

# 配置FireSIGHT系統以將警報傳送到外部系統日誌伺服器

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[傳送入侵警報](#)

[傳送運行狀況警報](#)

[第1部分：建立系統日誌警報](#)

[第2部分：建立運行狀況監視器警報](#)

[傳送影響標誌、發現事件和惡意軟體警報](#)

## 簡介

儘管FireSIGHT系統在其Web介面內提供了各種事件檢視，但您可能希望配置外部事件通知以促進對關鍵系統的持續監控。您可以將FireSIGHT系統配置為生成警報，在生成以下任一警報時通過電子郵件、SNMP陷阱或系統日誌通知您。本文描述如何配置FireSIGHT管理中心以在外部系統日誌伺服器上傳送警報。

## 必要條件

### 需求

思科建議您瞭解系統日誌和FireSIGHT管理中心。此外，防火牆中必須允許系統日誌埠（預設為514）。

### 採用元件

本檔案中的資訊是根據軟體版本5.2或更新版本。

**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，並使用已清除（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。

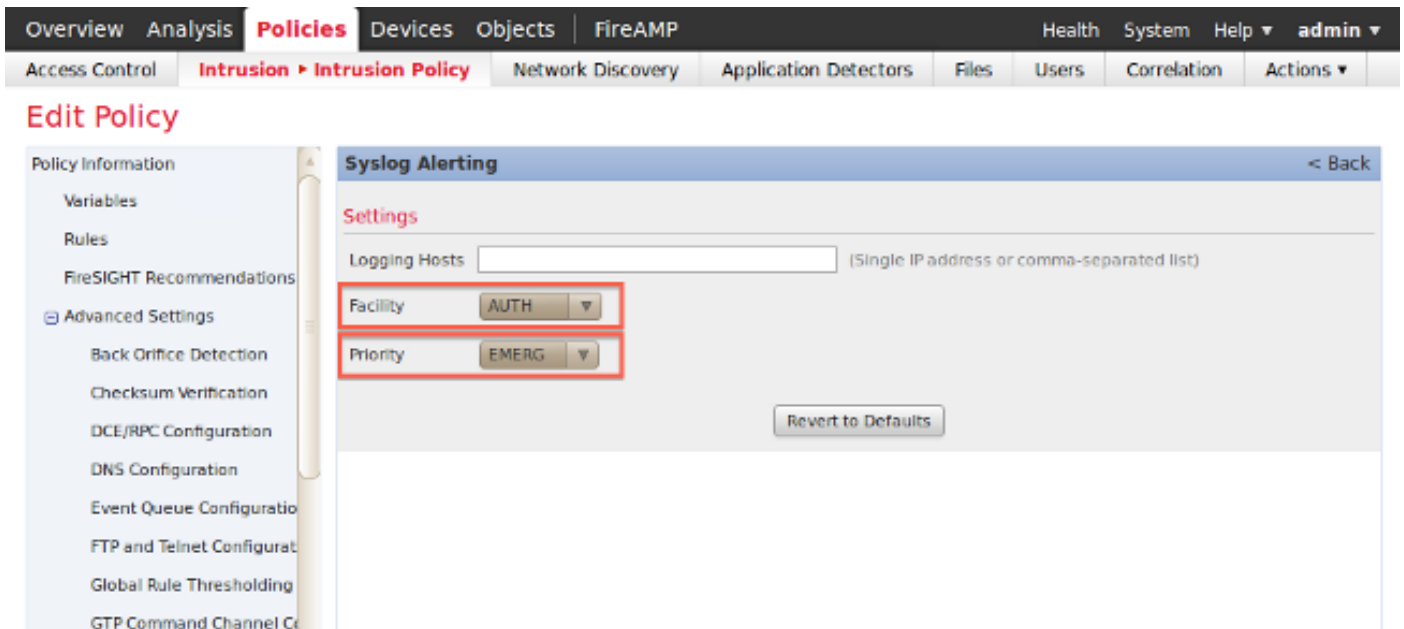
## 傳送入侵警報

- 1.登入到FireSIGHT管理中心的Web使用者介面。
- 2.導航至Policies > Intrusion > Intrusion Policy。
- 3.按一下要應用的策略旁邊的編輯。
- 4.按一下Advanced Settings。
- 5.在清單中找到Syslog Alerting，並將其設定為Enabled。

The screenshot shows the 'Edit Policy' page in the FireSIGHT web interface. The breadcrumb navigation is 'Policies > Intrusion > Intrusion Policy'. The left sidebar contains 'Policy Information' with sub-items: Variables, Rules, FireSIGHT Recommendations, Advanced Settings (selected), and Policy Layers. The main content area is titled 'Advanced Settings' and includes a '< Back' link. It is divided into two sections: 'Performance Settings' and 'External Responses'. Under 'Performance Settings', there are six rows, each with a configuration name, radio buttons for 'Enabled' or 'Disabled', and an 'Edit' icon. Under 'External Responses', there are two rows: 'SNMP Alerting' and 'Syslog Alerting'. The 'Syslog Alerting' row is highlighted with a red box, and a red arrow points to it from the 'Advanced Settings' link in the sidebar.

Section	Configuration	Enabled	Disabled	Action
Performance Settings	Event Queue Configuration	<input checked="" type="radio"/>	<input type="radio"/>	Edit
	Latency-Based Packet Handling	<input type="radio"/>	<input checked="" type="radio"/>	
	Latency-Based Rule Handling	<input type="radio"/>	<input checked="" type="radio"/>	
	Performance Statistics Configuration	<input checked="" type="radio"/>	<input type="radio"/>	Edit
	Regular Expression Limits	<input checked="" type="radio"/>	<input type="radio"/>	Edit
	Rule Processing Configuration	<input checked="" type="radio"/>	<input type="radio"/>	Edit
External Responses	SNMP Alerting	<input type="radio"/>	<input checked="" type="radio"/>	
	Syslog Alerting	<input checked="" type="radio"/>	<input type="radio"/>	Edit

- 6.按一下Syslog Alerting右側的Edit。
- 7.在Logging Hosts欄位中鍵入系統日誌伺服器的IP地址。
- 8.從下拉選單中選擇適當的Facility和Severity。除非將系統日誌伺服器配置為接受特定設施或嚴重性的警報，否則可以將這些警報保留為預設值。



9. 按一下此螢幕左上角附近的**Policy Information**。

10. 按一下**Commit Changes**按鈕。

11. 重新應用入侵策略。

**附註：**為了生成警報，請在訪問控制規則中使用此入侵策略。如果未配置訪問控制規則，則將此入侵策略設定為用作訪問控制策略的預設操作，然後重新應用訪問控制策略。

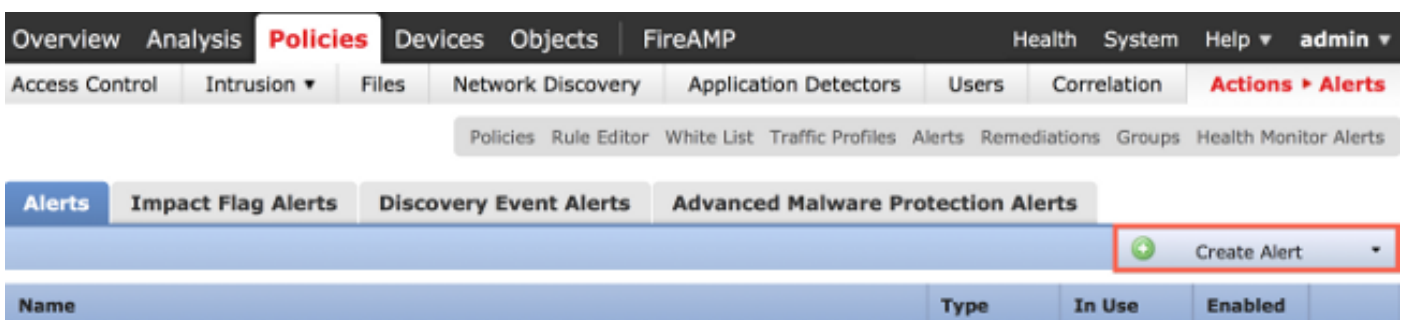
現在，如果在該策略上觸發了入侵事件，則還會向在入侵策略上配置的系統日誌伺服器傳送警報。

## 傳送運行狀況警報

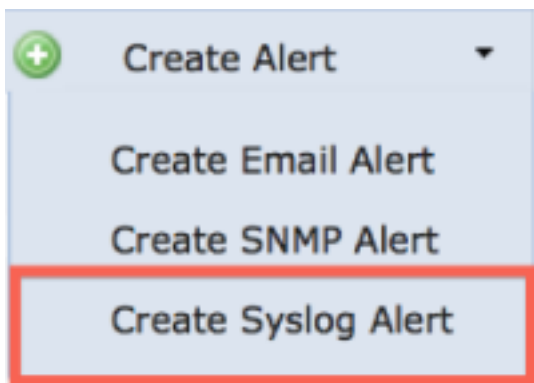
### 第1部分： 建立系統日誌警報

1. 登入到FireSIGHT管理中心的Web使用者介面。

2. 定位至**策略>操作>預警**。



3. 選擇Web介面右側的**Create Alert**。



4. 按一下**Create Syslog Alert**。系統將顯示配置彈出視窗。
5. 提供預警的名稱。
6. 在**主機**欄位中填寫系統日誌伺服器的IP地址。
7. 如果需要，更改系統日誌伺服器的埠（預設埠為514）。
8. 選擇適當的**Facility**和**Severity**。



### Create Syslog Alert Configuration

? X

Name	<input type="text"/>
Host	<input type="text"/>
Port	514
Facility	ALERT
Severity	ALERT
Tag	<input type="text"/>

Save Cancel

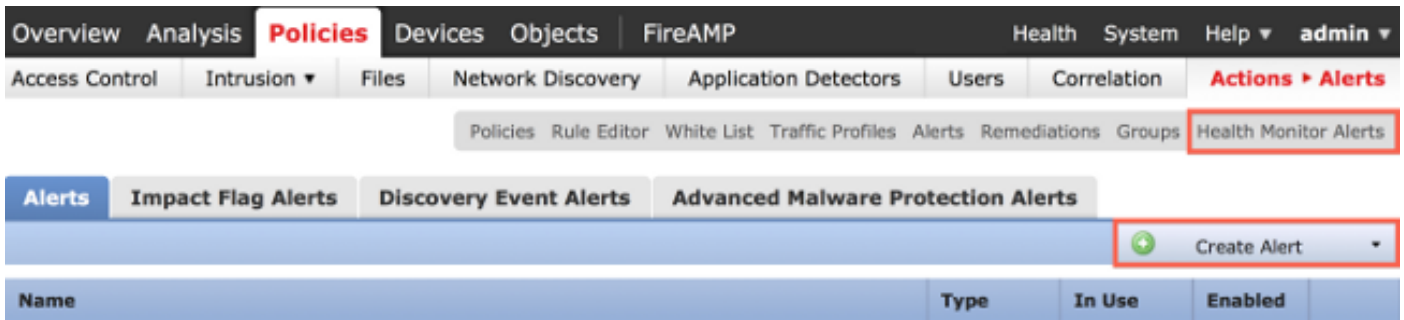
9. 按一下**Save**按鈕。您將返回Policies > Actions > Alerts頁。
10. 啟用系統日誌配置。

Type	In Use	Enabled	
Syslog	In Use	<input checked="" type="checkbox"/>	 

## 第2部分： 建立運行狀況監視器警報

以下說明描述了配置健康監控警報的步驟，該警報使用您剛剛建立的系統日誌警報（在上一節中）：

1. 轉至 **Policies > Actions > Alerts** 頁，然後選擇 **Health Monitor Alerts**，該頁位於頁面頂部。



2. 為健康警報命名。

3. 選擇 **Severity**（按住CTRL鍵的同時按一下可用來選擇多個嚴重性型別）。

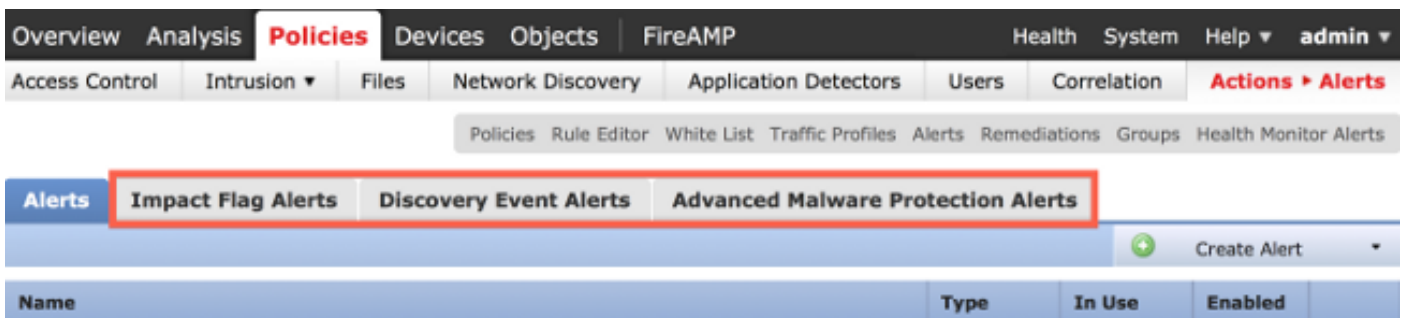
4. 在 **Module** 列中，選擇要向其傳送警報的系統日誌伺服器的運行狀況模組（例如，磁碟使用情況）。

5. 從 **Alerts** 列中選擇以前建立的syslog警報。

6. 按一下 **Save** 按鈕。

## 傳送影響標誌、發現事件和惡意軟體警報

您還可以配置FireSIGHT管理中心，以便針對具有特定影響標誌、特定型別的發現事件和惡意軟體事件的事件傳送系統日誌警報。為此，您必須執行[第1部分：建立系統日誌警報](#)，然後配置要傳送到系統日誌伺服器的事件型別。為此，您可以導航到 **Policies > Actions > Alerts** 頁，然後選擇所需警報型別的頁籤。



## 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）。