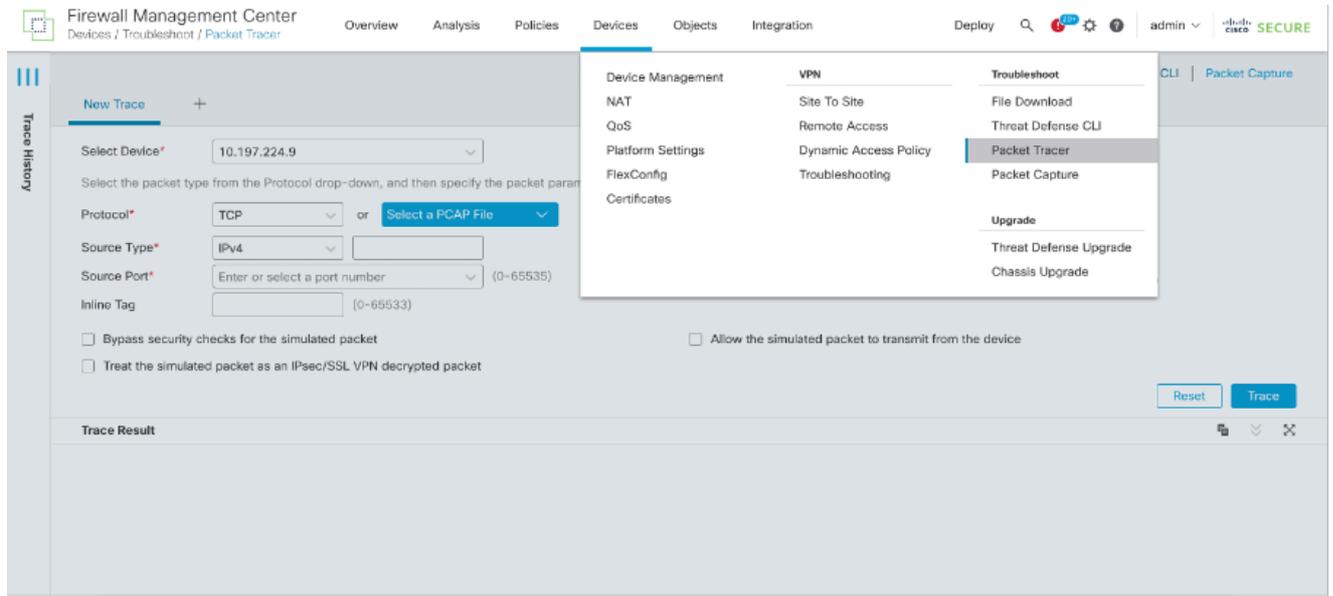
採用元件

- 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

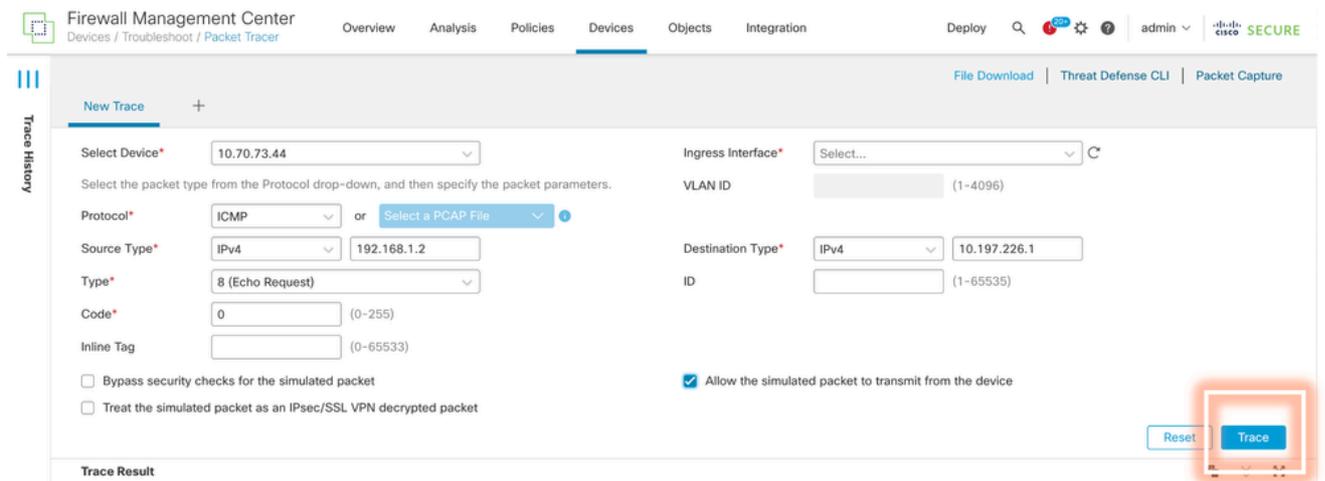
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

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。

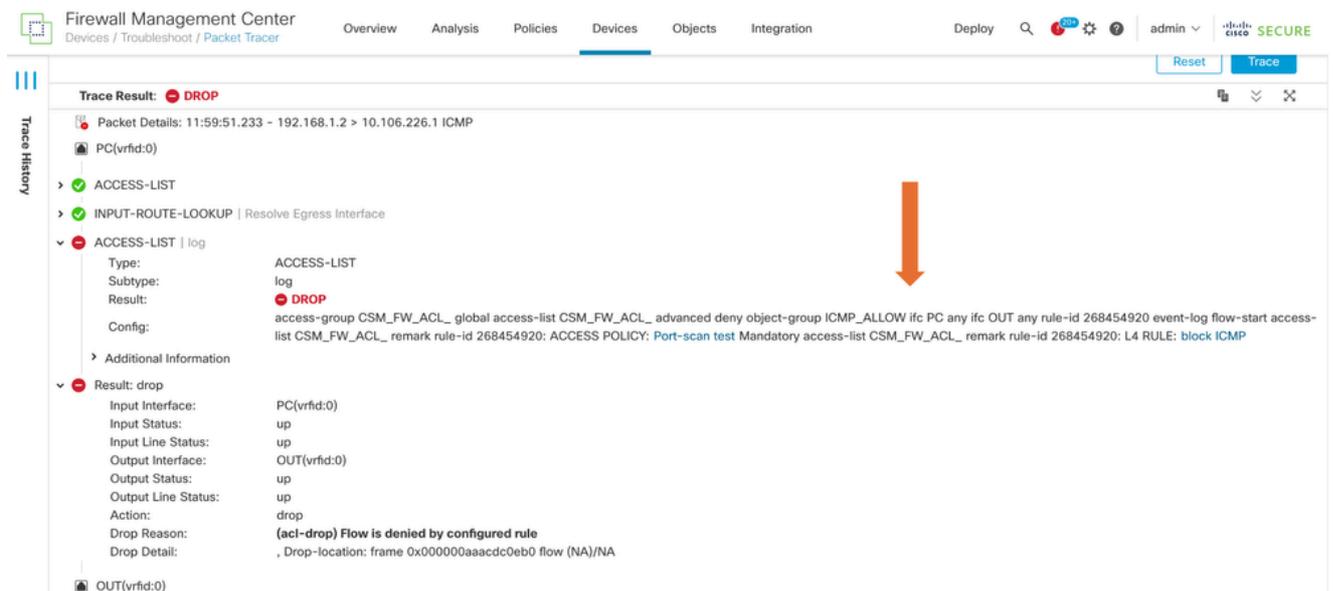


2. 提供源、目標、協定、入口介面的詳細資訊。按一下「追蹤」。



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）。

The screenshot shows the Firewall Management Center Packet Tracer interface. The 'New Trace' form is filled with the following details: Select Device: 10.70.73.44; Protocol: TCP; Source Type: IPv4, Source Port: 1234; Ingress Interface: PC - Ethernet1/1; Destination Type: IPv4, Destination Port: 443. The 'Trace Result' is 'ALLOW', indicated by a green checkmark and an orange arrow pointing to it. Below the result, the packet details are shown: 12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP. The trace steps are: INPUT-ROUTE-LOOKUP | Resolve Egress Interface, ACCESS-LIST | log, and CONN-SETTINGS.

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。

The screenshot shows the Firewall Management Center Packet Tracer interface. The 'New Trace 3' form is filled with the following details: Select Device: 10.197.224.9; Protocol: TCP; Source Type: IPv4; Ingress Interface: outside - GigabitEthernet0/1; Destination Type: IPv4. The 'Select a PCAP File' button is highlighted with a red box. The 'Trace Result' field is empty.

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

The screenshot shows the Cisco Firewall Management Center (FMC) Packet Tracer interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The main configuration area is for a packet trace, with fields for Protocol (UDP), Source Type (IPv4, 192.168.29.58), Source Port (60376), Destination Type (IPv4, 192.168.29.160), and Destination Port (161). The trace result shows an error: 'Error: Some packets from the PCAP file were not replayed.' The details for 'Packet 1: 11:58:21.875534' show it was dropped on the 'inside(vrfid:0)' interface. The drop reason is '(invalid-ip-header) Invalid IP header'.

Trace Result: ❗ Error: Some packets from the PCAP file were not replayed.

Packet 1: 11:58:21.875534

- Packet Details: 11:58:21.875534 192.168.29.58:60376 > 192.168.29.160:161 udp 80
- inside(vrfid:0)
- Result: drop
 - Input Interface: inside(vrfid:0)
 - Input Status: up
 - Input Line Status: up
 - Output Interface: NP Identity Ifc
 - Action: drop
 - Time Taken: 0 ns
 - Drop Reason: **(invalid-ip-header) Invalid IP header**
 - Drop Detail: Drop-location: frame 0x000055f7cfb1b71b flow (NA)/NA
- NP Identity Ifc

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）。