

瞭解FMC GUI上的Snort 3規則分析和CPU分析

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[功能概述](#)

[分析](#)

[規則探查器](#)

[運行規則分析](#)

[Snort 3效能分析選單](#)

[啟動規則分析](#)

[規則探查器結果](#)

[下載結果](#)

[CPU分析](#)

[Snort 3 CPU分析器概述](#)

[「CPU分析」頁籤](#)

[已解釋CPU分析器結果](#)

[CPU分析器結果 — 下載快照](#)

[CPU分析結果過濾](#)

簡介

本文檔介紹在FMC 7.6上新增的Snort 3規則和CPU分析功能。

必要條件

需求

思科建議您瞭解以下主題：

- Snort知識3
- 安全Firepower管理中心(FMC)
- 安全Firepower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：

- 本檔案適用於所有Firepower平台

- 執行軟體版本7.6.0的安全防火牆威脅防禦虛擬(FTD)
- 執行軟體版本7.6.0的安全防火牆管理中心虛擬(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。

功能概述

- Snort中已存在規則和CPU分析，但只能通過FTD CLI訪問。此功能的目標是擴展分析功能並使其更加簡單。
- 啟用debug intrusion rule performance issues並自行調整規則配置，然後聯絡TAC獲取故障排除幫助。
- 瞭解當Snort 3佔用高CPU時，哪些模組的效能不令人滿意。
- 建立使用者友好的方式來調試和微調入侵和網路分析策略以提高效能。

分析

- 規則分析和CPU分析都在FTD上運行，其結果儲存在裝置上，由FMC拉動。
- 您可以在不同的裝置上同時運行多個分析會話。
- 可以同時運行規則分析和CPU分析。
- 如果是高可用性，分析只能在會話開始時處於活動狀態的裝置上啟動。對於群集設定，可以在群集中的每個節點上運行效能分析。
- 如果在正在進行效能分析會話時觸發部署，則會向使用者顯示警告。

如果使用者選擇忽略警告並進行部署，則會取消當前分析會話，分析器結果會顯示有關此問題的消息。

新的分析會話需要在不被部署中斷的情況下啟動，才能獲得實際的分析結果。

規則探查器

- Snort 3規則探查器收集有關處理一組Snort 3入侵規則所用時間量的資料，從而突出顯示潛在問題，顯示效能不令人滿意的規則。
- Rule Profiler顯示100條檢查時間最長的IPS規則。
- 觸發規則探查器不需要重新載入或重新啟動Snort 3。
- 規則分析結果以JSON格式儲存在/ngfw/var/sf/sync/snort_profiling/目錄中，並在FMC上同步。
- 規則探查器位於Snort 3中，並使用Snort 3入侵檢測機制檢查流量；啟用規則分析對效能沒有任何顯著影響。

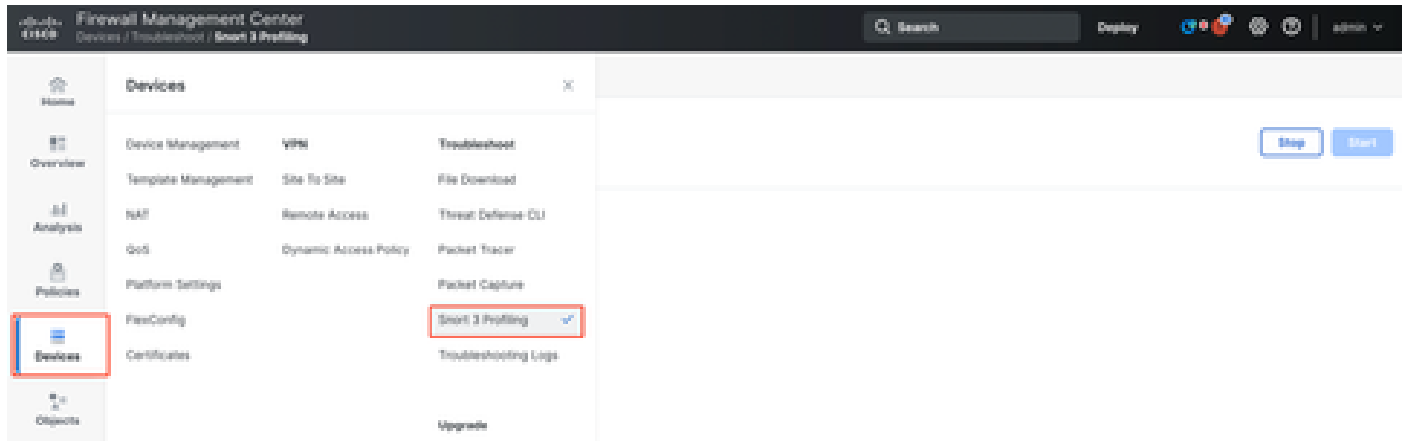
運行規則分析

- 流量必須流經裝置
- 通過選擇裝置，然後按一下「開始」按鈕啟動規則分析
 - 啟動效能分析會話將建立一個任務，該任務可在「任務」下的「通知」中進行監視
- 規則分析會話的預設持續時間為120分鐘
 - 通過按Stop按鈕，可在完成之前更快地停止Rule Profiling會話
- 結果可在GUI中檢視並下載

- 「效能分析歷史記錄」顯示以前的效能分析會話結果。使用者可以通過從「效能分析歷史記錄」左側面板中按一下卡來檢查特定的效能分析結果。

Snort 3效能分析選單

可以從Devices > Snort 3 Profiling選單訪問「效能分析」頁。該頁包含規則和CPU分析，分為兩個頁籤。



裝置

啟動規則分析

要啟動規則分析會話，請按一下Start。會話在120分鐘後自動停止。

使用者無法配置效能分析會話的長度，但可以在兩小時過去之前停止該會話。



規則分析

Rule Profiling CPU Profiling

Select device for Rule Profiling

FTD1 Running Stop Start



Rule Profiling started 8 seconds ago

Profiling takes around 120 minutes. The task manager will send notification when the profiling task is complete.

running

啟動規則分析會話後，將建立一個任務。可以在Notifications > Tasks中選中此選項。

Deployments Upgrades Health **Tasks** Show Pop-up Notifications

20+ total 0 waiting 3 running 0 retrying 20+ success 1 failure

Rule profiler

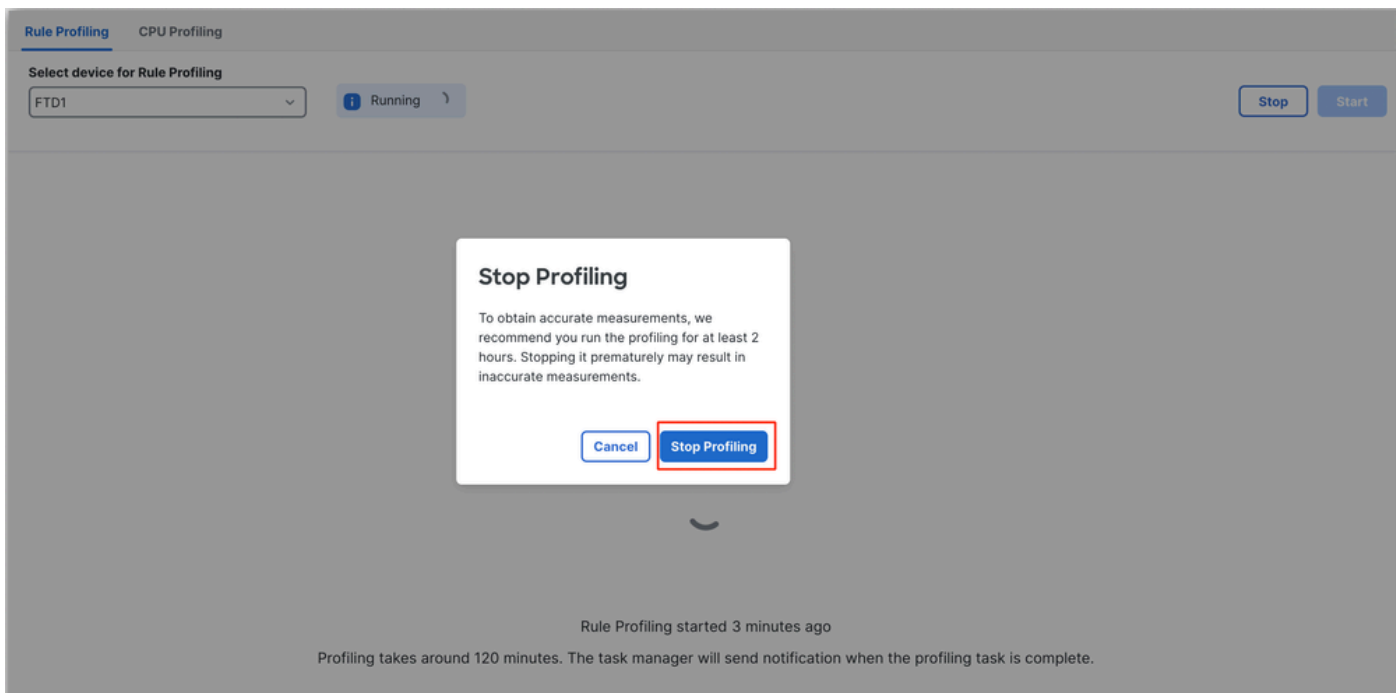
Generate Rule Profiling File 2m 6s

Generate rule profiling file for FTD1

Remote status: Generating rule profiling file

工作

要停止正在進行的規則分析會話，如果您需要在自動停止之前中斷它，請按一下停止並確認。



停止分析

選擇裝置後，最新的效能分析結果會自動顯示在Rule Profiling Results部分。

該表包含規則的統計資訊，這些規則處理花費的時間最多，按它們花費的總時間(以微秒(μ s)為單位進行降序排序。

Filter by % of Snort time Search Total 40

Guid/Sid	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (μ s)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html	0.00003%	13	17	0	0	143	8	0	8	0	0
1:28585	FILE-PDF Adobe Acrobat Reader OTF font head table size overflow atte...	0.00001%	8	16	0	0	49	3	0	3	0	0
1:47030	MALWARE-CNC Win.Malware.Innaput variant outbound connection	0.00001%	1	37	0	0	44	1	0	1	0	0
1:37651	MALWARE-TOOLS Win.Trojan.Downloader outbound connection attempt	0.00001%	3	6	0	0	42	7	0	7	0	0

結果

規則探查器結果

IPS規則的規則探查器輸出包括以下欄位：

- Snort時間百分比 — 處理規則所花費的時間，相對於Snort 3的操作時間
- Checks - IPS規則執行的次數
- Matches - IPS規則完全匹配的次數
- Alerts - IPS規則觸發IPS警報的次數
- Time(μ s)- Snort檢查IPS規則所用的時間 (以微秒為單位)
- Avg/Check - Snort對規則進行一次檢查所用的平均時間
- Avg/Match - Snort在一次檢查中導致匹配所花費的平均時間
- Avg/Non-Match - Snort執行一次未導致匹配的檢查所花費的平均時間
- 超時 — 規則超出規則處理的次數 — 在AC策略的基於延遲的效能設定中配置的閾值
- Suspends — 由於連續出現閾值違規而暫停規則的次數

下載結果

- 使用者可以通過按一下「Download Snapshot」按鈕下載效能分析結果(「snapshot」)。下載的檔案採用.csv格式，並包含配置檔案結果頁面中的所有欄位。
- 從快照.csv檔案中提取：

Device,Start Time,End Time,GID:SID,Rule Description,% of Snort Time,Rev,Checks,Matches,Alerts,Time (µs)

快照.csv檔案檢視：

Rule_Profiling_172.16.0.102_2024-03-13 11_08_41

Device	Start Time	End Time	GID:SID	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (µs)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	2000:1000001	TEST 1	0.00014	1	4	4	1	284	71	71	0	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:28585	FILE-PDF Adobe Acrobat Reader OTF font table size overflow attempt	0.00006	8	4	0	0	113	28	0	28	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html	0.00003	13	4	0	0	64	16	0	16	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:55993	PROTOCOL-ICMP Microsoft Windows IPv6 DNSSL option record denial of service attempt	0.00002	1	4	0	0	32	8	0	8	0	0

快照

CPU分析

Snort 3 CPU分析器概述

- CPU分析器會分析Snort 3的模組/檢查員在給定時間間隔內處理資料包所花費的CPU時間。它提供了每個模組消耗的CPU數量（相對於Snort 3進程消耗的CPU總數）的資訊。
- 使用CPU探查器不需要重新載入配置或重新啟動Snort 3，從而避免了停機時間。
- CPU分析器結果顯示所有模組在上次分析會話期間所用的處理時間。
- CPU分析結果以JSON格式儲存在/ngfw/var/sf/sync/cpu_profiling/目錄下，並在FMC /var/sf/peers/<device UUID>/sync/cpu_profiling目錄上同步。
- 在FMC UI中新增了新的Snort 3分析頁面
- 可以從Devices > Snort 3 Profiling選單> CPU Profiling頁籤訪問此頁
- 使用CPU分析頁籤上的Download Snapshot，以CSV格式下載分析結果的快照。

「CPU分析」頁籤

可從Devices > Snort 3 Profiling 選單> CPU Profiling 頁籤訪問「CPU Profiling」頁面。

它包含裝置選擇器、Start/Stop按鈕、Download Snapshot按鈕、效能分析結果部分，以及左側的Profiling History部分，按一下該部分時將展開該部分。

Firewall Management Center
 Devices / Troubleshoot / Snort 3 Profiling

Search Deploy admin

Home Overview Analysis Policies **Devices** Objects Integration

Rule Profiling **CPU Profiling**

Select device for CPU Profiling
 FTD1 Stop Start

CPU Profiling Results - FTD1 (30 seconds ago) Download Snapshot

Start: 2025-01-16 10:18:25 IST Access Control Policy: test VDB: 392 Snort Version: 3.1.79.1-121
 Finish: 2025-01-16 11:14:01 IST Access Control Policy revision time: 2025-01-15 13:15:26 IST LSP: lsp-rel-20250114-1341 Device Version: 7.6.0-113

Filter by % of Snort time Search Total 4

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
daq	100	6674110782	893694	100
perf_monitor	0	39946	5	0
firewall	0	16360	2	0
mpse	0	2181	0	0

Cpu分析

要啟動CPU分析會話，請按一下啟動。啟動會話時會顯示此頁面。

Rule Profiling **CPU Profiling**

Select device for CPU Profiling
 FTD1 Stop Start

CPU Profiling Results - FTD1 (30 seconds ago) Download Snapshot

Start: 2025-01-16 10:18:25 IST Access Control Policy: test VDB: 392 Snort Version: 3.1.79.1-121
 Finish: 2025-01-16 11:14:01 IST Access Control Policy revision time: 2025-01-15 13:15:26 IST LSP: lsp-rel-20250114-1341 Device Version: 7.6.0-113

Filter by % of Snort time Search Total 4

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
daq	100	6674110782	893694	100
perf_monitor	0	39946	5	0
firewall	0	16360	2	0
mpse	0	2181	0	0

開始

State Profiling CPU Profiling

Select device for CPU Profiling

FTD1 Running

Dismiss all notifications

CPU profiler
Generate CPU Profiling File
Generate CPU profiling file for FTD1
Remote status: Generating CPU profiling file

CPU Profiling started 8 seconds ago
Profiling takes around 120 minutes. The task manager will send notification when the profiling task is complete.


running

啟動CPU分析會話後，將建立一個任務。可以將其簽入Notifications > Tasks。

! Deployments Upgrades ! Health ! **Tasks** ↓

20+ total 0 waiting 2 running 0 retrying 20+ success

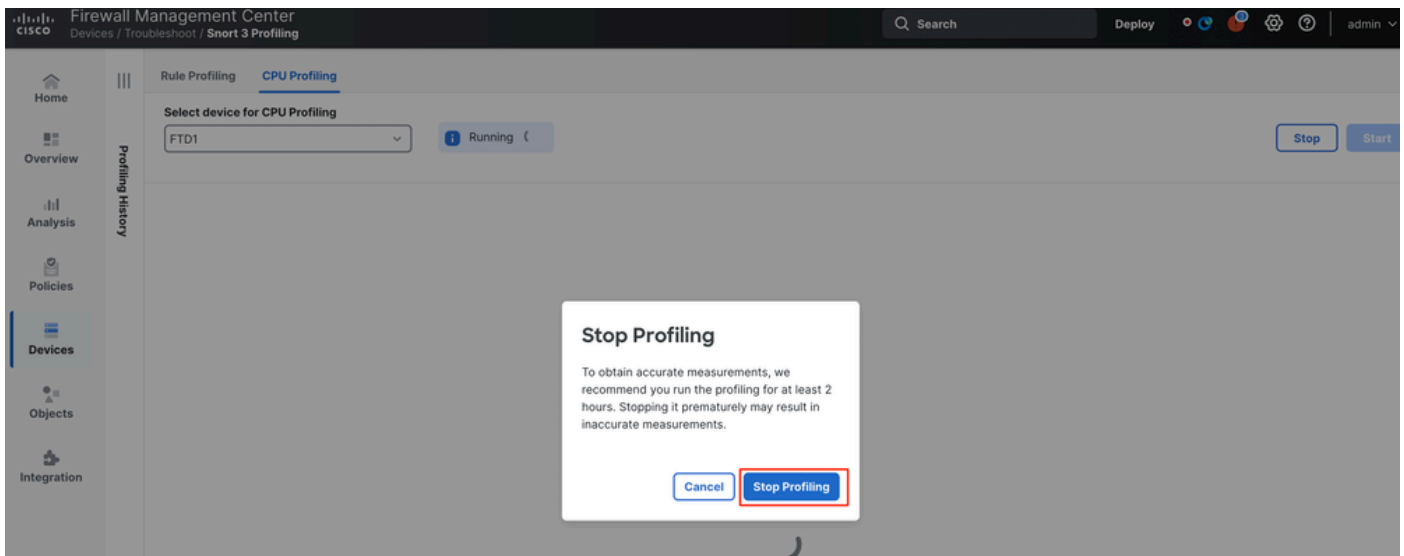
1 failure

 CPU profiler

Generate CPU Profiling File
Generate CPU profiling file for FTD1
Remote status: Generating CPU profiling file

工作

- 要停止正在進行的CPU分析會話，請按一下停止。
- 此時將顯示確認對話方塊。按一下Stop Profiling。



停止運行

最新的效能分析結果將顯示在「CPU效能分析結果」部分。

CPU Profiling Results - FTD1 (20 seconds ago) [Download Snapshot](#)

Start: 2025-01-16 11:20:00 EST Access Control Policy: local VM: 393 Snort Version: 3.1.78.1-101
Profile: 2025-01-16 11:23:04 EST Access Control Policy revision time: 2025-01-15 13:10:28 EST LSP: top-net-20050014-1041 Device Version: FTD-110

Filter by % of Snort time Search Total 4

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
diag	100	394444909	900060	100
perf_monitor	0	1462	4	0
firewall	0	913	3	0
mgmt	0	101	0	0

結果

已解釋CPU分析器結果

- 「模組」列表示模組/檢查器的名稱。
- 「% Total of CPU Time」(CPU總時間百分比)列表示模組在處理流量時花費的時間相對於Snort 3花費的總時間的百分比。如果該值明顯大於其他模組的值，則模組對Snort 3的效能不滿意的貢獻更大。
- 「時間(µs)」表示每個模組所花費的總時間(以微秒為單位)。
- 「Avg/Check」表示每次呼叫模組時模組花費的平均時間。
- 「% Caller」表示子模組(如果已配置)相對於主模組所用的時間。主要用於開發者調試的目的。

CPU分析器結果 — 下載快照

- 使用者可以通過按一下Download Snapshot來下載效能分析結果快照。下載的檔案採用.csv格式，並包含分析結果頁面中的所有欄位，如本例所示。
- 從快照.csv檔案中提取：

CPU_Profiling_FTD1_2025-01-16 00_55_45

Device	Start Time	End Time	Module	% Total of CPU time	Time (μs)	Avg/Check	%/Caller
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	daq	100	366446909	900360	100
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	perf_monitor	0	1662	4	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	firewall	0	923	2	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	mpse	0	101	0	0

快照

CPU分析結果過濾

可使用以下內容過濾效能分析結果：

- 「按Snort時間的%過濾」 — 允許您過濾執行時間超過分析時間n%的模組。
- 搜尋(Search) — 允許您對結果表中存在的任何欄位執行文本搜尋。

除「模組」以外的任何列都可以按一下其標題進行排序。

Filter by % of Snort time 0.20 % Total 10

Module	% Total of CPU time	Time (μs)	Avg/Check	% Caller
rule_eval	20.89	26138283	3	20.89
mpse	14.11	17661177	0	14.11

結果

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）。