

使用「1秒效能監視器」選項收集效能統計資訊

目錄

[簡介](#)

[1秒效能監控器](#)

[在5.4版或更高版本上啟用](#)

[在5.4之前的版本上啟用](#)

[相關檔案](#)

簡介

在運行Sourcefire軟體的裝置上，您可以配置用於監控和報告其自身效能的基本引數。效能統計資訊對於解決運行Snort的裝置上的效能相關問題至關重要。本文檔提供使用FireSIGHT管理中心啟用此功能的步驟。

警告：如果您的網路處於活動狀態，並且您在生產系統上啟用了1秒效能，這可能會影響網路效能。只有在思科技術支援出於故障排除目的而提出此請求時，您才應啟用此功能。

注意：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。

1秒效能監控器

1秒效能監視器功能允許您通過配置以下內容來指定系統更新裝置效能統計資訊的時間間隔：

- 秒數
- 分析的資料包數

自上次效能統計資訊更新後，指定的秒數已過時，系統將驗證指定的資料包數是否已進行分析。如果是，系統會更新效能統計資訊。如果不是，系統會等待分析指定數量的資料包。

在5.4版或更高版本上啟用

第1步：選擇Policies > Access Control。系統將顯示Access Control Policy頁面。

第2步：按一下要編輯的訪問控制策略旁邊的鉛筆圖示。

步驟3:選擇Advanced頁籤。系統將顯示access control policy advanced settings頁面。

Default Access Control

Enter a description

Rules Targets Security Intelligence HTTP Responses **Advanced**

第4步：按一下效能設定旁邊的鉛筆圖示。

Performance Settings 	
Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default
Regular Expression - Recursion Limit	Default
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

第5步：在顯示的彈出視窗中選擇Performance Statistics頁籤。如上所述修改取樣時間或最小資料包數。

Performance Settings ? ×

Pattern Matching Limits	Performance Statistics	Regular Expression Limits	Intrusion Event Logging Limits
Sample time (seconds)	<input type="text" value="300"/>		
Minimum number of packets	<input type="text" value="10000"/>		

Troubleshooting Options ▼

Revert to Defaults OK Cancel

第6步：或者，展開Troubleshoot Options部分，並僅在思科TAC要求的情況下修改這些選項。

第7步：按一下「OK」（確定）。

第8步：必須儲存並應用訪問控制策略，更改才能生效。

在5.4之前的版本上啟用

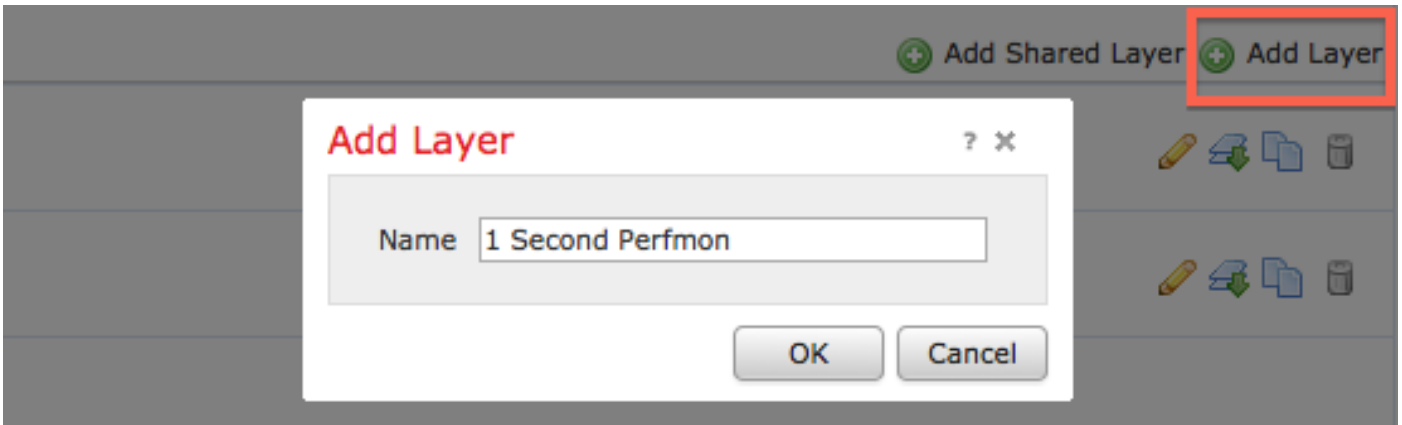
第1步：導航到Intrusion Policy頁面。登入到FireSIGHT管理中心。導航到Policies > Intrusion > Intrusion Policy。

第2步：編輯要應用的入侵策略。按一下pencil圖示編輯策略。

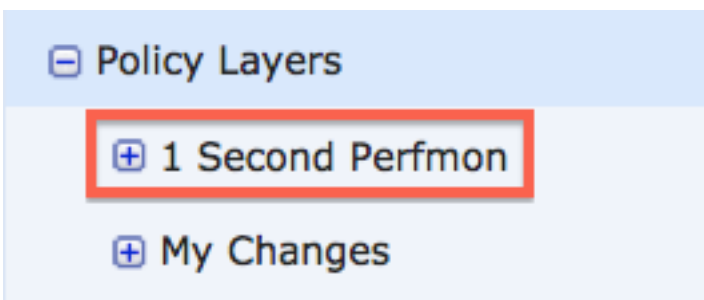


附註：由於此高級設定的設計原因，您只能在用作訪問控制策略的預設操作的入侵策略中修改此配置。

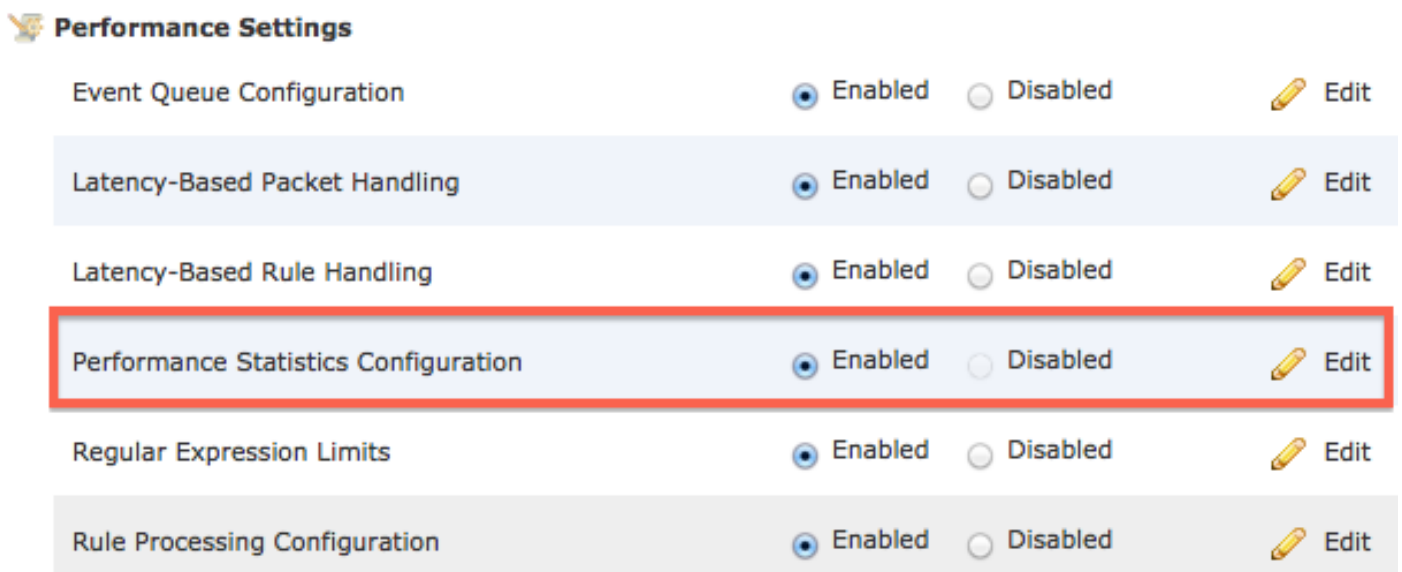
步驟3:新增策略層。按一下**Policy Layers**，然後按一下**Add Layer**。將層命名為「1秒Perfmon」。



檢查左側面板中的**Policy Layers**，並確保新的層「1 Second Perfmon」位於所有其他層之上。



第4步：啟用效能統計資訊配置。在**Performance Settings**下，選擇**Performance Statistics Configuration**旁邊的單選按鈕**Enabled**，然後按一下**Edit**。



第5步：將預設取樣時間修改為1秒，將最小資料包數修改為100個資料包。

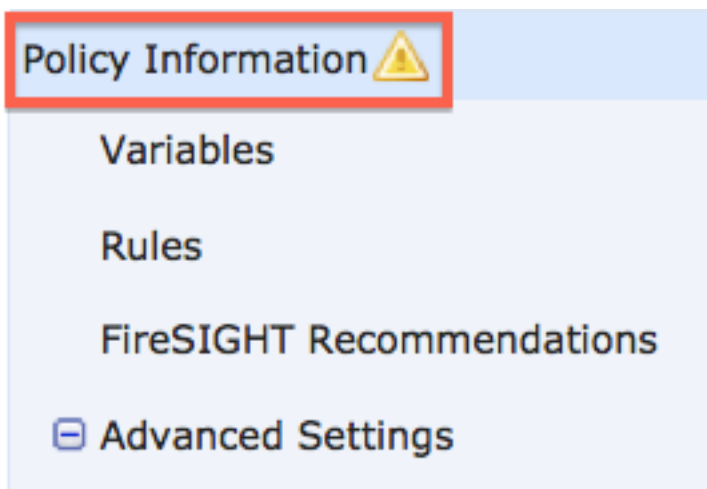
Performance Statistics Configuration

Settings

Sample time seconds

Minimum number of packets

第6步：按一下左側面板中的Policy Information，提交更改，然後將更新的策略應用到您要分析的裝置。



第7步：收集資料後恢復設定。要恢復，只需刪除「1秒Perfmon」策略層。

注意：不要忘記恢復配置。否則可能會導致效能問題。

相關檔案

- [檢視入侵事件效能](#)
- [生成入侵事件效能統計圖表](#)