Cisco FireSIGHT系統上的自定義本地Snort規則

目錄

簡介

FireSIGHT系統上的自定義本地規則是自定義標準Snort規則，可從本地電腦以ASCII文本檔案格式匯入。FireSIGHT系統允許您使用Web介面匯入本地規則。匯入本地規則的步驟非常簡單。但是，要編寫最佳本地規則，使用者需要深入瞭解Snort和網路協定。

本文檔旨在向您提供一些提示和幫助，以便編寫自定義本地規則。有關建立本地規則的說明，請參閱*Snort使用者手冊*，該手冊位於snort.org。思科建議您先下載並閱讀《使用者手冊》，然後再編寫自定義本地規則。

> **附註**：Sourcefire規則更新(SRU)包中提供的規則由Cisco Talos安全情報和研究組建立和測試，並受思科技術支援中心(TAC)支援。 Cisco TAC不提供編寫或調整自定義本地規則的幫助，但是，如果您在FireSIGHT系統的規則匯入功能方面遇到任何問題，請與Cisco TAC聯絡。

> **警告：**編寫不當的自定義本地規則可能會影響FireSIGHT系統的效能，從而導致整個網路的效能下降。如果您的網路中遇到任何效能問題，且您的FireSIGHT系統上啟用了一些自訂本機Snort規則，思科建議您停用這些本機規則。

必要條件

需求

思科建議您瞭解Snort規則和FireSIGHT系統。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- FireSIGHT管理中心（也稱為防禦中心）
- 軟體版本5.2或更高版本

使用自定義本地規則

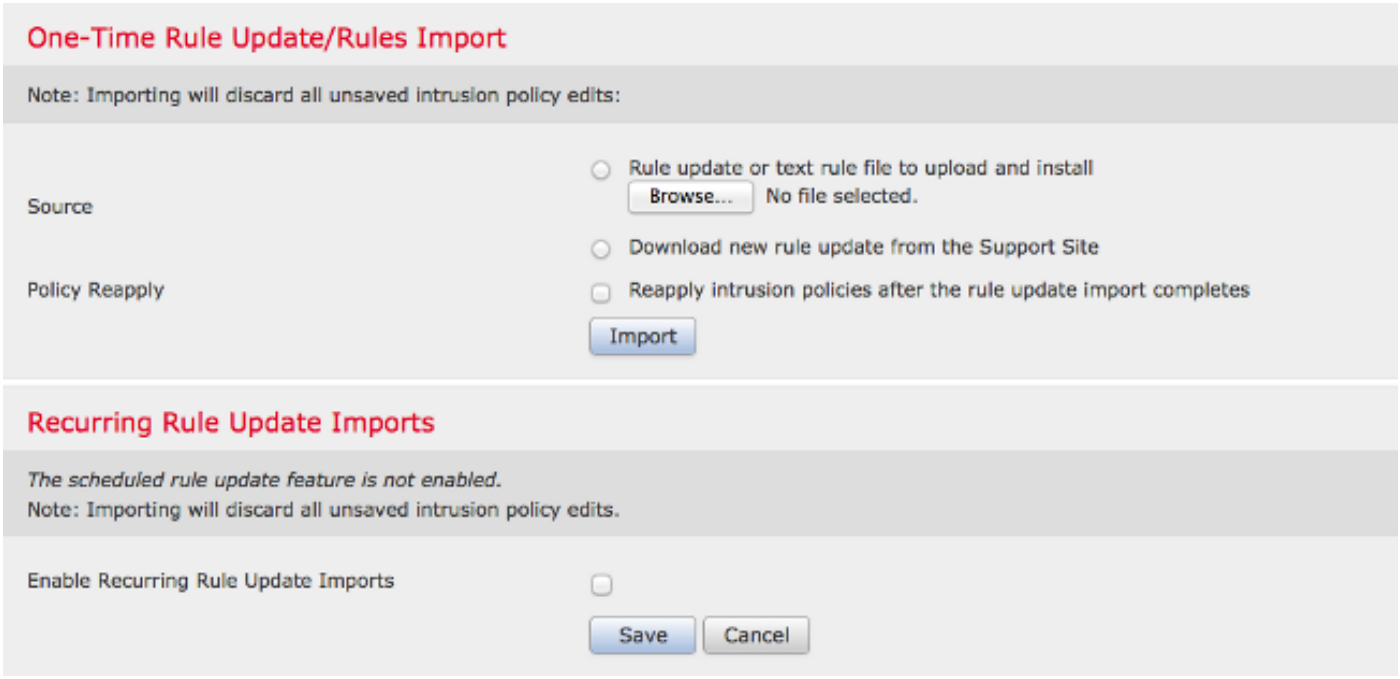
匯入本地規則

開始之前，必須確保檔案中的規則不包含任何跳脫字元。規則匯入程式要求使用ASCII或UTF-8編碼匯入所有自定義規則。

以下步驟說明如何從本地電腦匯入本地標準文本規則：

1.導航到**Policies > Intrusion > Rule Editor**，即可訪問「**Rule Editor**」頁。

2.按一下**匯入規則**。系統將顯示**Rule Updates**頁面。



圖：Rule Updates頁面的螢幕截圖

3.選擇**Rule update or text rule file to upload and install**，然後按一下**Browse**選擇規則檔案。

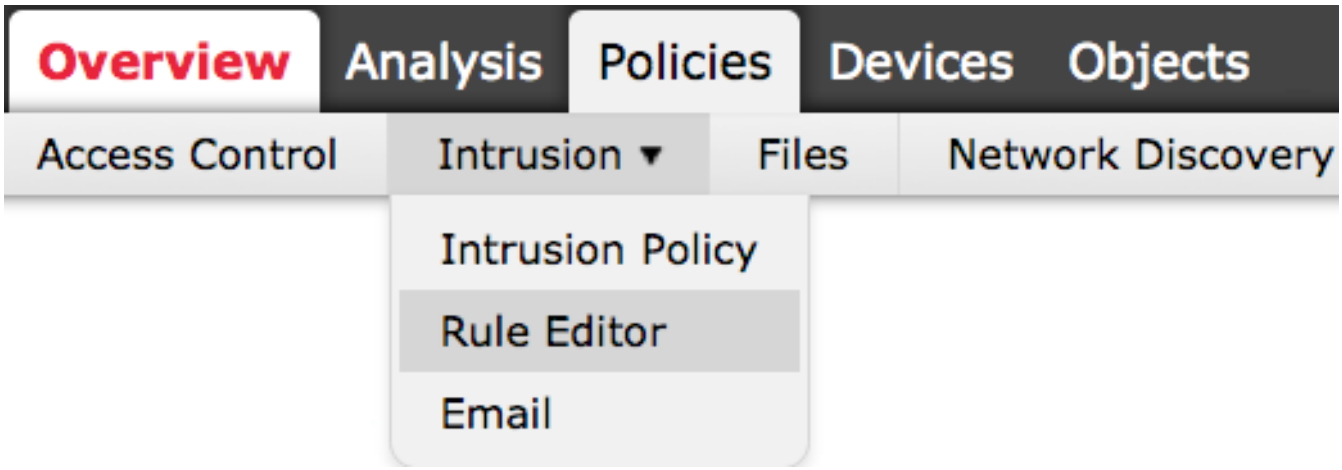
附註：所有上載的規則都儲存在本**地規則**類別。

4.按一下**匯入**。規則檔案被匯入。

注意：FireSIGHT系統不使用新規則集進行檢查。要啟用本地規則，需要在入侵策略中啟用該規則，然後應用該策略。

檢視本地規則

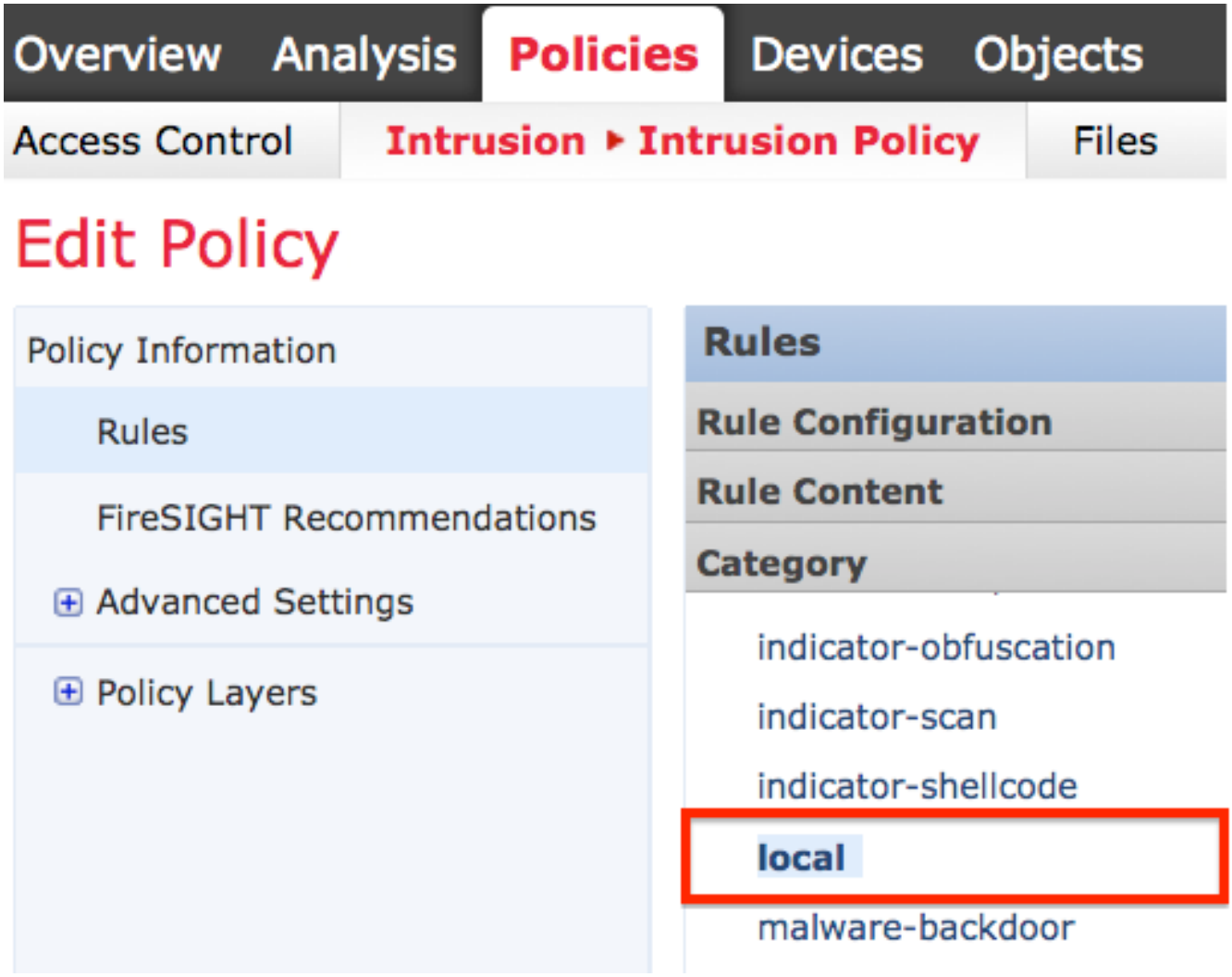
- 要檢視當前本地規則的修訂版號，請導航到**Rule Editor**頁面(**Policies > Intrusion > Rule Editor**)。



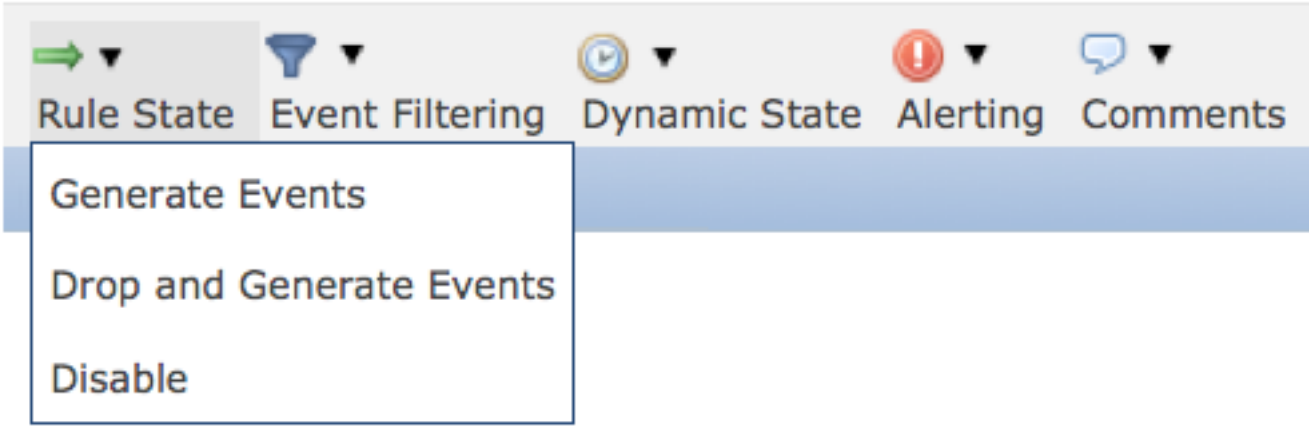
- 在「規則編輯器」(Rule Editor)頁面中，按一下**Local Rule**類別以展開資料夾，然後按一下規則旁邊的**Edit**。
- 所有匯入的本地規則將自動儲存在**本地規則**類別。

啟用本地規則

- 預設情況下，FireSIGHT系統將本地規則設定為禁用狀態。必須先手動設定本地規則的狀態，然後才能在入侵策略中使用它們。
- 若要啟用本地規則，請導航到Policy Editor頁面(**Policies > Intrusion > Intrusion Policy**)。 在左側面板中選擇**Rules**。在**Category**下，選擇**local**。如果可用，應顯示所有本地規則。



- 選擇所需的本地規則後，選擇規則的狀態。



- 選擇規則狀態後，按一下左側面板上的**Policy Information**選項。選擇**Commit Changes**按鈕。入侵策略已驗證。

附註：如果啟用匯入的本地規則（該規則將precated threshold關鍵字與入侵策略中的入侵事件閾值功能結合使用），則策略驗證將失敗。

檢視已刪除的本地規則

- 所有已刪除的本地規則都將從本地規則類別移動到已刪除的規則類別。

- 要檢視已刪除的本地規則的修訂版號，請轉到**規則編輯器**頁，按一下**deleted**類別展開資料夾，然後按一下*鉛筆*圖示在**規則編輯器**頁中檢視規則的詳細資訊。

本地規則編號

- 不必指定生成器(GID);如果指定，則只能為標準文本規則指定GID 1，為敏感資料規則指定138。
- 首次匯入規則時，不要指定Snort ID(SID)或修訂版號；這樣可避免與其他規則的SID發生衝突，包括刪除的規則。
- FireSIGHT管理中心會自動分配下一個可用的自定義規則SID 1000000或更多，並且版本號為1。
- 如果嘗試匯入SID大於2147483647的入侵規則，則會發生驗證錯誤。
- 匯入先前匯入的本地規則的更新版本時，必須包含由IPS分配的SID以及大於當前修訂版本號的修訂版本號。
- 您可以通過使用IPS分配的SID和大於當前修訂號的修訂號匯入規則，恢復已刪除的本地規則。請注意，刪除本地規則時，FireSIGHT管理中心會自動增加修訂版號；這是允許您恢復本地規則的裝置。

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）。