使用Web使用者介面下載資料包資料（PCAP檔案）

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[下載PCAP檔案的步驟](#)

簡介

使用Web使用者介面可以下載觸發Snort規則的資料包。本文提供使用Sourcefire FireSIGHT管理系統的Web使用者介面下載資料包捕獲資料（PCAP檔案）的步驟。

必要條件

需求

思科建議您瞭解Sourcefire FirePOWER裝置和虛擬裝置模型。

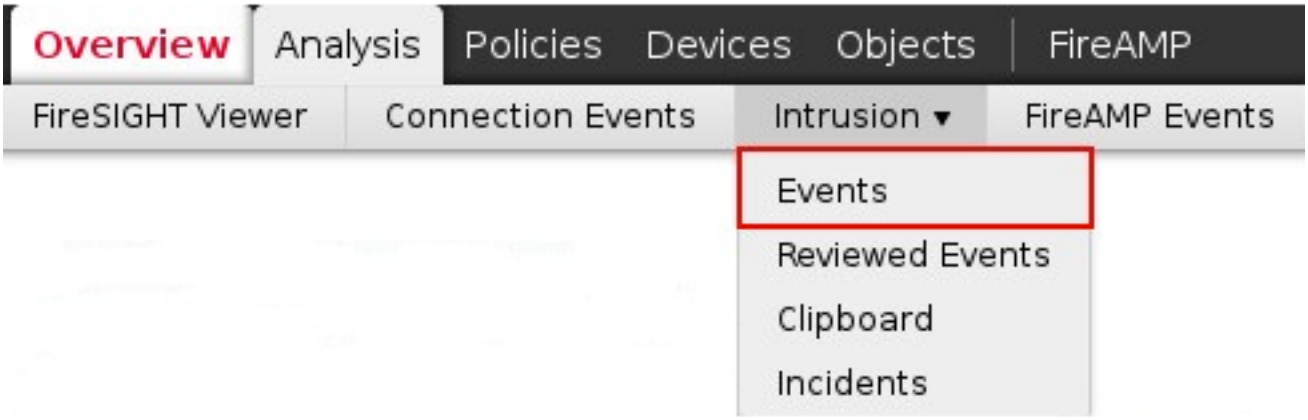
採用元件

本文檔中的資訊基於運行軟體版本5.2或更高版本的Sourcefire FireSIGHT管理中心（也稱為Defense Center）。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

下載PCAP檔案的步驟

第1步：登入到Sourcefire防禦中心或管理中心，然後導航到「入侵事件」頁面，如下所示：



第2步：使用覈取方塊，選擇要下載資料包捕獲資料（PCAP檔案）的事件。

步驟3:滾動到頁面底部，並執行以下操作：

- 點選Download Packet下載觸發選定入侵事件的資料包
- 點選Download All Packets，下載當前受約束檢視中觸發入侵事件的所有資料包

附註：下載的資料包將儲存為PCAP。 如果要分析資料包捕獲，您需要下載並安裝能夠讀取PCAP檔案的軟體。

第4步：出現提示時，將PCAP檔案儲存到您的硬碟。