# FirePOWER管理中心以錯誤的方向顯示某些TCP連線事件

## 目錄



## 簡介

本文檔介紹FirePOWER管理中心(FMC)在反向顯示TCP連線事件的原因和緩解步驟，其中發起方IP是TCP連線的伺服器IP，響應方IP是TCP連線的客戶端IP。

> **附註**：發生此類事件的原因有多種。本文檔解釋了導致此症狀的最常見原因。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- FirePOWER技術
- 自適應安全裝置(ASA)基礎知識
- 對傳輸控制協定(TCP)計時機制的理解

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本6.0.1及更高版本的ASA Firepower威脅防禦(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- 運行軟體版本6.0.1及更高版本的ASA Firepower威脅防禦(5512-X、5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、FP9300、FP4100)
- ASA，包含運行軟體版本6.0.0及更高版本的Firepower模組(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X、5515-X、ASA 5525-X、ASA 5555-X、ASA 5585-X)
- Firepower管理中心(FMC)版本6.0.0及更高版本

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清除（預設）組

態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

# 背景

在TCP連線中，**client**是指傳送初始封包的IP。當受管裝置（感測器或FTD）看到連線的初始TCP資料包時，FirePOWER管理中心會生成連線事件。

跟蹤TCP連線狀態的裝置已定義**空閒超時**，以確保未被端點錯誤關閉的連線不會長時間消耗可用記憶體。FirePOWER上已建立TCP連線的預設空閒超時為**三分鐘**。FirePOWER IPS感測器不會跟蹤閒置三分鐘或更長時間的TCP連線。

超時後的後續資料包將視為新的TCP流，並根據與此資料包匹配的規則做出轉發決策。當資料包來自伺服器時，伺服器的IP將記錄為此新流的發起者。為規則啟用日誌記錄後，會在FirePOWER管理中心上生成連線事件。

> **附註**：根據配置的策略，超時後資料包的轉發決策與初始TCP資料包的決策不同。如果配置的預設操作為「Block」，則丟棄資料包。

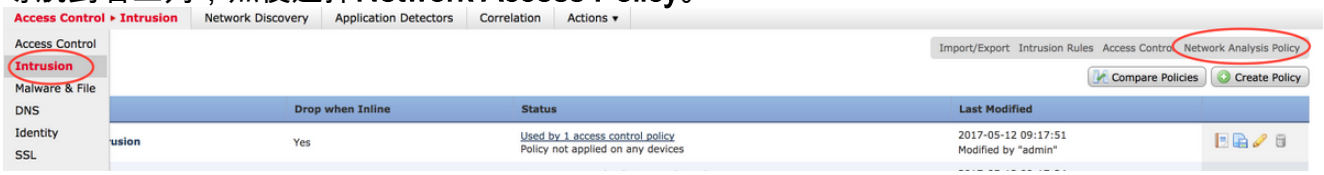
以下螢幕截圖顯示了此症狀：

| First Packet | Last Packet | Action | Reason | Initiator IP | Initiator Country | Responder IP | Responder Country | Ingress Security Zone | Egress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2017-05-12 17:48:05 | | Block | | 10.32.38.30 | | 192.168.38.30 | | | | 443 (https) / tcp | 44705 / tcp |
| 2017-05-12 17:39:13 | | Allow | | 192.168.38.30 | | 10.32.38.30 | | | | 44705 / tcp | 443 (https) / tcp |

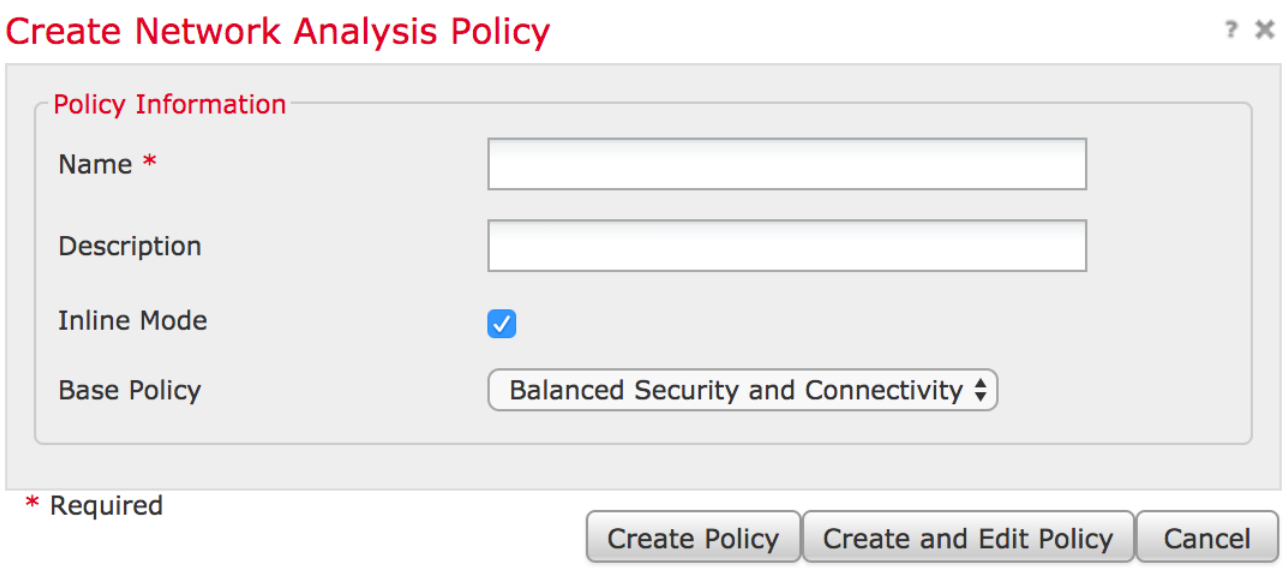
# 解決方案

通過增加TCP連線的**超時**可以緩解上述問題。若要變更逾時，

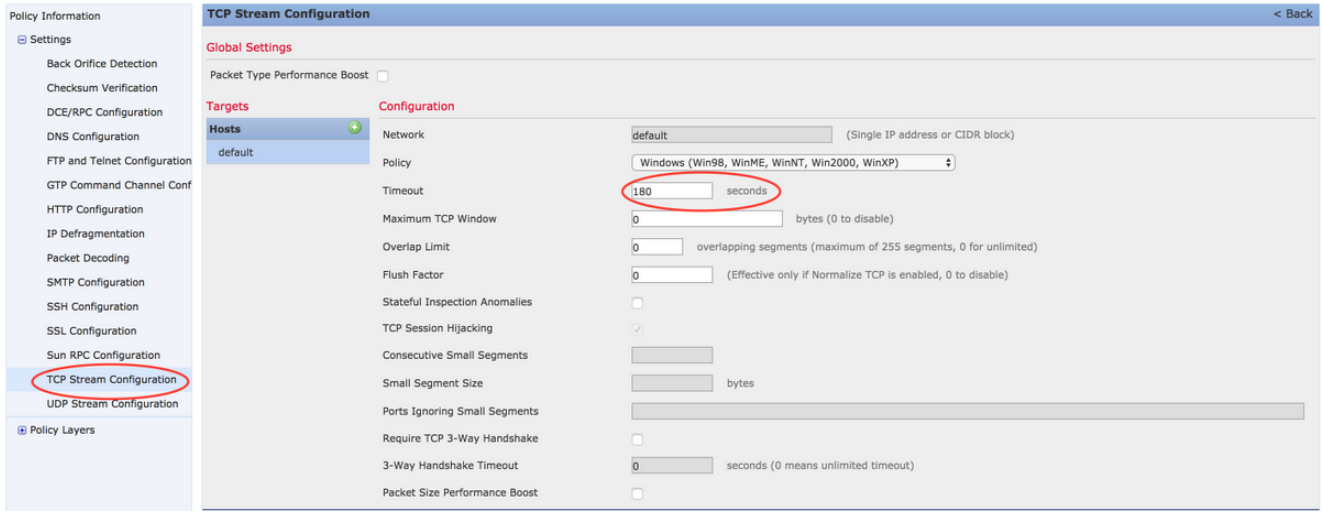
1. 導航到**Policies > Access Control > Intrusion**。
2. 導航到右上角，然後選擇**Network Access Policy**。



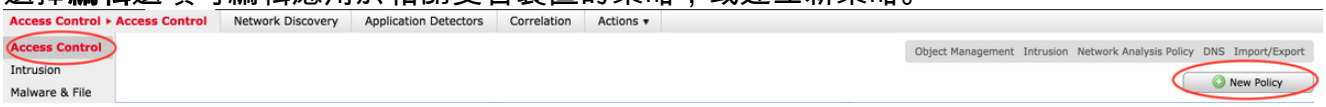

3. 選擇**Create Policy**，選擇一個名稱，然後按一下**Create and Edit Policy**。請勿修改基**本策略。**



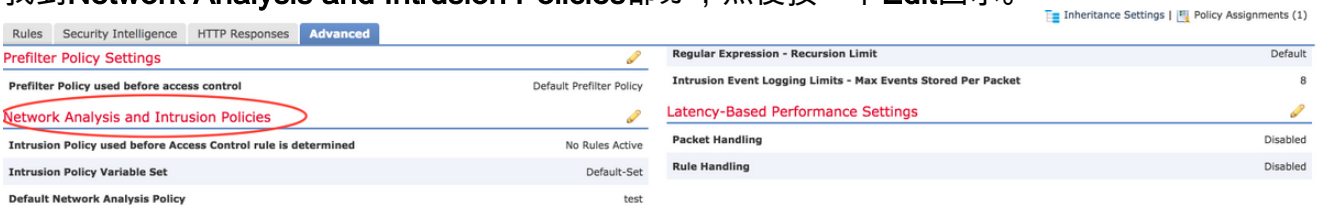

4. 展開**Settings**選項，然後選擇**TCP Stream Configuration**。
5. 導航到配置部分，然後根據需要更改**Timeout**的值。




6. 導覽至**Policies > Access Control > Access Control**。
7. 選擇**編輯**選項可編輯應用於相關受管裝置的策略，或建立新策略。




8. 在Access策略中選擇**Advanced**頁籤。
9. 找到**Network Analysis and Intrusion Policies**部分，然後按一下**Edit**圖示。




10. 從**Default Network Analysis Policy**的下拉選單中，選擇在步驟2中建立的策略。
11. 按一下「**OK**」，然後「**Save**」變更內容。
12. 按一下**Deploy**選項將策略部署到相關的受管裝置。

**注意**：增加超時預計會導致記憶體利用率提高，FirePOWER必須跟蹤端點在較長時間內未關閉的流。每個唯一網路的記憶體利用率實際增長情況不同，因為它取決於網路應用程式使TCP連線保持空閒的時間。

## 結論

每個網路的TCP連線空閒超時基準都不同。它完全取決於正在使用的應用程式。通過觀察網路應用程式使TCP連線空閒的時間長短，必須建立一個最佳值。對於與思科ASA上的FirePOWER服務模組相關的問題，當無法推斷最佳值時，可以通過將超時值逐步增加到ASA超時值來調整超時。

## 相關資訊

- 適用於ASA的Cisco Firepower威脅防禦快速入門手冊
- 技術支援與文件 - Cisco Systems
- ASA Firepower快速入門手冊