使用CLI和FMC GUI從Firepower感測器驗證自定義SID清單

簡介

本文說明如何使用CLI和FMC GUI從Firepower威脅防禦(FTD)或FirePOWER模組獲取自定義SID清單。如果導航到***Objects > Intrusion Rules***，可以在FMC ***GUI上找到SID資訊。***在某些情況下，需要從CLI獲取可用SID的清單。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Firepower威脅防禦(FTD)
- 具備FirePOWER服務的Cisco ASA
- Cisco Firepower Management Center(FMC)
- Linux基礎知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- Firepower管理中心6.6.0
- Firepower威脅防禦6.4.0.9
- FirePOWER模組6.2.3.2

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

入侵規則是一組關鍵字和引數，系統使用這些關鍵字和引數來檢測利用網路漏洞的企圖。系統分析網路流量時，會根據每個規則中指定的條件比較資料包。如果資料包資料匹配規則中指定的所有條件，則規則觸發。如果規則是警報規則，則會生成入侵事件。如果是通行規則，則會忽略流量。對於內聯部署中的丟棄規則，系統會丟棄資料包並生成事件。您可以從Firepower管理中心Web控制檯檢視和評估入侵事件。

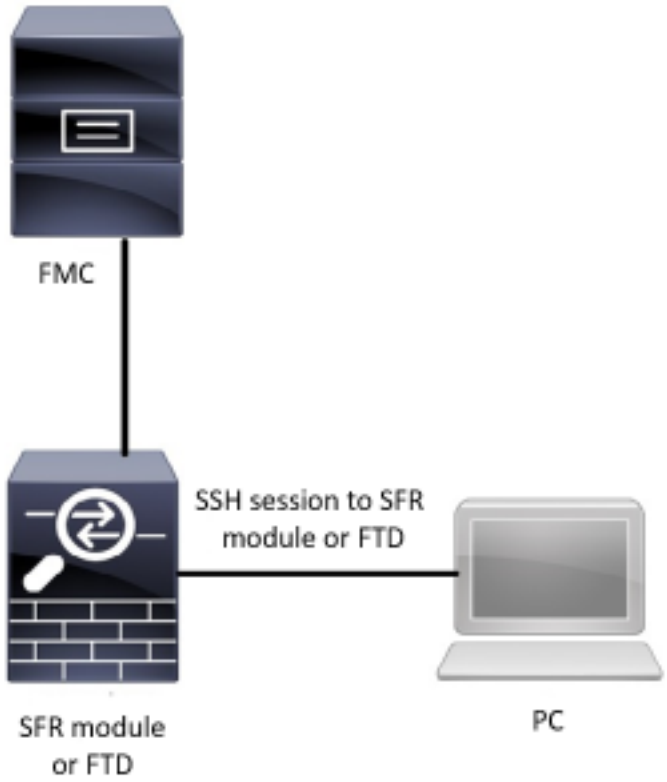
Firepower系統提供兩種型別的入侵規則：***共用對象規***則和***標準文本規則***。Cisco Talos安全情報和研究小組(Talos)可以使用共用對象規則來檢測對漏洞的攻擊，其方式是傳統標準文本規則無法實現的。無法建立共用對象規則。當入侵規則自行編寫時，必須建立標準文本規則。自定義標準文本規則，以調整您可能看到的事件型別。通過編寫規則並指定規則的事件消息，可以更輕鬆地識別指示攻擊和策略規避的流量。

在自定義入侵策略中啟用自定義標準文本規則時，請記住某些規則關鍵字和引數要求首先以某種方式解碼或預處理流量。

Firepower系統上的***自定義本地規則***是自定義標準Snort規則，您可從本地電腦以ASCII文本檔案格式匯入該規則。Firepower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。

> **警告：**在生產環境中使用規則之前，請確保使用受控網路環境來測試所編寫的任何入侵規則。編寫不當的入侵規則可能會嚴重影響系統的效能

網路圖表

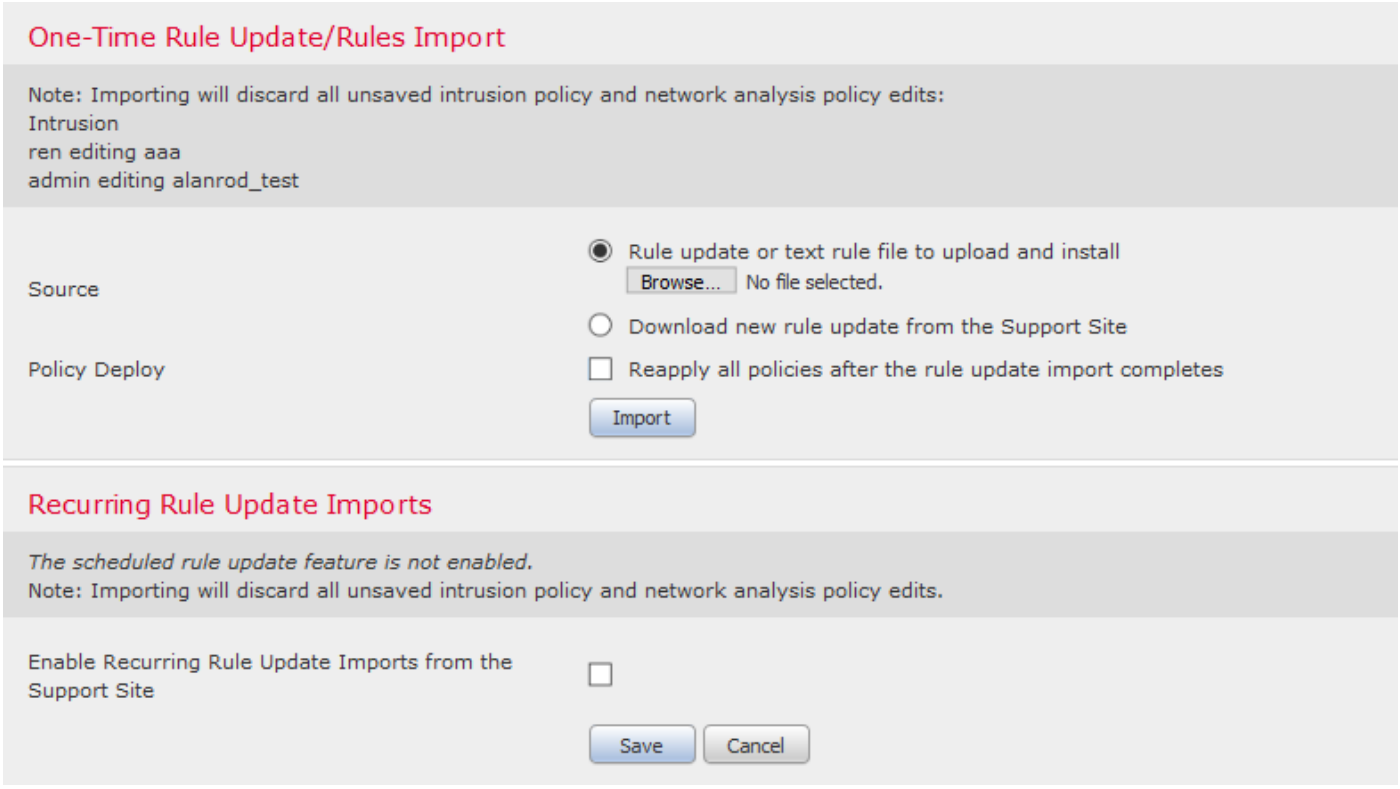


設定

匯入本地規則

開始之前，您需要確保自定義檔案中列出的規則不包含任何特殊字元。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。

步驟1.導航到**Objects > Intrusion Rules > Import Rules**，即可訪問**Import Rules**(匯入規則)**頁籤。此時會顯示Rule Updates**頁面，如下圖所示：



步驟2.選擇要上傳和安裝的規則更新或文本規則檔案，然後單擊Browse以選擇自定義規則檔案

附註：所有上載的規則都儲存在本**地規則**類別

步驟3.按一下Import。規則檔案已匯入

註:Firepower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。

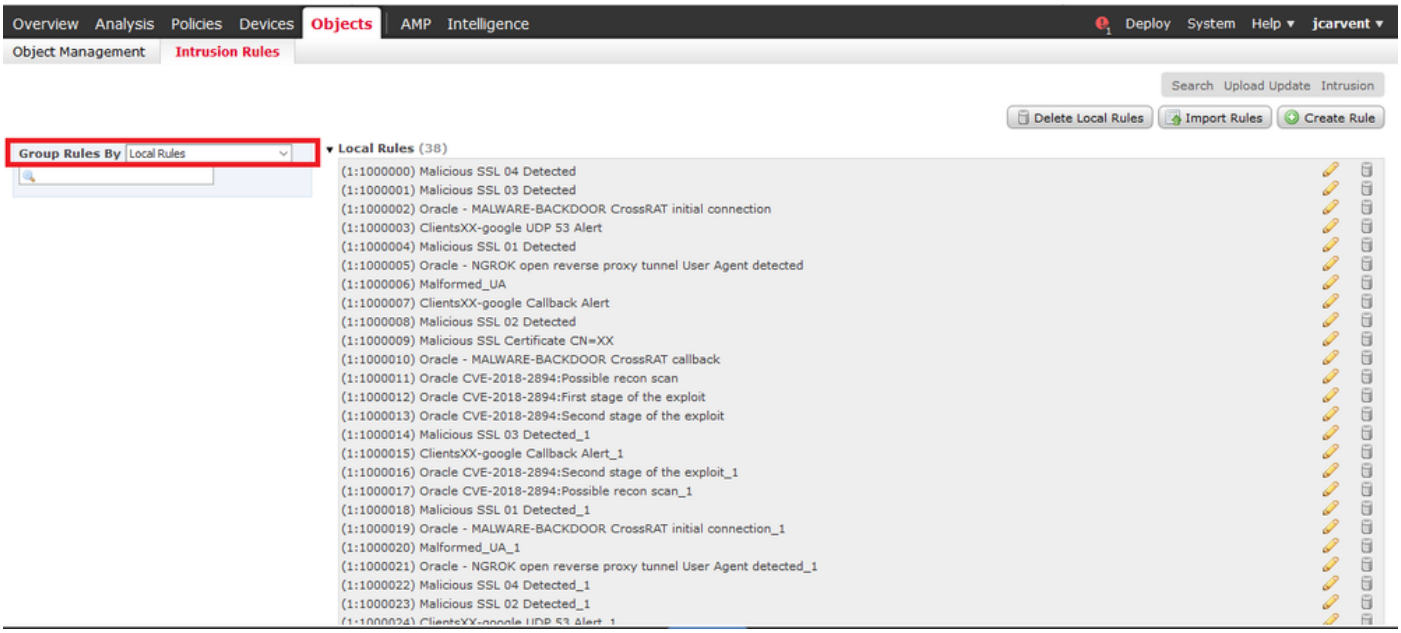
驗證

在FMC GUI上

1.檢視從FMC GUI匯入的本地規則

步驟1.導覽至Objects > Intrusion Rules

步驟2.從Group Rules中選擇Local Rules



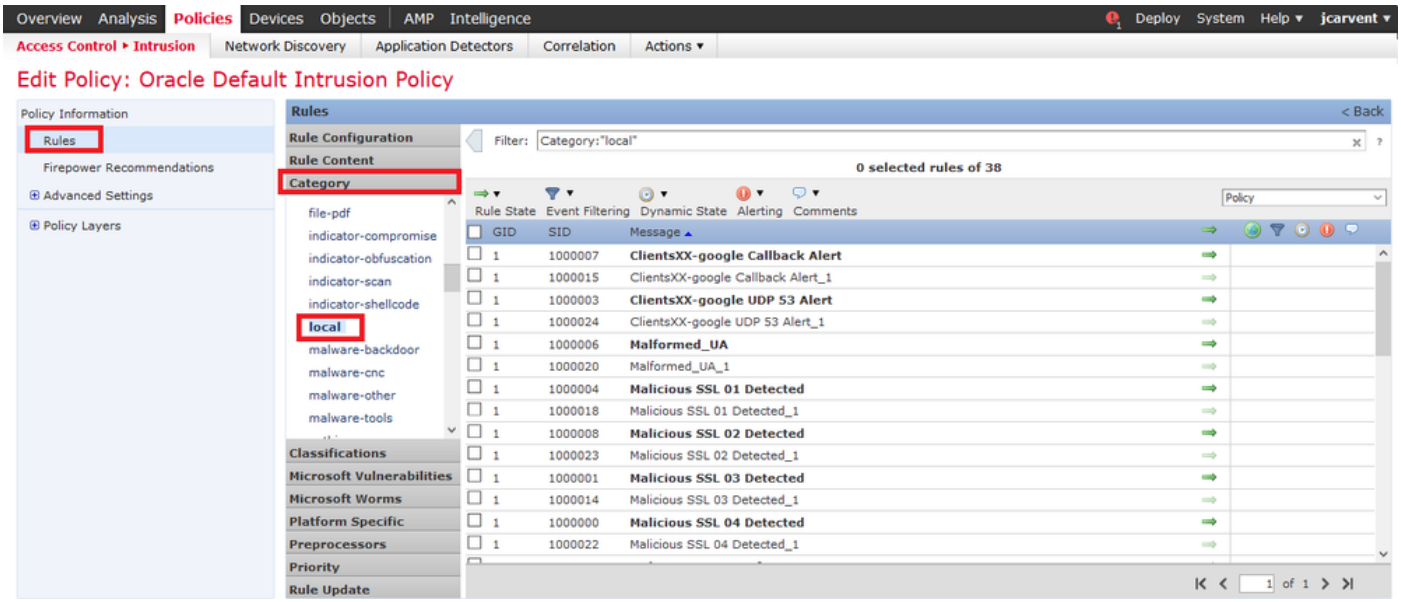
預設情況下，Firepower系統將本地規則設定為禁用狀態。這些本地規則必須手動設定本地規則的狀態，然後才能在入侵策略中使用它們。

2.從入侵策略啟用本地規則

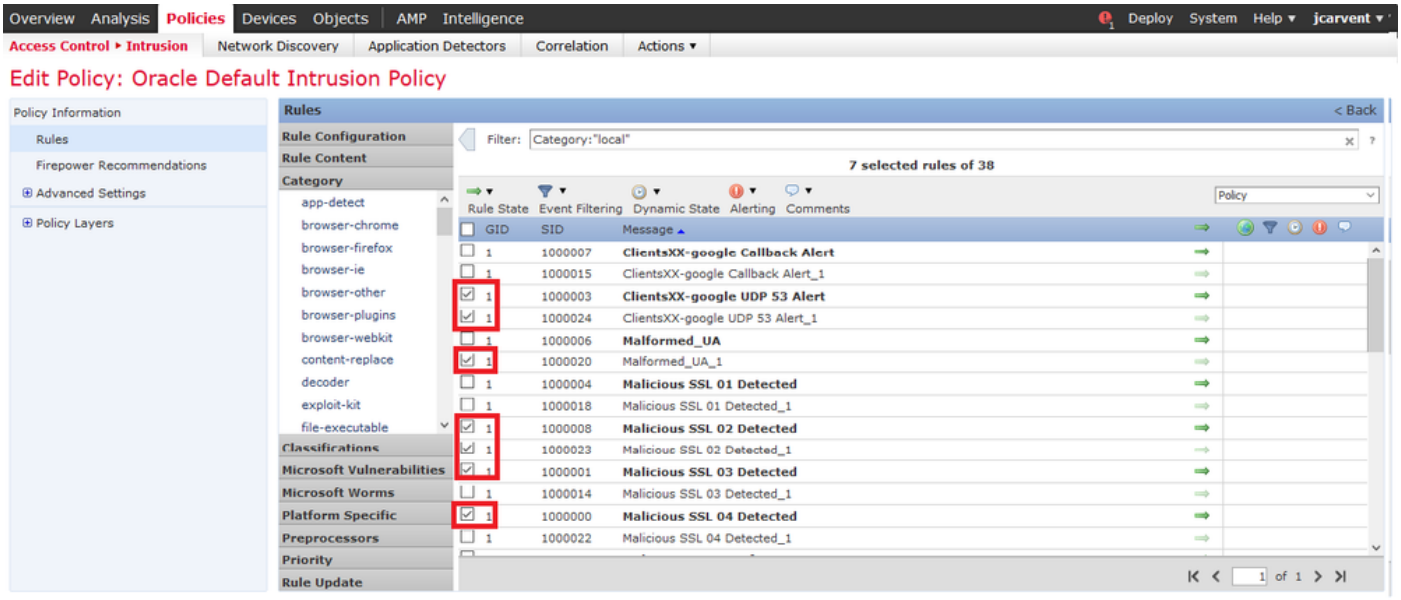
步驟1.導覽至Policies > Intrusion > Intrusion Policy下的Policy Editor頁面

步驟2.在左面板中選擇Rules

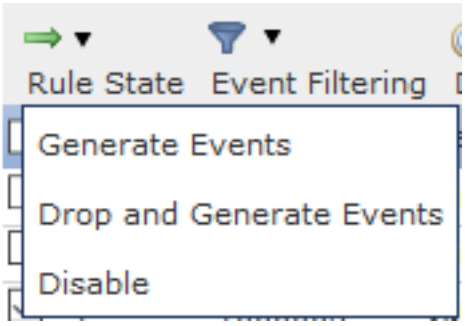
步驟3.在Category下選擇local。如果可用，應顯示所有本地規則：



步驟4. 選擇所需的本地規則：



步驟5.選擇所需的本地規則後，從**Rule State**（規則狀態）中選擇**一個狀態**



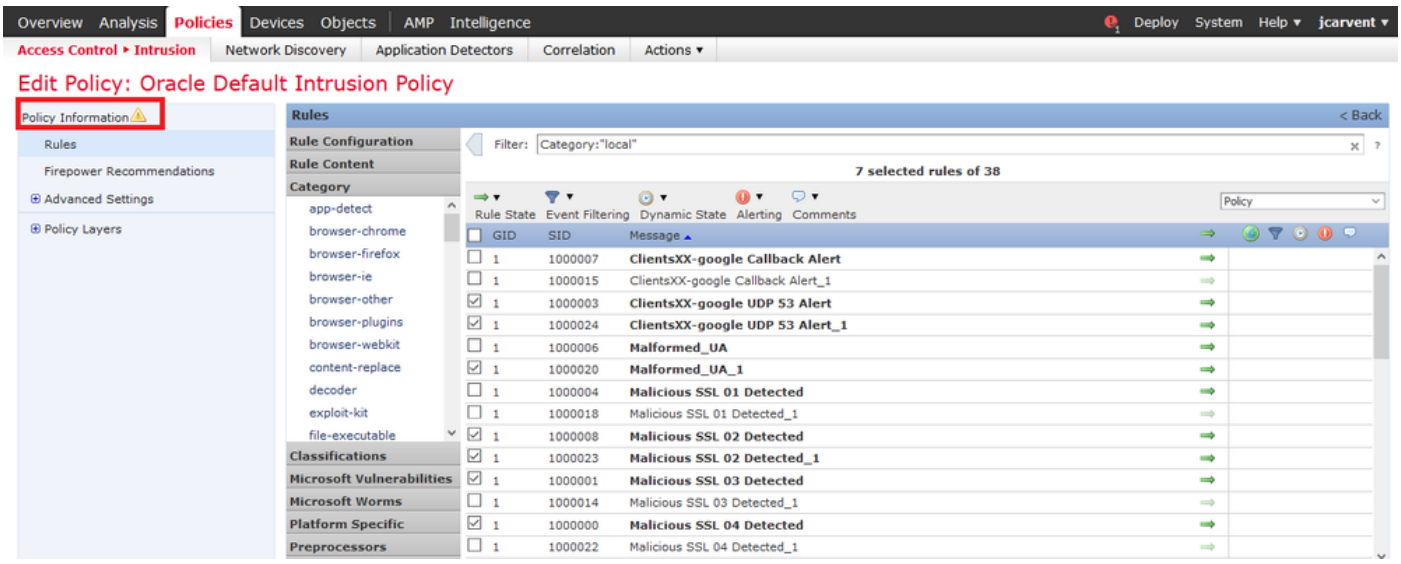
提供以下選項：

— **生成事件**：啟用規則並生成事件

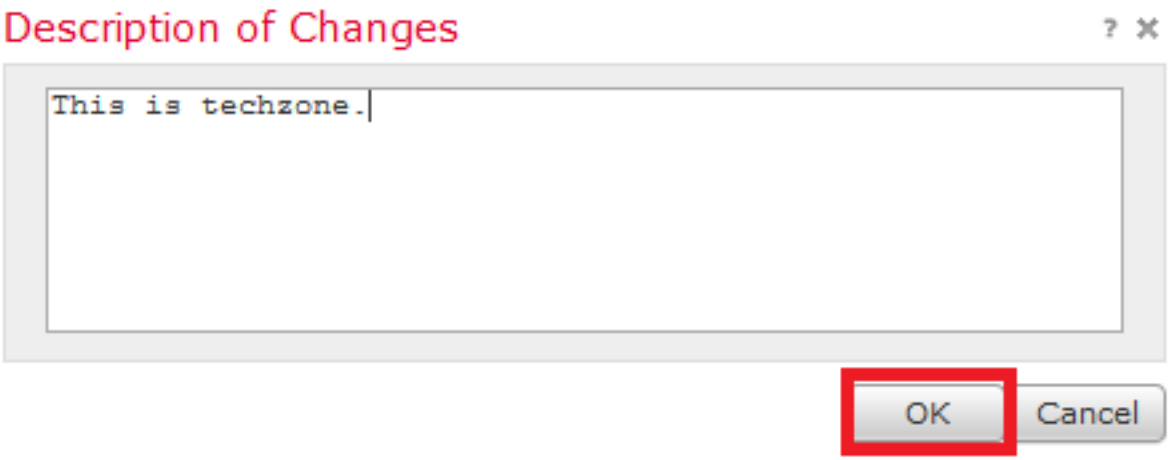
— **丟棄並生成事件**：啟用規則、丟棄流量並生成事件

— **禁用**：沒有啟用規則，沒有事件

步驟6. 選擇規則狀態後，按一下 **左側面板上的「策略資訊」選項**



步驟7.選擇Commit Changes按鈕，並提供更改的簡要說明。稍後按一下OK。入侵策略已驗證。



注意：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。

步驟8.部署更改

在FTD或SFR模組CLI上

1.檢視從FTD或SFR模組CLI匯入的本地規則

步驟1.從SFR模組或FTD建立SSH或CLI會話

步驟2.導航至專家模式

```
> expert
admin@firepower:~$
```

步驟3.獲取管理員許可權

```
admin@firepower:~$ sudo su -
```

步驟4.輸入您的密碼

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

步驟5.導覽至/ngfw/var/sf/detection_engine/UUID/intrusion/

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

附註：如果您使用的是SFR模組，請不要使用/ngfw/var/sf/detection_engine/*/intrusion path。使用**/var/sf/detection_engine/*/intrusion**

步驟6.引入以下命令

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```
請參閱下圖作為工作範例：

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```
這將列出由FTD或SFR模組啟用的客戶SID清單。

疑難排解

步驟1.確保從FMC detection_engine建立到SFR模組或FTD的SSH會話

步驟2.命令grep -Eo "sid:*([0-9]{1,8})" */*local.rules僅在入侵目錄下運行，該命令無法從其他目錄使用

步驟3.使用grep -Eo "sid:*([0-9]{1,8})" */*.rules命令獲取所有類別的完整SID清單

匯入本地入侵規則的最佳實踐

匯入本地規則檔案時，請遵循以下准則：

- 規則匯入程式要求所有自定義規則都匯入到以ASCII或UTF-8編碼的純文字檔案檔案中
- 文本檔名可以包含字母數字字元、空格，並且除了下劃線(_)、句點(.)和短劃線(-)外，不包含其他特殊字元
- 系統會匯入以單個磅字元(#)開頭的本地規則，但這些規則會被標籤為已刪除
- 系統匯入以單個磅字元(#)開頭的本地規則，而不匯入以兩個磅字元(##)開頭的本地規則
- 規則不能包含任何跳脫字元
- 匯入本地規則時，不必指定生成器ID(GID)。如果指定，則僅為標準文本規則指定GID 1
- 在首次匯入規則時，請執行以下操作 *不* 指定 Snort ID (SID)或修訂號。這樣可避免與其他規則的SID衝突，包括刪除的規則。系統將自動為規則分配下一個可用的自定義規則SID 1000000或更高，修訂版號為1
- 如果必須匯入具有SID的規則，則SID必須是介於1,000,000和9,999,999之間的唯一數字
- 在多域部署中，系統將SID分配到上所有域使用的共用池中的匯入規則 Firepower管理中心.如果多個管理員同時匯入本地規則，則單個域中的SID可能顯示為非順序的，因為系統將該序列中的干預編號分配給了另一個域
- 匯入先前匯入的本地規則的更新版本時，或者恢復已刪除的本地規則時，必須包括由系統分配的***SID以及大於當前修訂版本號的修訂版***號。您可以通過編輯規則來確定當前或被刪除規則的修訂號

  註：刪除本地規則時，系統會自動增加修訂版號；這是允許您恢復本地規則的裝置。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。

- 在高可用性對中匯入主Firepower管理中心的本地規則，以避免SID編號問題
- 如果規則包含以下任何內容，匯入將失敗：SID大於2147483647長度超過64個字元的源或目標埠的清單
- 如果啟用匯入的本地規則(該規則將已棄用的***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
- 所有匯入的本地規則將自動儲存在本地規則類別中
- 系統始終設定匯入到禁用規則狀態的本地規則。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

相關資訊

以下是一些與snort SID相關的參考文檔：

更新入侵規則

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

入侵規則編輯器

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html