

在FMC上配置其他Snort 3規則操作

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[功能詳細資訊](#)

[FMC演練](#)

簡介

本檔案將介紹Firepower管理中心(FMC)對7.1版本中新增的其他Snort 3規則操作功能的支援。

背景資訊

雖然Firepower威脅防禦(FTD)在7.0中支援七個入侵策略規則操作警報/禁用/阻止/拒絕/重寫/通過/丟棄，但FMC僅支援三個Snort 3規則操作：「Alert」、「Disable」和「Block」。

從Firepower 7.1.0中，FMC支援配置新規則操作。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解開源Snort
- Firepower管理中心(FMC)7.1.0+
- Firepower威脅防禦(FTD)7.0.0+

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 本文檔適用於運行Snort 3的所有Firepower平台
- 思科Firepower威脅防禦虛擬(FTD)，運行軟體版本7.4.2
- 運行7.4.2版軟體的Firepower管理中心虛擬(FMC)

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。

功能詳細資訊

新增的新Snort 3規則操作及其說明如下：

通過：不生成任何事件，允許資料包通過，而無需後續任何Snort規則進行進一步評估。

Drop:生成事件，丟棄匹配的資料包，並且不會阻塞此連線中的更多流量。

拒絕：生成事件、丟棄匹配資料包、阻止此連線中的更多流量並向源主機和目的主機傳送TCP重置或ICMP埠不可達。

重寫：根據規則中的replace選項生成事件並覆蓋資料包內容。

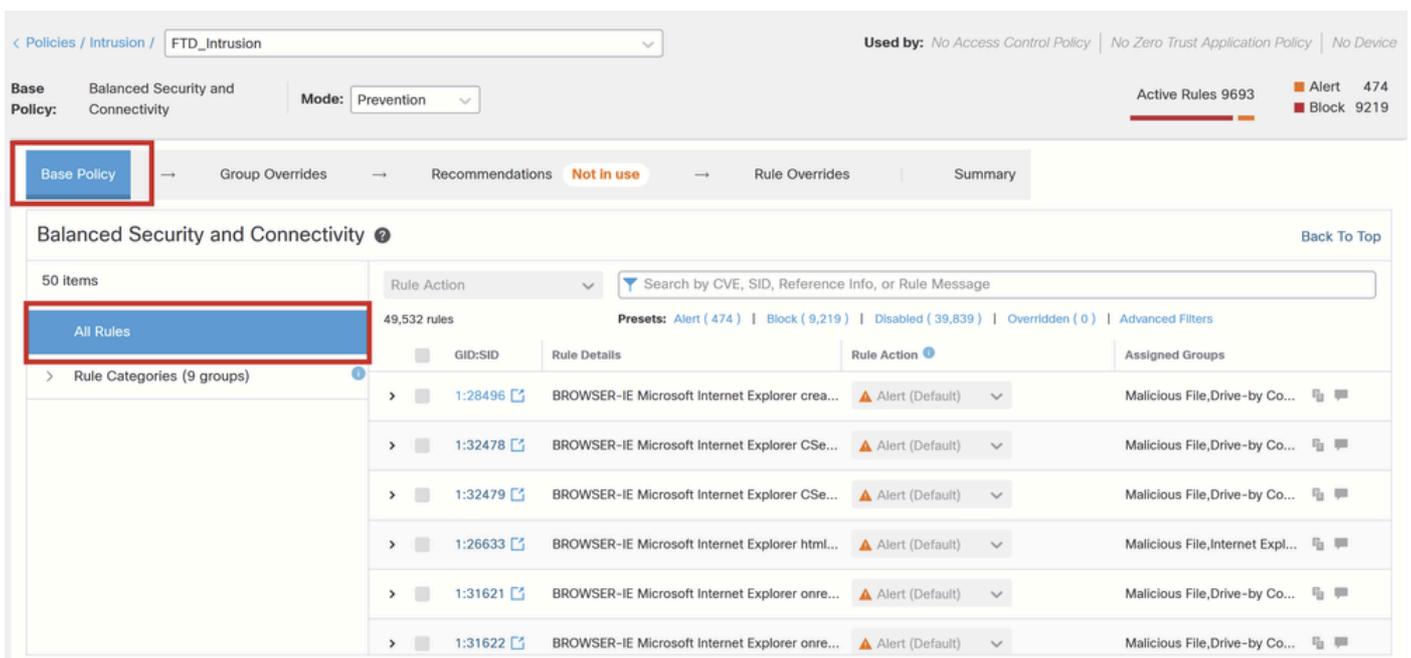
FMC演練

要檢視入侵策略中的Snort 3規則，請導航至FMC Policies > Access Control > Intrusion,然後，按一下策略右上角的Snort 3版本選項，如下圖所示：



Snort 3版本

按一下Base Policy > All Rules，可以看到所有系統定義的Snort 3規則的預設操作。



基本策略

要將規則操作更改為任何這些新規則操作，請導航至規則覆蓋>所有規則，然後從所選規則的下拉選

單中選擇規則操作。

The screenshot shows the 'Rule Overrides' page in a security management interface. The page title is 'Rule Overrides' and it shows 102 items. The 'Rule Action' dropdown menu is open, showing options: Alert (Default), Block, Alert (Default), Rewrite, Drop, Reject, Disable, and Revert to default. The 'Block' option is highlighted with a red box. The table below shows a list of rules with columns for 'GID:SID', 'Rule Details', 'Rule Action', 'Set By', and 'Assigned Groups'. The first rule is 1:28496 BROWSER-IE Microsoft Internet ... with the 'Alert (Default)' action.

其他規則操作

The screenshot shows the 'Rule Overrides' page with a notification: 'Rule action changed successfully'. The 'Rule Action' dropdown menu is open, showing options: Reject, Alert (Default), Alert (Default), and Alert (Default). The 'Reject' option is highlighted with a red box. The table below shows a list of rules with columns for 'GID:SID', 'Rule Details', 'Rule Action', 'Set By', and 'Assigned Groups'. The first rule is 1:28496 BROWSER-IE Microsoft Internet ... with the 'Reject' action.

更改規則操作

在Rule Overrides > Overridden Rules下可以找到被覆蓋的規則。

< Policies / Intrusion / FTD_Intrusion

Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity | Mode: Prevention

Active Rules 9693 | Alert 473 | Block 9219 | Others 1

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

Rule Overrides

102 items | All x

Search by CVE, SID, Reference Info, or Rule Message

Presets: Alert (0) | Block (0) | Disabled (0) | **Overridden (1)** | Advanced Filters | Reject (1)

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
> 1:28496	BROWSER-IE Microsoft Internet ...	Reject		Malicious File, Drive...

被覆蓋規則

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）。