在FTD的Snort3中設定自訂本機Snort規則

目錄

簡介

本檔案介紹在防火牆威脅防禦(FTD)的Snort3中設定自訂本機Snort規則的程式。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Firepower管理中心(FMC)
- 防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

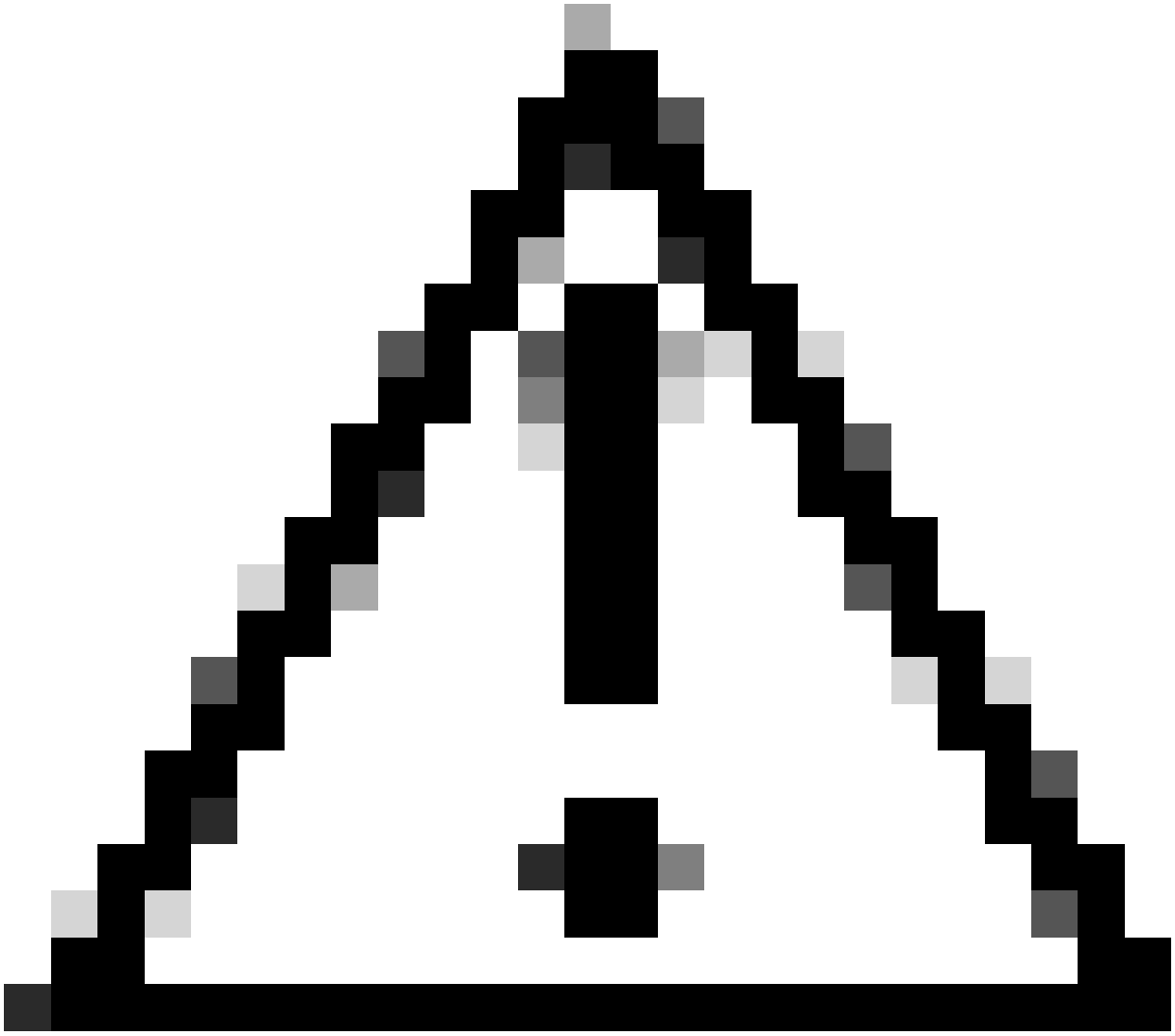
- 適用於VMWare的Cisco Firepower管理中心7.4.1
- Cisco Firepower 2120 7.4.1

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

使用管理中心在威脅防禦中對Snort 3的支援從版本7.0開始。對於7.0版及更高版本的新裝置和重新映像裝置，Snort 3是預設檢測引擎。

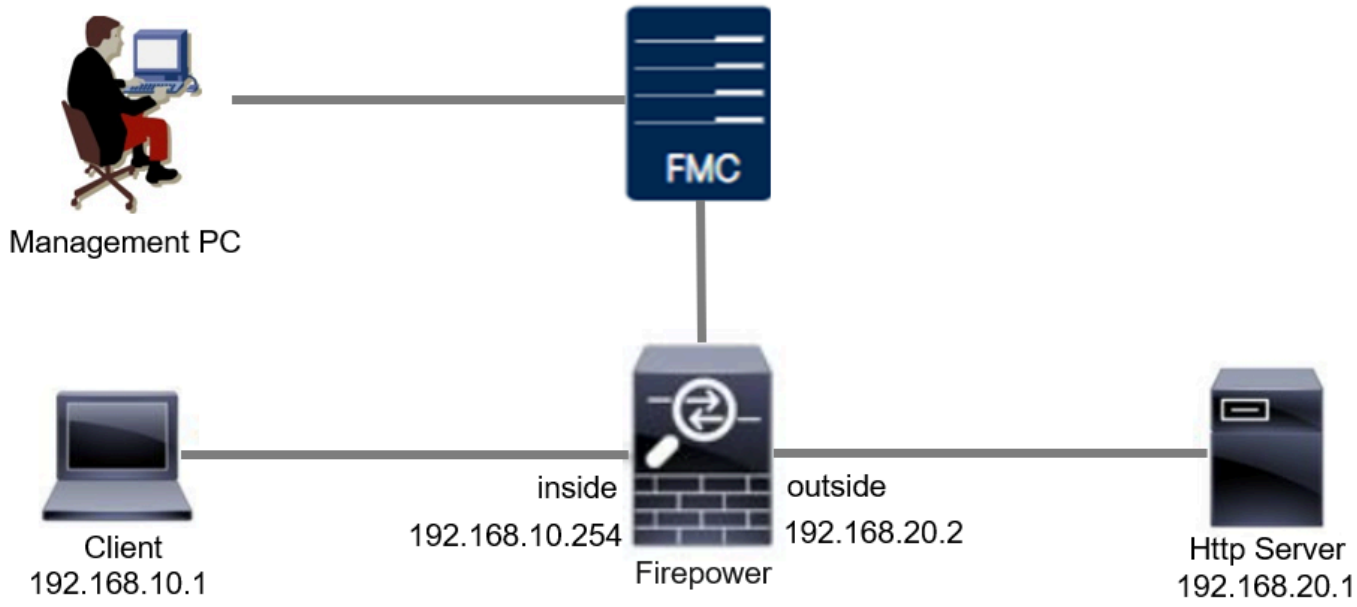
本文提供如何針對Snort 3自訂Snort規則的範例，以及實際的驗證範例。具體而言，介紹了如何使用自定義Snort規則配置和驗證入侵策略，以丟棄包含特定字串（使用者名稱）的HTTP資料包。



注意：建立自定義本地Snort規則並提供支援不在TAC支援範圍之內。因此，本文檔只能用作參考，並要求您自行斟酌決定並自行負責建立和管理這些自定義規則。

網路圖表

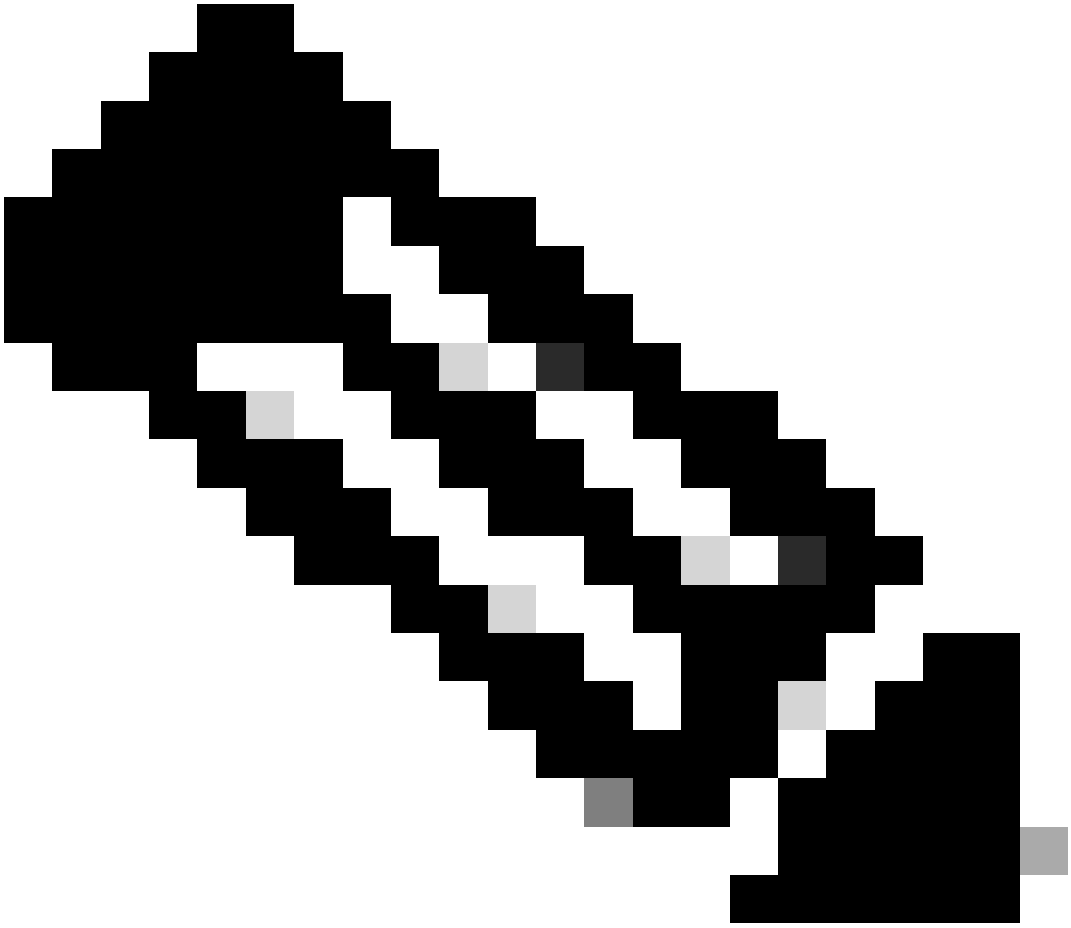
本文檔介紹此圖中Snort3中自定義本地Snort規則的配置和驗證。



網路圖表

組態

這是自訂本機Snort規則的組態，可偵測和捨棄包含特定字串（使用者名稱）的HTTP回應封包。

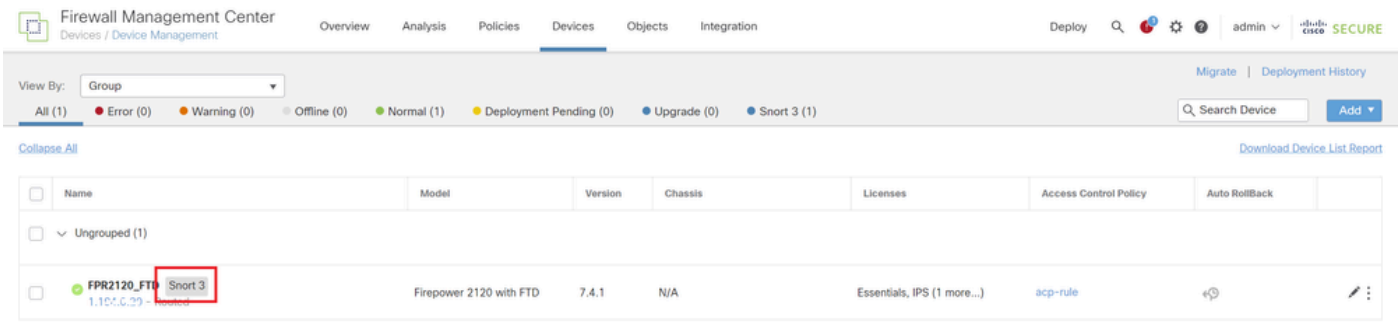


注意：到目前為止，無法從FMC GUI中的Snort 3全部規則頁面增加自定義本地Snort規則。您必須使用本檔案中介紹的方法。

方法1.從Snort 2匯入Snort 3

步驟1.確認Snort版本

導航到裝置>FMC上的裝置管理，點選裝置頁籤。確認snort版本為Snort3。



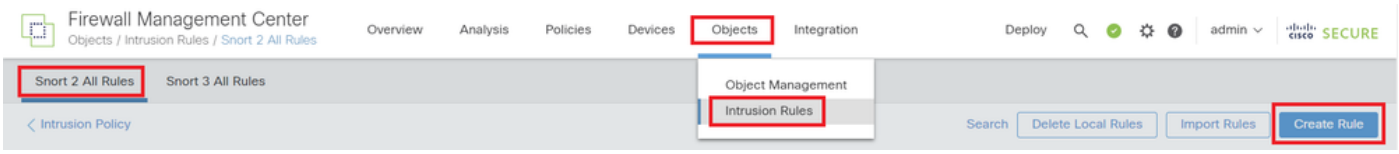
Snort版本

步驟 2.在Snort 2中建立或編輯自定義本地Snort規則

在FMC上導航到對象>入侵規則> Snort 2所有規則。點選Create Rulebutton增加自定義本地Snort規則，或者導航到Objects > Intrusion Rules > Snort 2 All Rules > Local Rules on FMC，點選Edit 按鈕編輯現有自定義本地Snort規則。

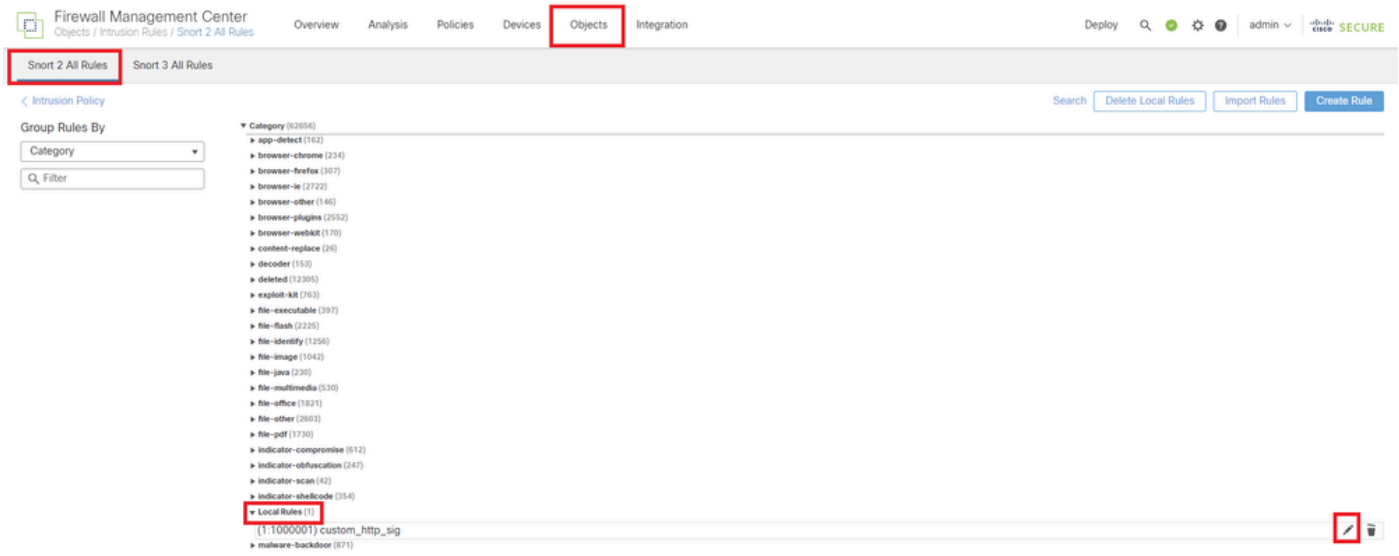
有關如何在Snort 2中建立自定義本地Snort規則的說明，請參閱在FTD的Snort2中配置自定義本地Snort規則。

增加新的自定義本地Snort規則，如圖所示。



新增自訂規則

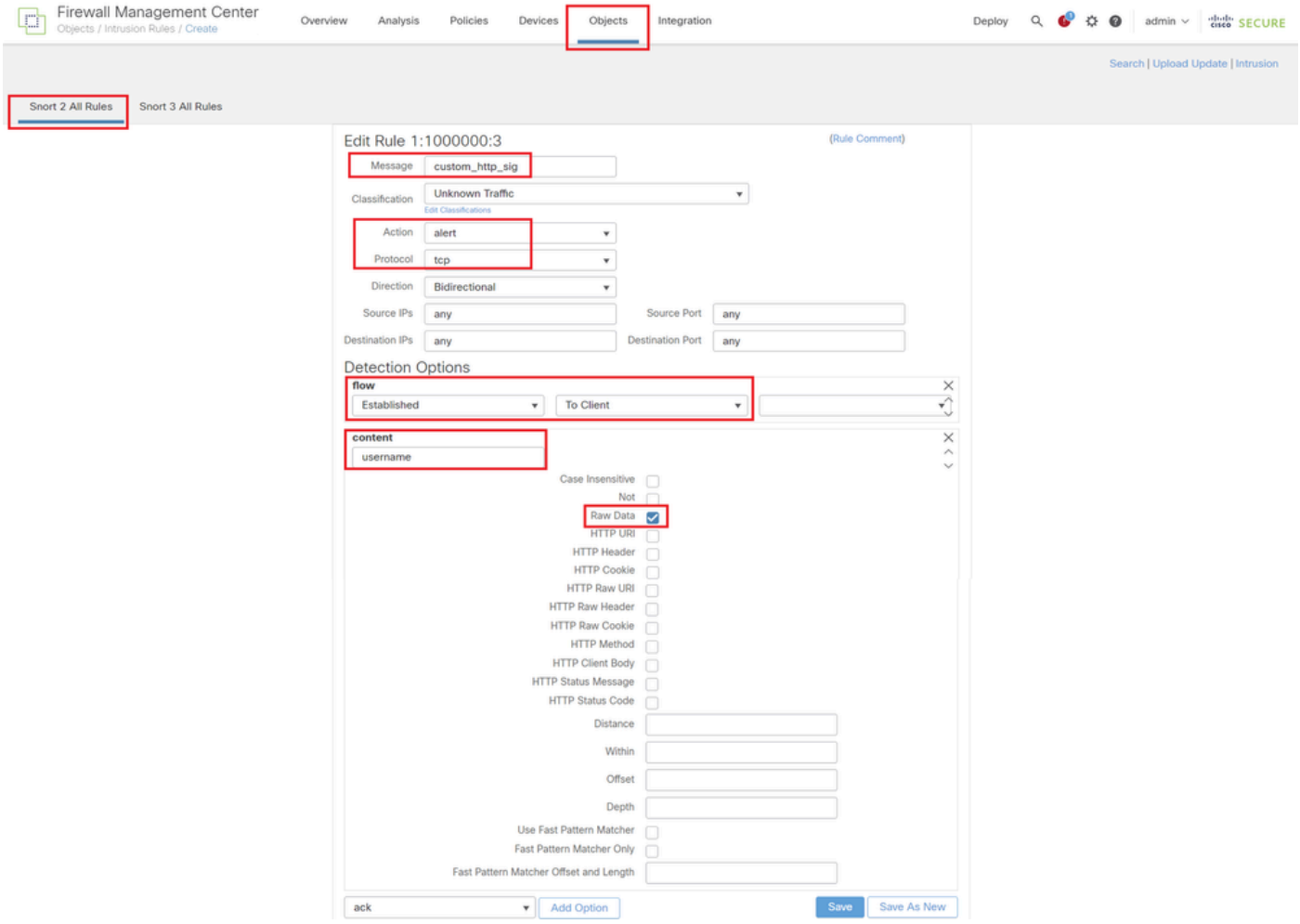
編輯如圖所示的現有自定義本地Snort規則。在此範例中，編輯現有的自訂規則。



編輯現有的自訂規則

輸入簽名資訊以檢測包含特定字串（使用者名稱）的HTTP資料包。

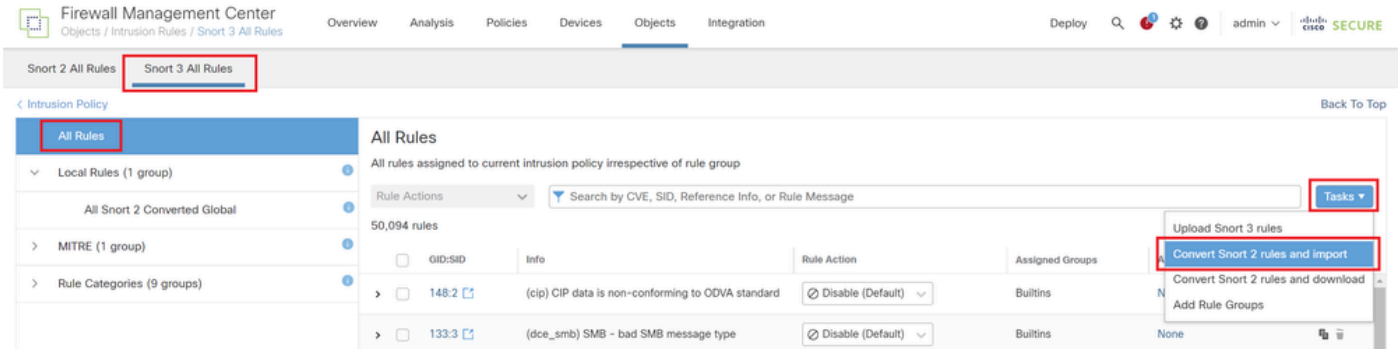
- 消息： custom_http_sig
- 操作：警報
- 協定：tcp
- flow：Established，到客戶端
- 內容：使用者名稱（原始資料）



輸入規則的必要資訊

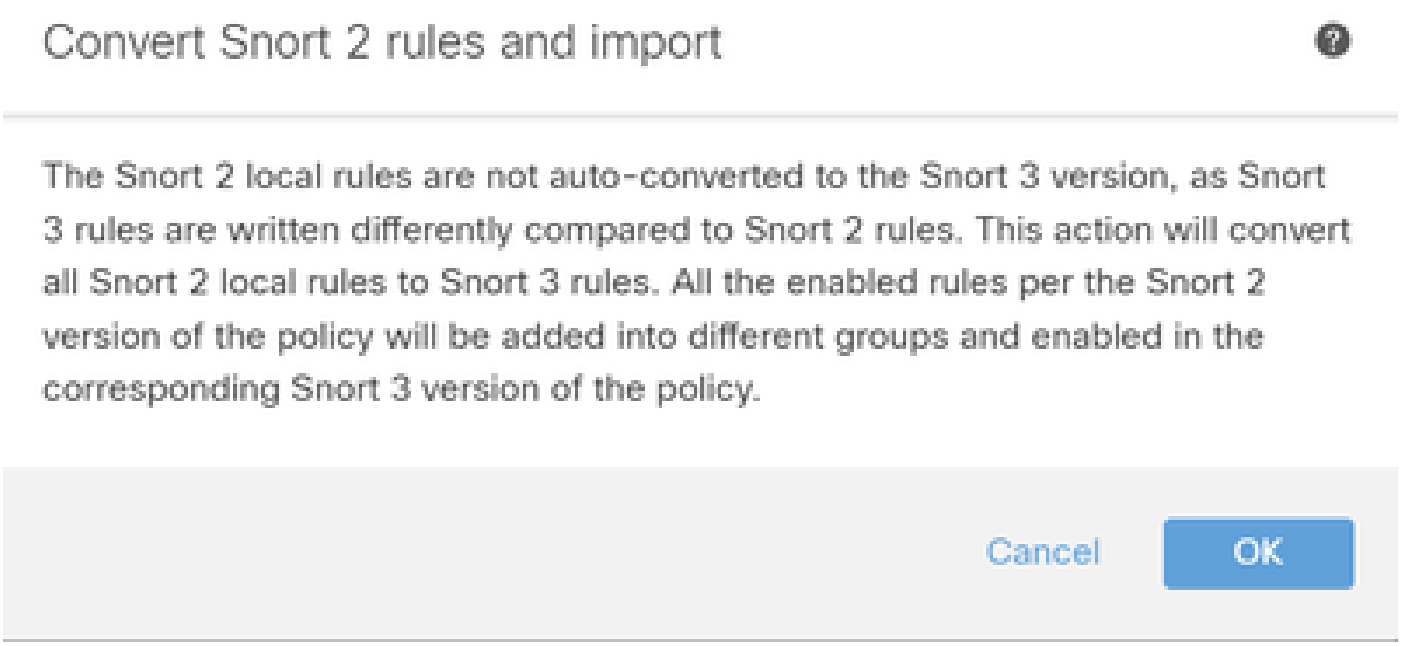
步驟 3.將自定義本地Snort規則從Snort 2導入Snort 3

在FMC上導航到對象>入侵規則> Snort 3所有規則>所有規則，從任務下拉選單中按一下轉換Snort 2規則和導入。



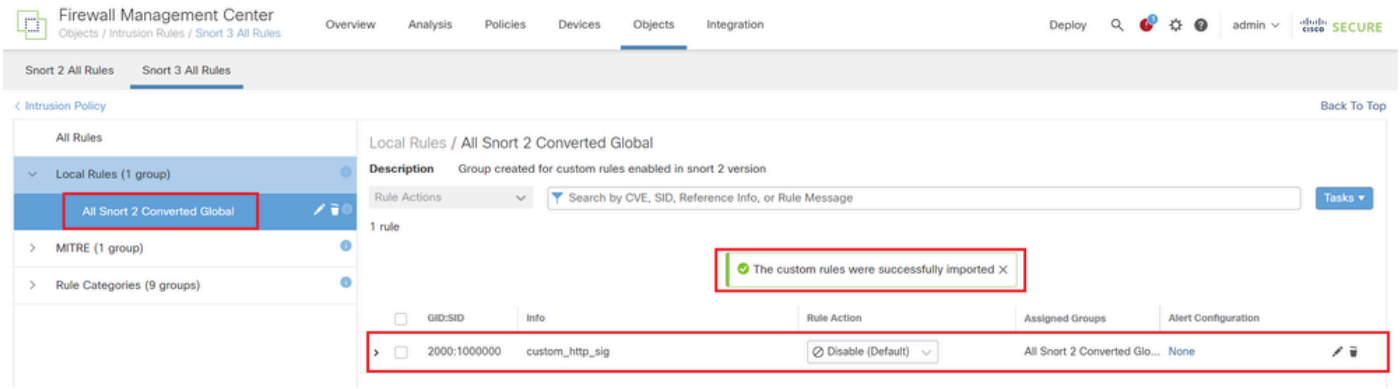
將自定義規則導入Snort 3

檢查警告消息並按一下OK。



警告訊息

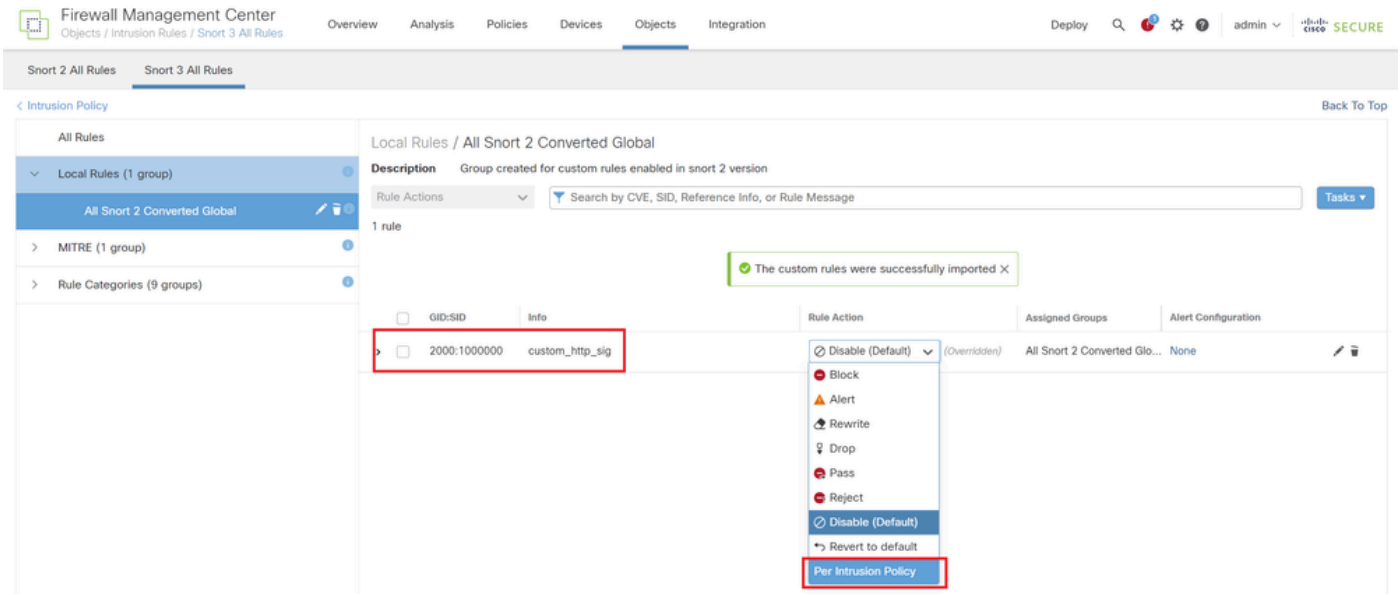
導航到FMC上的對象>入侵規則> Snort 3所有規則，點選所有Snort 2轉換的全局以確認導入的自定義本地Snort規則。



確認匯入的自訂規則

步驟 4.變更規則動作

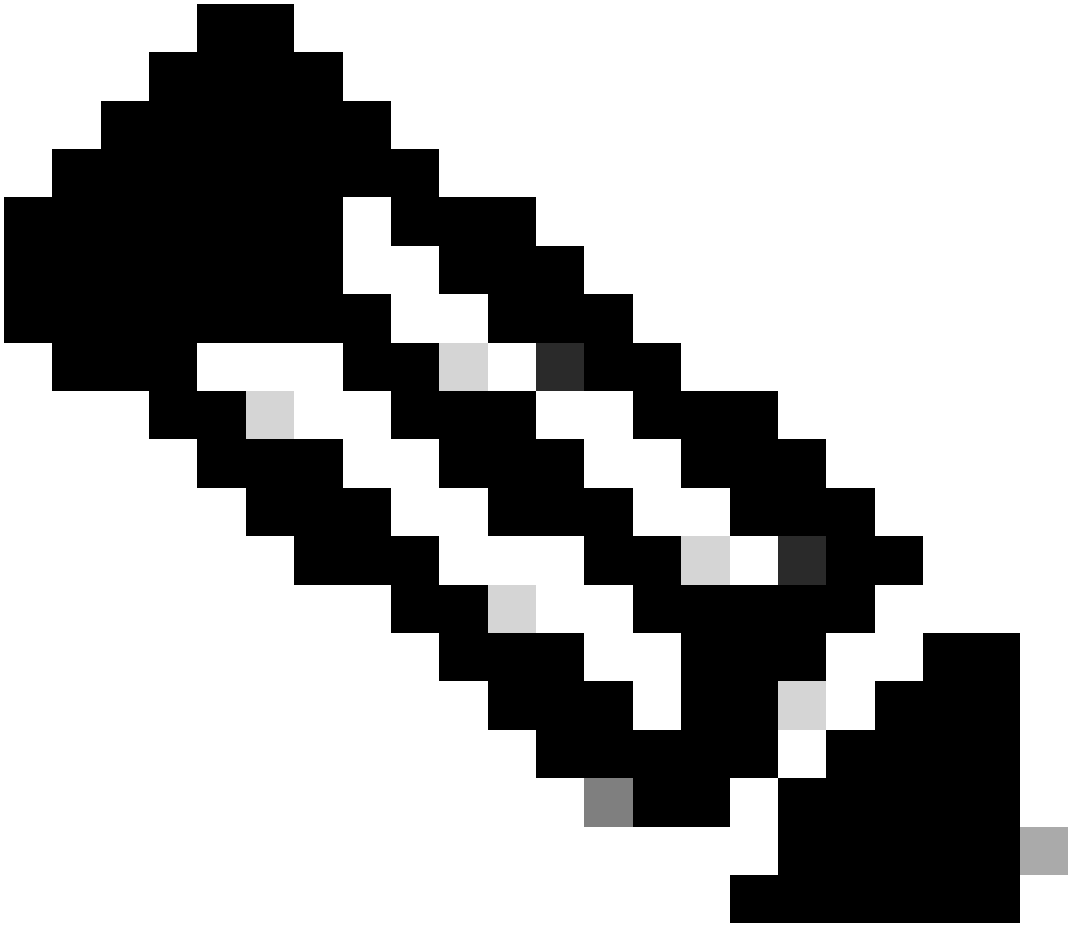
根據目標自定義規則的Rule Action，按一下Per Intrusion Policy。



變更規則動作

在Edit Rule Action螢幕中，輸入Policy和Rule Action的資訊。

- 策略：snort_test
- 規則操作：阻止



附註：規則動作包括：

阻止-生成事件，阻止當前匹配的資料包以及此連線中的所有後續資料包。

警報-僅生成匹配資料包的事件，不丟棄資料包或連線。

Rewrite —根據規則中的替換選項生成事件並覆蓋資料包內容。

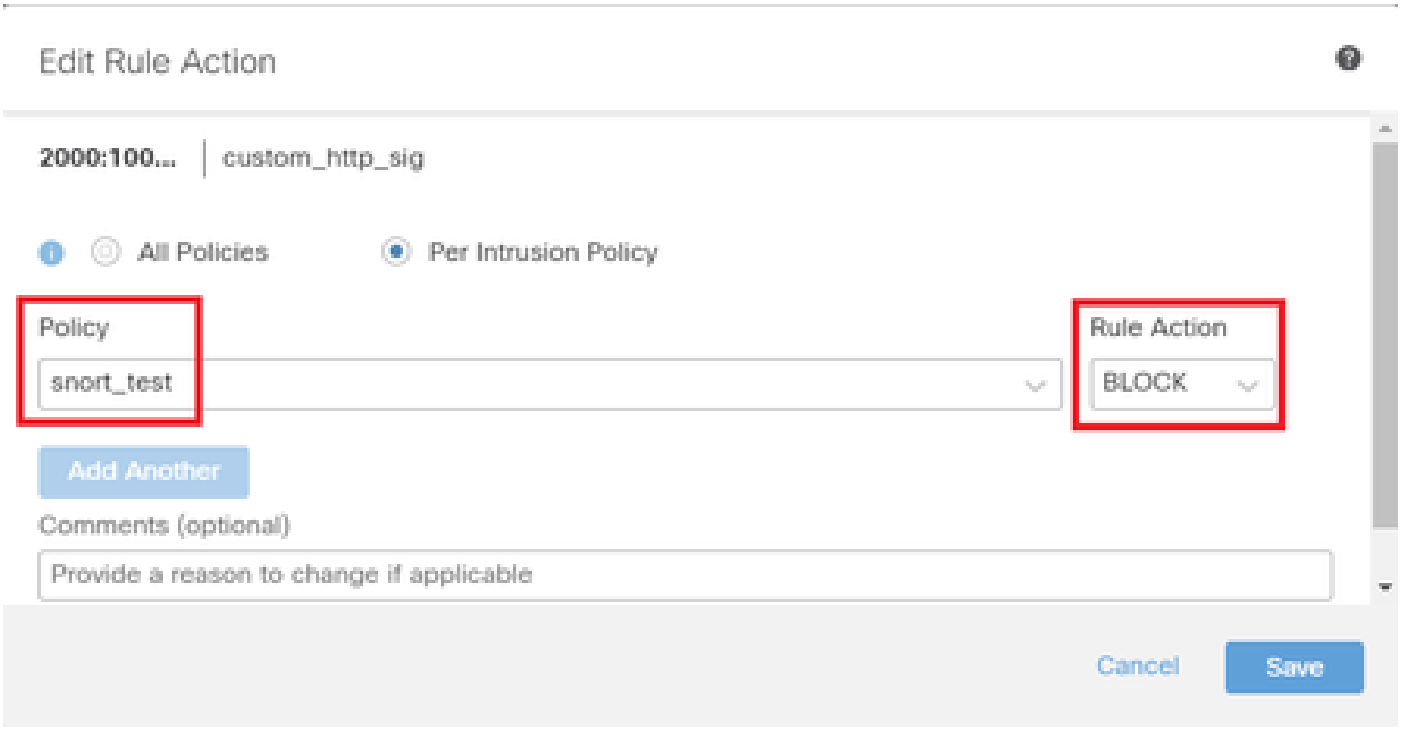
透過-不生成任何事件，允許資料包通過，而無需任何後續Snort規則進一步評估。

丟棄-生成事件，丟棄匹配的資料包，並且不阻塞此連線中的更多流量。

拒絕—生成事件，丟棄匹配的資料包，阻止此連線中的進一步流量，如果是TCP協定，則向源主機和目的主機傳送TCP重置。

Disable -不與此規則匹配流量。未生成任何事件。

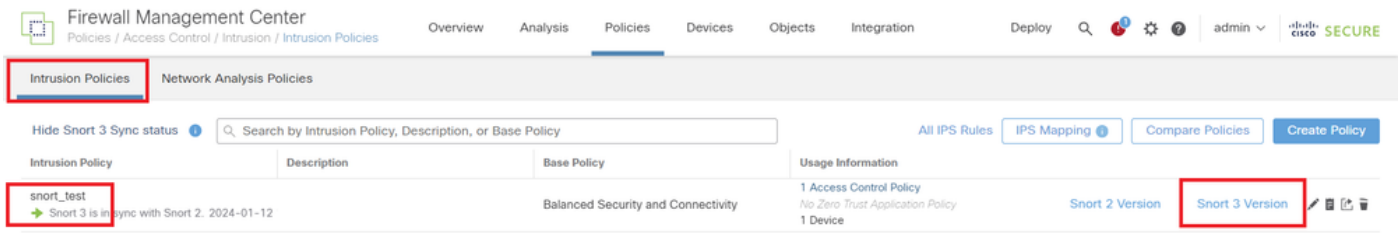
預設-恢復系統預設動作。



編輯規則動作

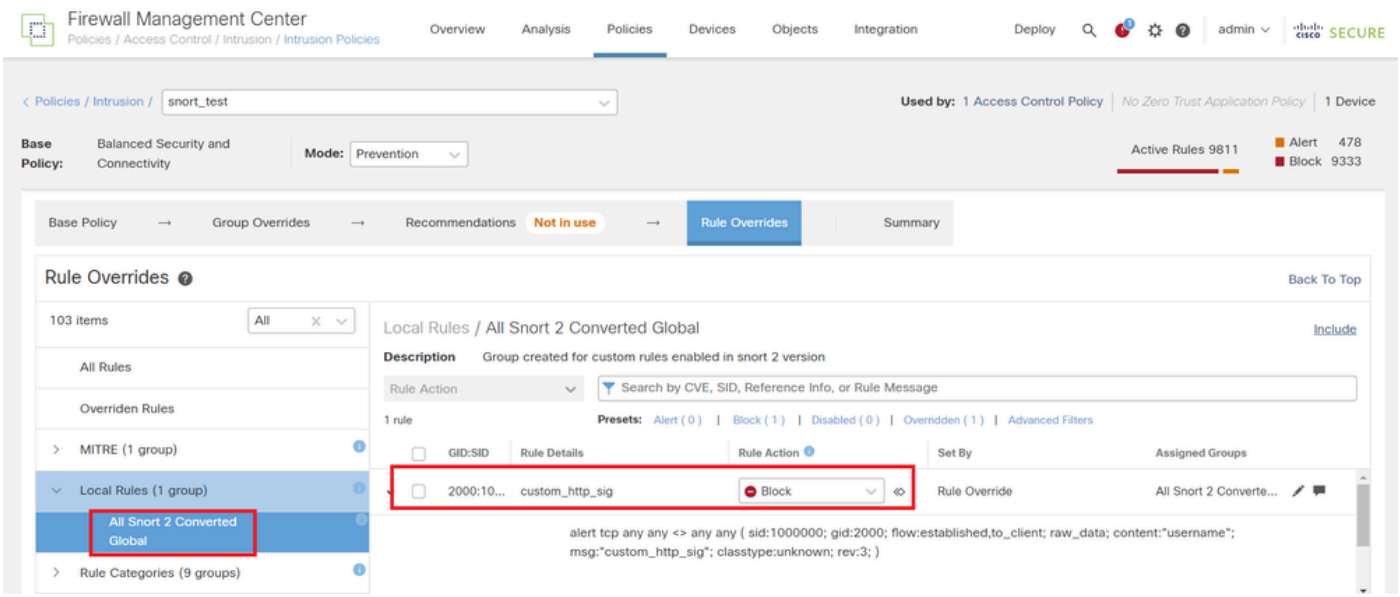
步驟 5.確認導入的自定義本地Snort規則

導航到FMC上的Policies > Intrusion Policies，點選行中對應於目標入侵策略的Snort 3版本。



確認匯入的自訂規則

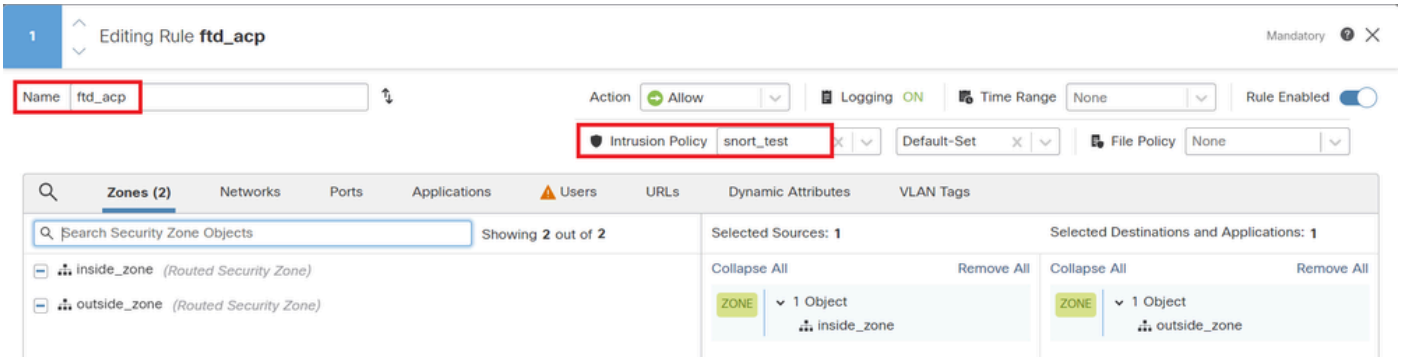
按一下Local Rules > All Snort 2 Converted Global以檢查自定義本地Snort規則的詳細資訊。



確認匯入的自訂規則

步驟 6.將入侵策略與訪問控制策略(ACP)規則關聯

導航到策略 > 訪問控制 FMC，將入侵策略與ACP關聯。



與ACP規則關聯

步驟 7.部署變更

將變更部署到FTD。

部署變更

方法2.上傳本地檔案

步驟 1.確認Snort版本

與方法1中的步驟1相同。

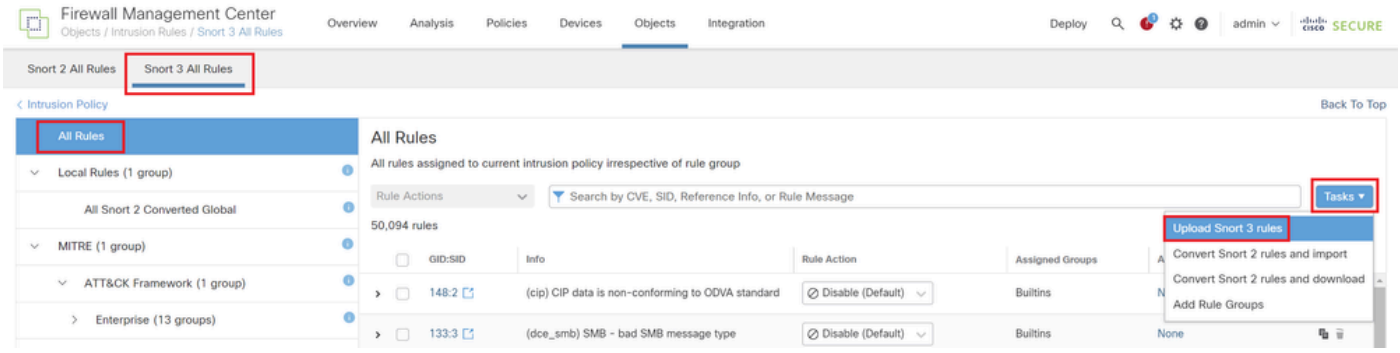
步驟 2.建立自定義本地Snort規則

手動建立自定義本地Snort規則，並將其儲存在名為custom-rules.txt的本地檔案中。

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

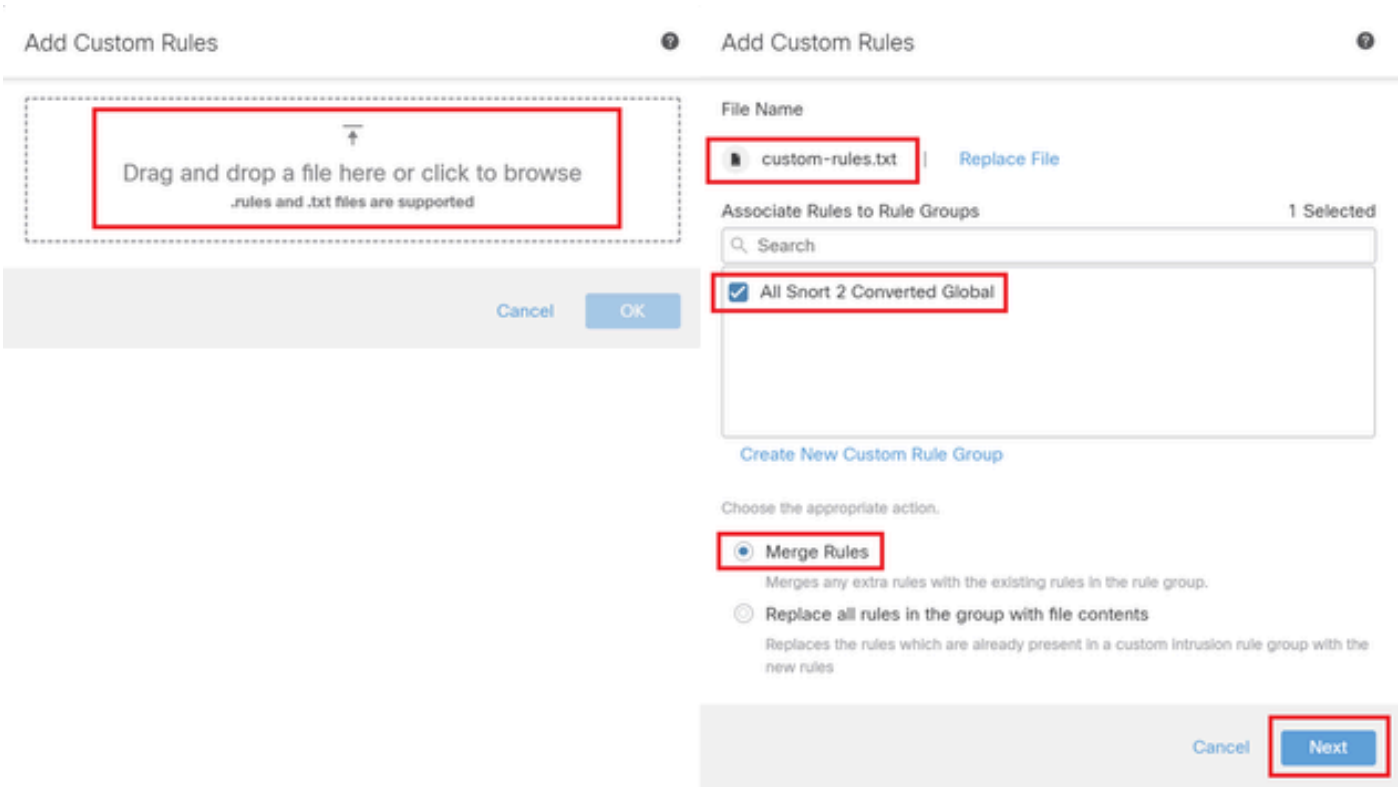
步驟 3.上傳自定義本地Snort規則

在FMC上導航到對象>入侵規則> Snort 3所有規則>所有規則，從任務下拉選單中按一下上傳Snort 3規則。



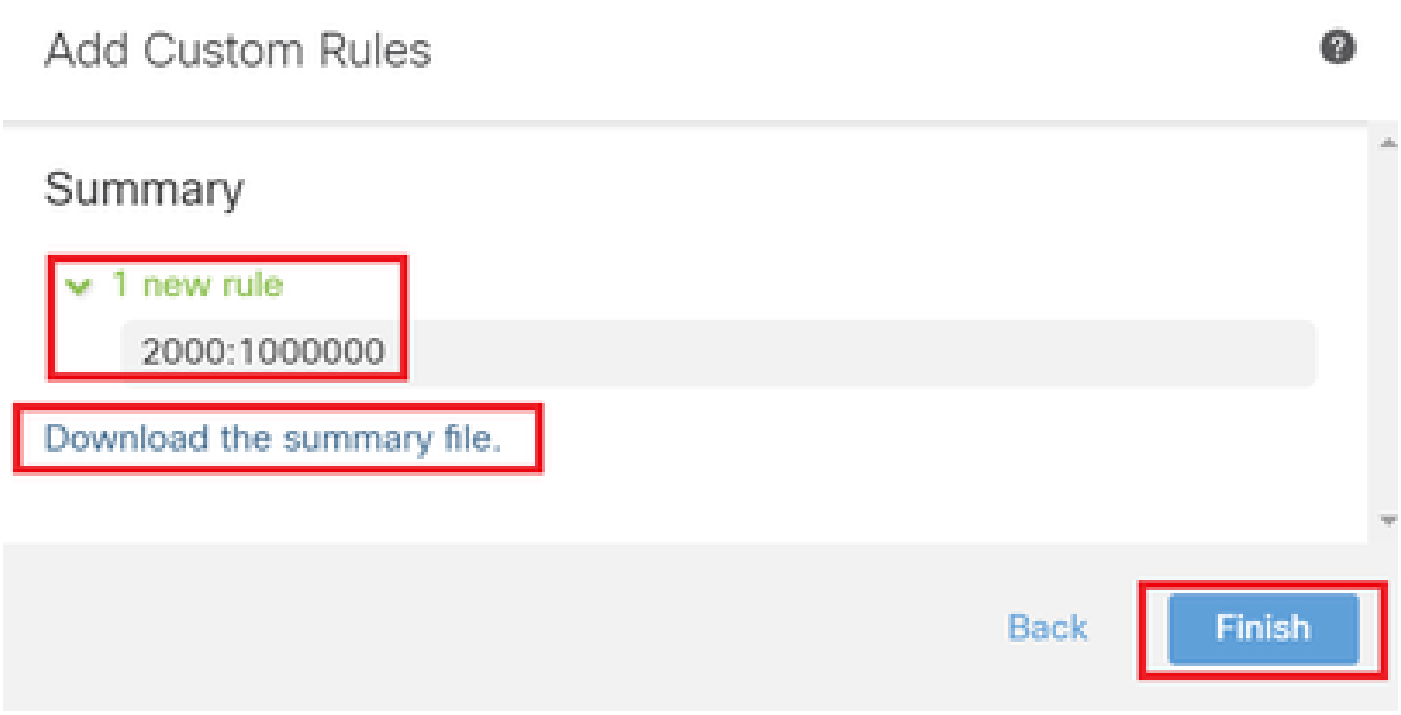
上傳自訂規則

在Add Custom Rules螢幕中，拖放本地custom-rules.txt檔案，選擇Rule Groups和Suitable Action（本示例中為Merge Rules），然後按一下Next按鈕。



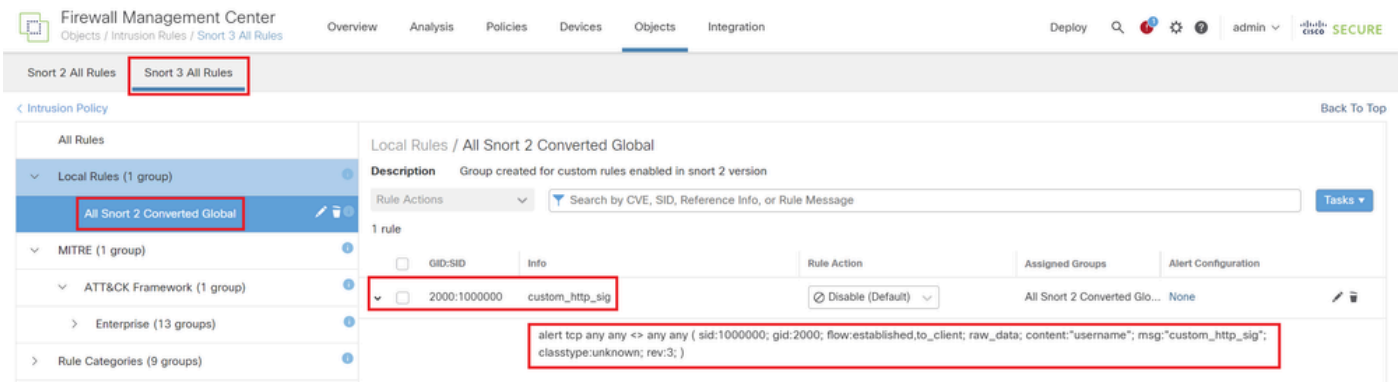
增加自定義規則

確認已成功上載本地規則檔案。



確認上傳結果

導航到FMC上的Objects > Intrusion Rules > Snort 3 All Rules，點選All Snort 2 Converted Global以確認上傳的自定義本地Snort規則。



自定義規則的詳細資訊

步驟 4.變更規則動作

與方法1中的步驟4相同。

步驟 5.確認上傳的自訂本機Snort規則

與方法1中的步驟5相同。

步驟 6.將入侵策略與訪問控制策略(ACP)規則關聯

與方法1中的步驟6相同。

步驟 7.部署變更

與方法1中的步驟7相同。

驗證

步驟 1.設定HTTP伺服器中的檔案內容

將HTTP伺服器端的test.txt檔案內容設定為username。

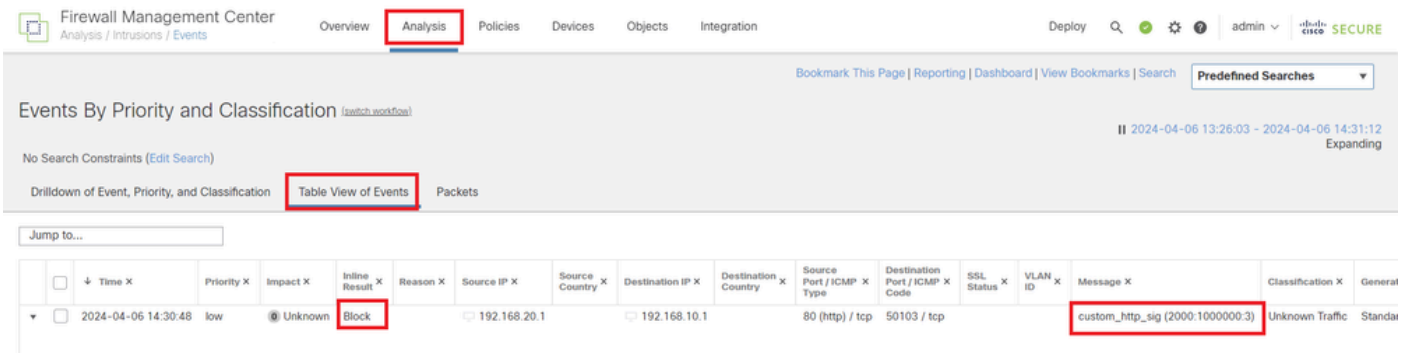
步驟 2.初始HTTP請求

從使用者端(192.168.10.1)的瀏覽器存取HTTP伺服器(192.168.20.1/test.txt)，並確認已封鎖HTTP通訊。

初始HTTP請求

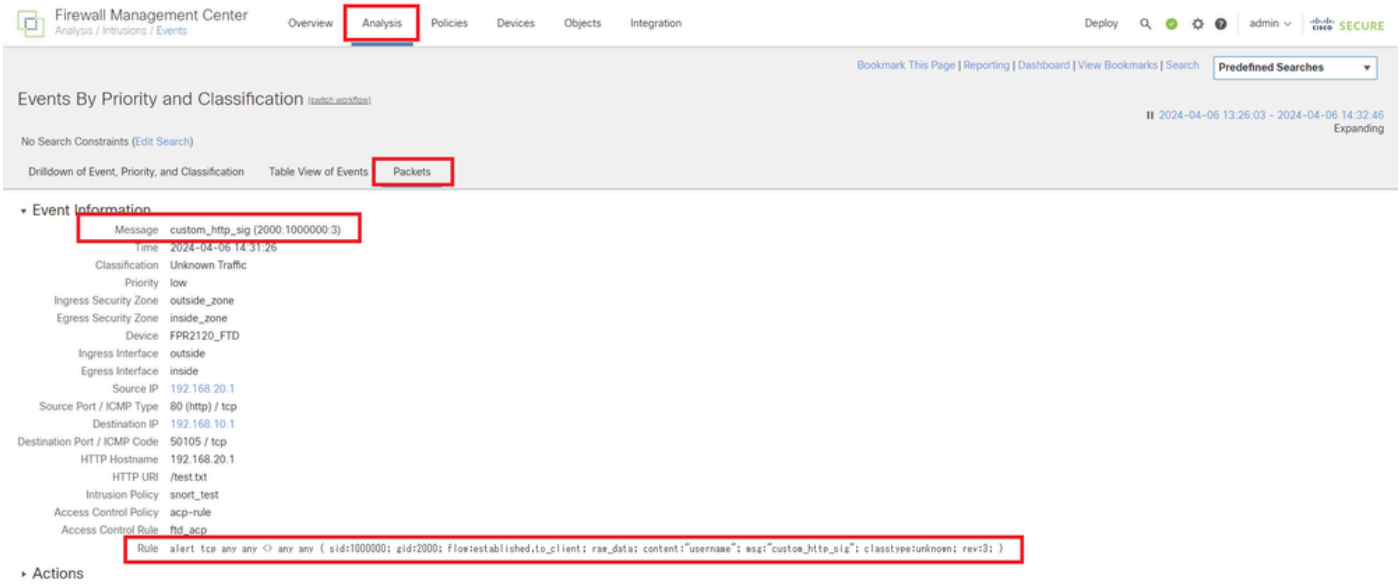
步驟 3.確認入侵事件

導航到Analysis>Intrusions>Eventson FMC，確認入侵事件由自定義本地Snort規則生成。



入侵事件

點選Packetstab，確認入侵事件的詳細資訊。



入侵事件的詳細資訊

常見問題 (FAQ)

問：建議使用哪一種，Snort 2或Snort 3？
答：與Snort 2相比，Snort 3提高了處理速度，並提供了新功能，使其成為更推薦的選項。

問：從7.0之前的FTD版本升級到7.0或更高版本後，Snort版本是否自動更新為Snort 3？
答：否，檢測引擎仍在Snort 2上。若要在升級後使用Snort 3，您必須明確啟用它。請注意，Snort 2計畫在未來版本中不再使用，強烈建議您立即停止使用。

問：在Snort 3中，是否可以編輯現有自定義規則？
答：不，您無法編輯它。若要編輯特定自訂規則，您必須刪除相關規則並重新建立。

疑難排解

運行system support trace命令以確認FTD上的行為。在本例中，HTTP流量被IPS規則(2000：1000000：3)阻止。

```
<#root>

>

system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '

ftd_acp
```

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

Event

:

2000:1000000:3

, Action

block

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

ips, block

参考

Cisco Secure Firewall Management Center Snort 3配置指南

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）。