

在FTD的Snort2中設定自訂本機Snort規則

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[步驟 1. 確認Snort版本](#)

[步驟 2. 在Snort 2中建立自定義本地Snort規則](#)

[步驟 3. 確認自定義本地Snort規則](#)

[步驟 4. 變更規則動作](#)

[步驟 5. 將入侵策略與訪問控制策略\(ACP\)規則關聯](#)

[步驟 6. 部署變更](#)

[驗證](#)

[未觸發自定義本地Snort規則](#)

[步驟 1. 設定HTTP伺服器中的檔案內容](#)

[步驟 2. 初始HTTP請求](#)

[已觸發自定義本地Snort規則](#)

[步驟 1. 設定HTTP伺服器中的檔案內容](#)

[步驟 2. 初始HTTP請求](#)

[步驟 3. 確認入侵事件](#)

[疑難排解](#)

簡介

本檔案介紹在防火牆威脅防禦(FTD)的Snort2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：

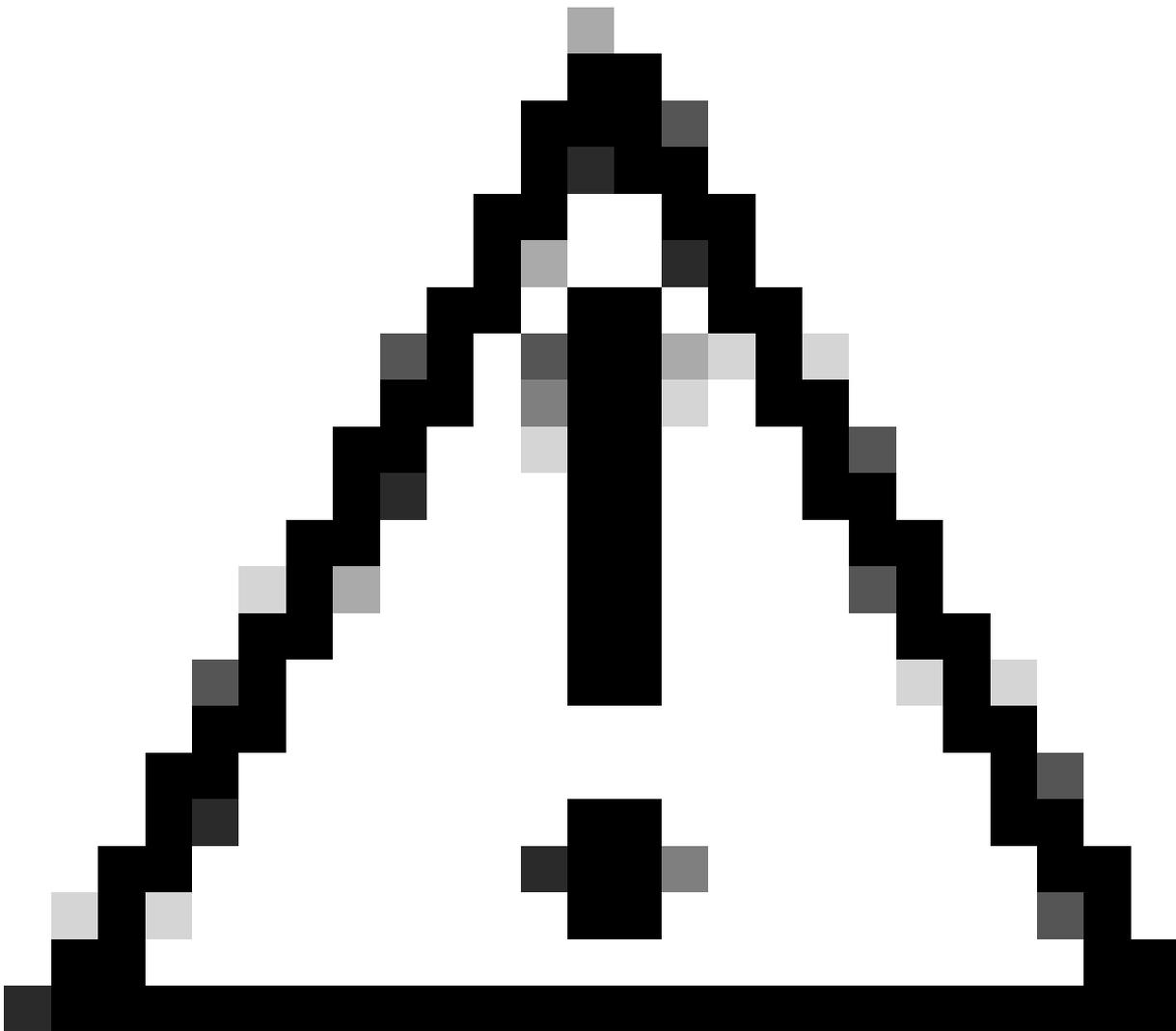
- 適用於VMWare的Cisco Firepower管理中心7.4.1
- Cisco Firepower 2120 7.4.1

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

自訂本機Snort規則是指使用者定義規則，您可以在整合至FTD的Snort入侵偵測與防禦系統中建立及實作。在Cisco FTD中建立自訂本機Snort規則時，基本上就是定義了Snort引擎可以注意的新模式或條件集。如果網路流量符合自定義規則中指定的條件，Snort可以採取規則中定義的操作，例如生成警報或丟棄資料包。管理員使用自定義本地Snort規則處理一般規則集未涵蓋的特定威脅。

本文檔介紹了如何配置和驗證用於檢測和丟棄包含特定字串（使用者名稱）的HTTP響應資料包的自定義本地Snort規則。

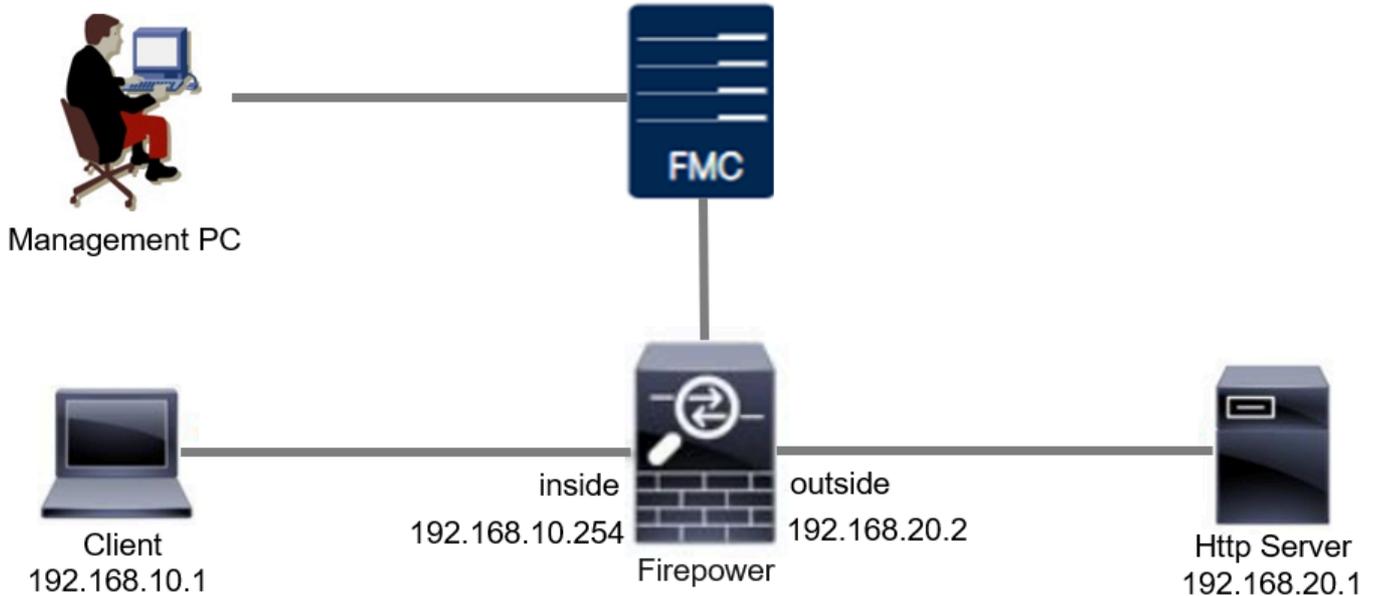


注意：建立自定義本地Snort規則並為其提供支援不屬於TAC支援範圍。因此，本文檔只能用作參考，並要求您自行斟酌決定並自行負責建立和管理這些自定義規則。

設定

網路圖表

本文檔介紹此圖中Snort2自定義本地Snort規則的配置和驗證。



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。

步驟 1. 確認Snort版本

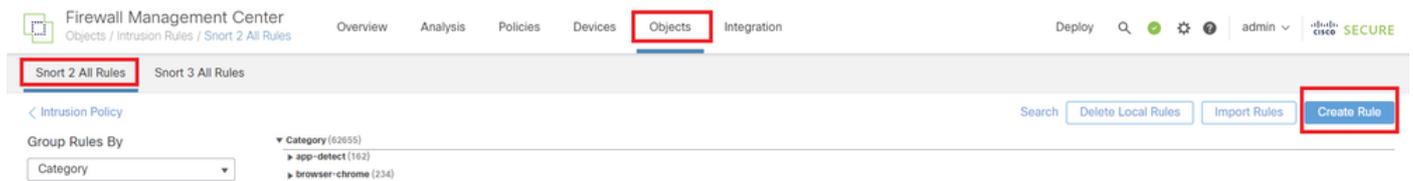
導航到裝置 > FMC上的裝置管理，點選裝置頁籤。確認snort版本為Snort2。

The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' tab is selected, and the configuration for a Cisco Firepower 2120 Threat Defense device is displayed. The 'Inspection Engine' section is highlighted, showing 'Inspection Engine: Snort 2'.

Snort版本

步驟 2. 在Snort 2中建立自定義本地Snort規則

在FMC上導航到Objects > Intrusion Rules > Snort 2 All Rules，然後按一下Create Rule按鈕。

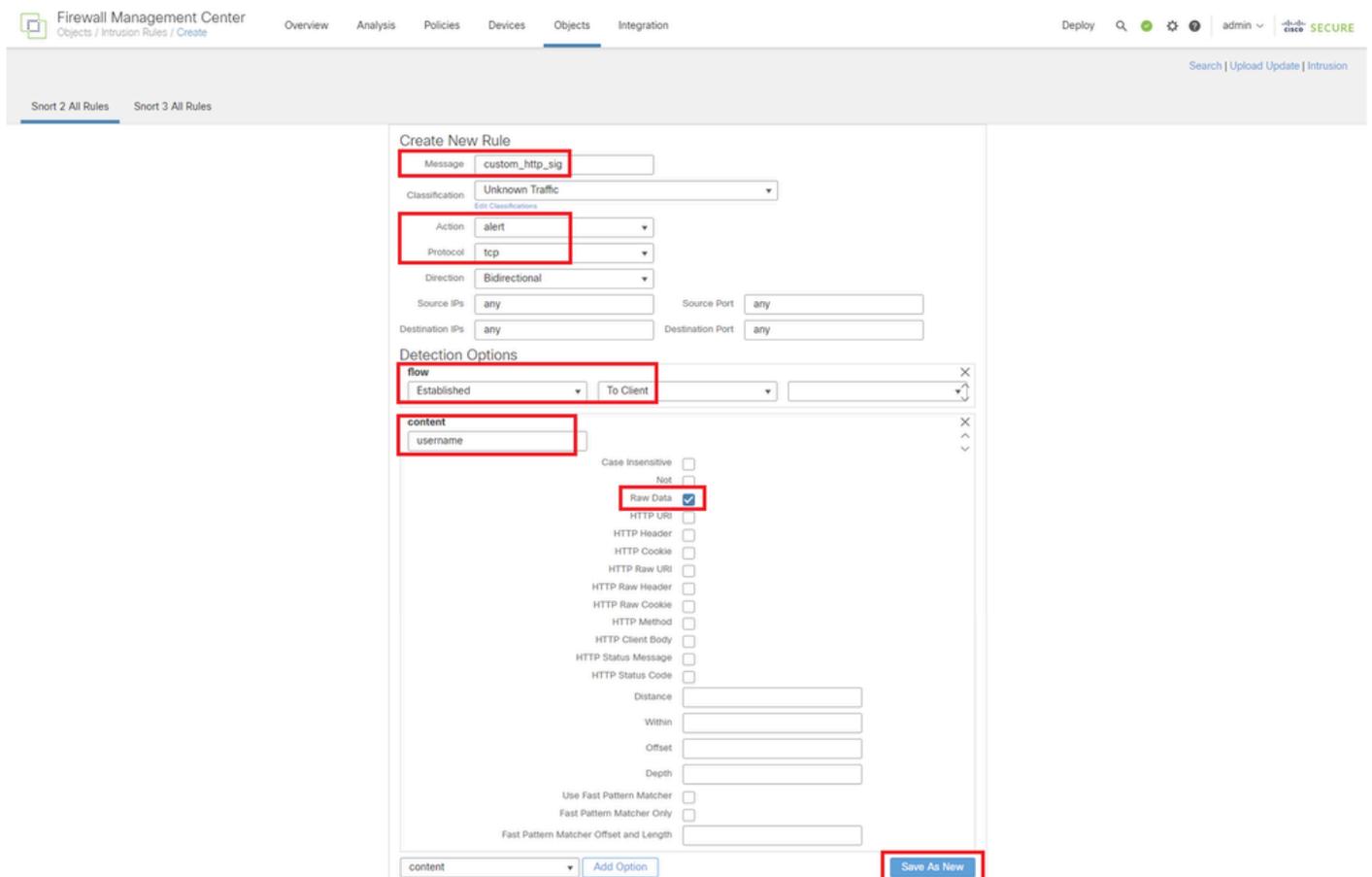


建立自訂規則

輸入自定義本地Snort規則的必要資訊。

- 入侵 (客戶端/惡意客戶端) : custom_http_sig
- 操作 : 警報
- 協定 : tcp
- flow : Established , 到客戶端

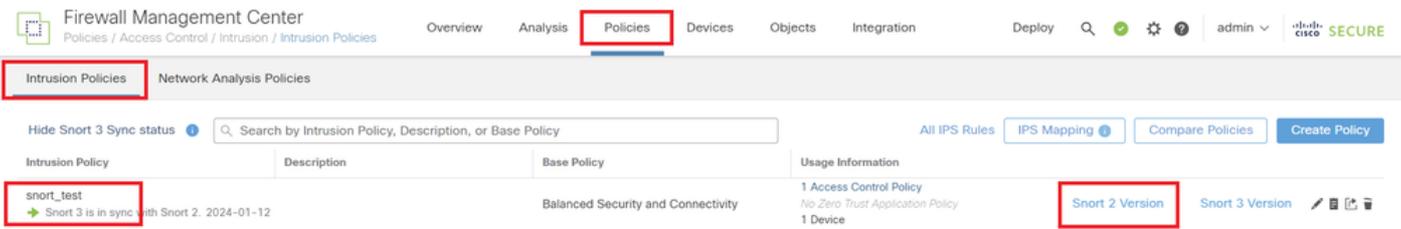
- 內容 : 使用者名稱 (原始資料)



輸入規則的必要資訊

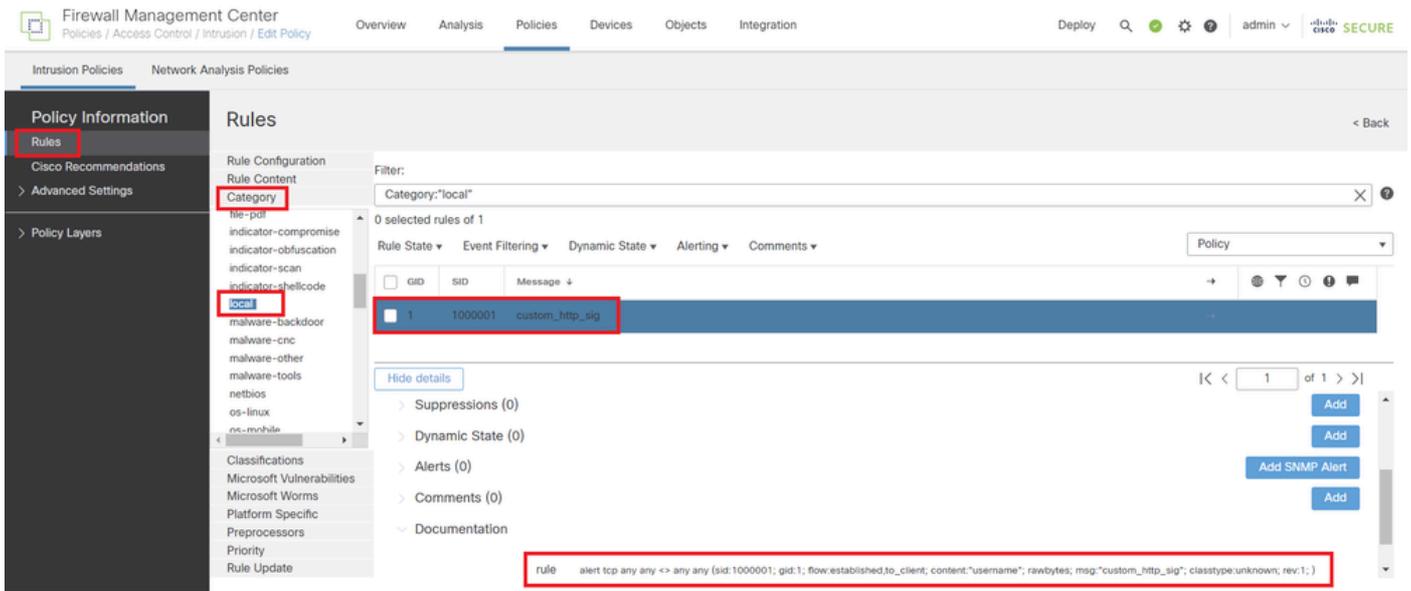
步驟 3. 確認自定義本地Snort規則

導航到FMC上的Policies > Intrusion Policies，點選Snort 2 Version按鈕。



確認自定義規則

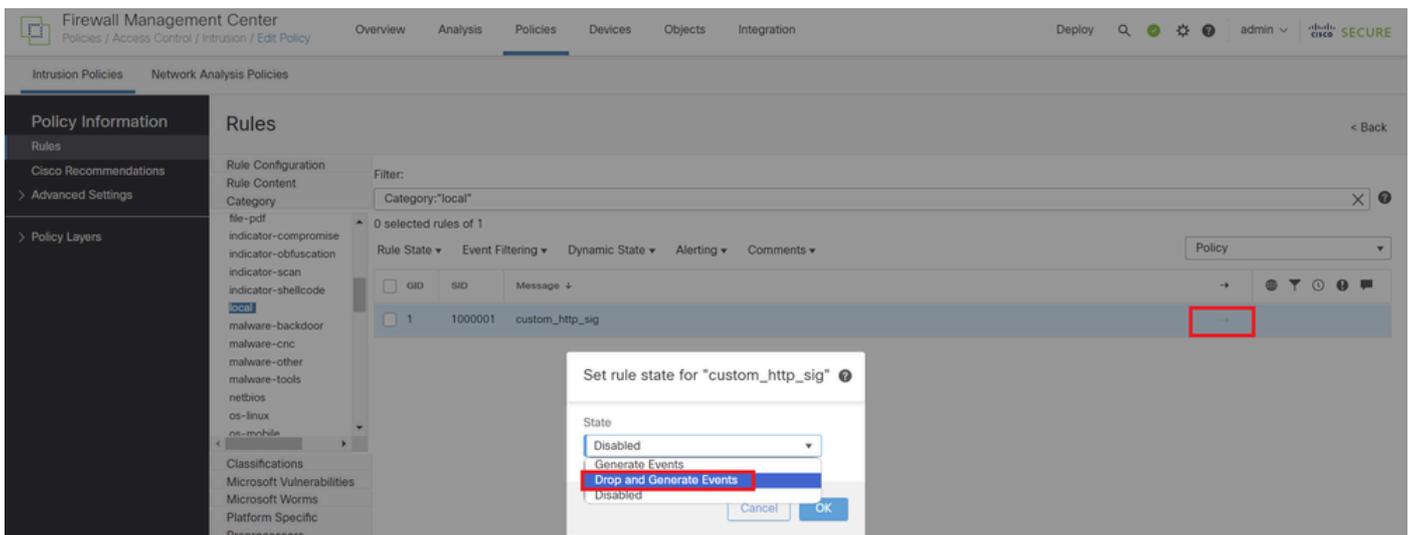
導航到FMC上的規則 >類別>本地，確認自定義本地Snort規則的詳細資訊。



自定義規則的詳細資訊

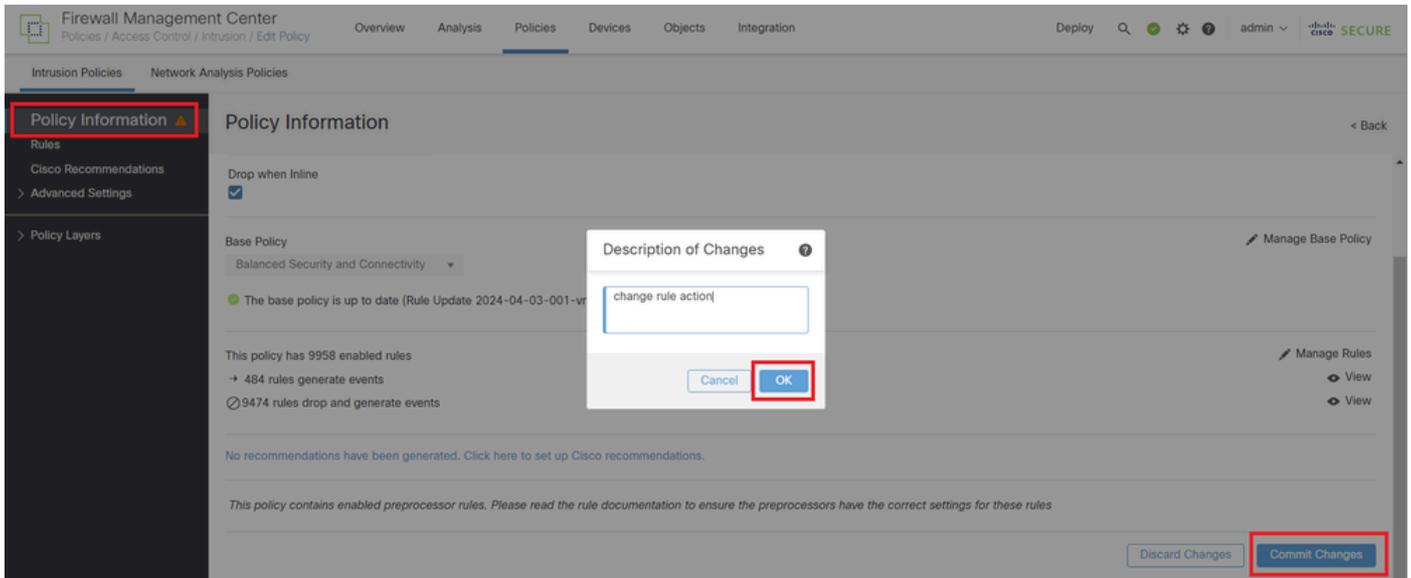
步驟 4. 變更規則動作

按一下State按鈕，將State設定為Drop and Generate Events，然後按一下OK按鈕。



變更規則動作

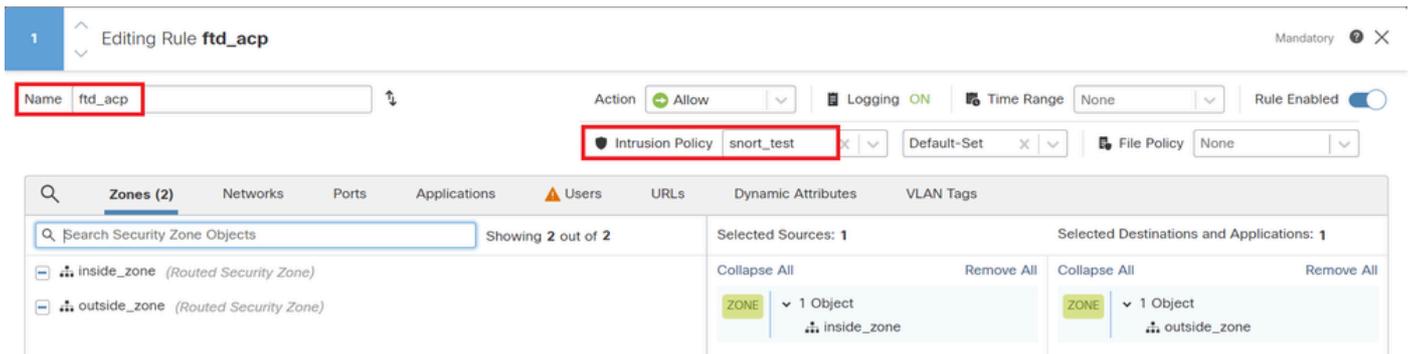
依次按一下Policy Information 按鈕和Commit Changes 按鈕以儲存更改。



提交更改

步驟 5. 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 (在FMC上) , 將入侵策略與ACP關聯。



與ACP規則關聯

步驟 6. 部署變更

將變更部署到FTD。



部署變更

驗證

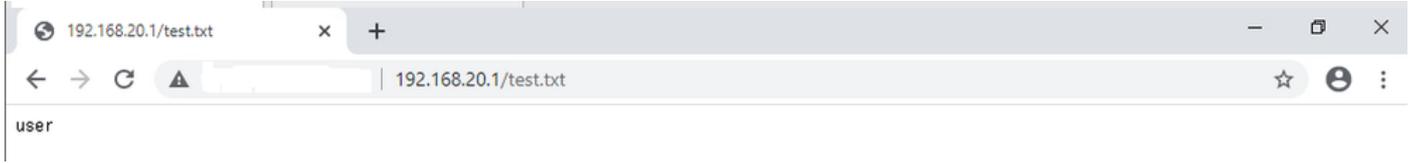
未觸發自定義本地Snort規則

步驟 1. 設定HTTP伺服器中的檔案內容

將HTTP伺服器端的test.txt檔案內容設定為使用者。

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)，並確認允許HTTP通訊。



初始HTTP請求

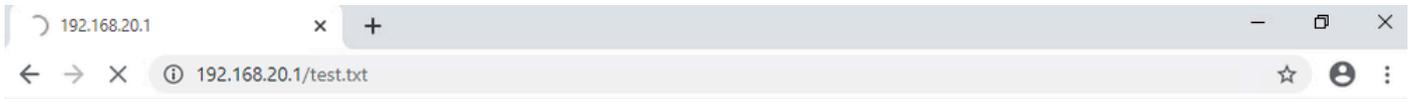
已觸發自定義本地Snort規則

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

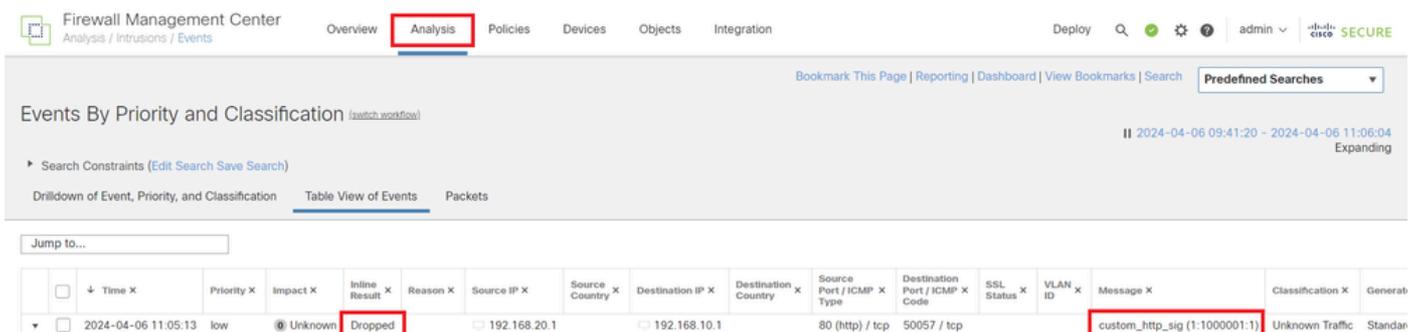
從使用者端(192.168.10.1)的瀏覽器存取HTTP伺服器(192.168.20.1/test.txt)，並確認已封鎖HTTP通訊。



初始HTTP請求

步驟 3. 確認入侵事件

在FMC上導航到分析 > 入侵 > 事件，確認入侵事件由自定義本地Snort規則生成。



入侵事件

按一下Packets頁籤，確認入侵事件的詳細資訊。

Firewall Management Center
Analysis / Intrusions / Events

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Admin Admin Panel

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search

Predefined Searches

Events By Priority and Classification (watch workflow)

Search Constraints (Edit Search Save Search)

Drilldown of Event, Priority, and Classification Table View of Events **Packets**

Event Information

Message: custom_http_sig (1:1000001:1)

Time: 2024-04-06 11:06:34

Classification: Unknown Traffic

Priority: low

Ingress Security Zone: outside_zone

Egress Security Zone: inside_zone

Device: FPR2120_FTD

Ingress Interface: outside

Egress Interface: inside

Source IP: 192.168.20.1

Source Port / ICMP Type: 80 (http) / tcp

Destination IP: 192.168.10.1

Destination Port / ICMP Code: 50061 / tcp

HTTP Hostname: 192.168.20.1

HTTP URI: /test.txt

Intrusion Policy: snort_test

Access Control Policy: acp_rule

Access Control Rule: ftd_acp

Rule: alert tcp any any -> any any (sid:1000001; gid:1; flow:established,to_client; content:'username'; raxbytes: size:'custom_http_sig'; classtype:unknown; rev:1;)

Actions

入侵事件的詳細資訊

疑難排解

運行system support trace命令以確認FTD上的行為。在本示例中，HTTP流量被IPS規則阻止(gid 1，sid 1000001)。

```
<#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:
```

```
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

```
ftd_acp
```

```
', allow
```

```
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0
```

```
IPS Event
```

```
:
```

```
gid 1
```

```
,
```

```
sid 1000001
```

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ==>

Blocked by IPS

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）。