了解FMC GUI上的Snort 3规则分析和CPU分析

目录

简介

本文档介绍在FMC 7.6上添加的Snort 3规则和CPU分析功能。

先决条件

要求

Cisco 建议您了解以下主题：

· Snort知识3
·安全Firepower管理中心(FMC)
·安全Firepower威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 本文档适用于所有Firepower平台

- 运行软件版本7.6.0的安全防火墙威胁防御虚拟(FTD)
- 运行软件版本7.6.0的安全防火墙管理中心虚拟(FMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

功能概述

- Snort中已存在规则和CPU分析，但只能通过FTD CLI访问。此功能的目的是扩展分析功能并使之更加简单。
- 启用debug intrusion rule performance issues并自行调整规则配置，然后联系TAC获取故障排除帮助。
- 了解当Snort 3消耗高CPU时，哪些模块的性能不理想。
- 创建用户友好的方式来调试和微调入侵和网络分析策略，以获得更好的性能。

分析

- Rule Profiling和CPU Profiling都在FTD上运行，其结果存储在设备上并由FMC调用。
- 您可以在不同的设备上同时运行多个分析会话。
- 您可以同时运行规则分析和CPU分析。
- 在高可用性情况下，只能在会话开始时处于活动状态的设备上启动分析。
  对于集群设置，可以在集群中的每个节点上运行分析。
- 如果在分析会话正在进行时触发部署，则会向用户显示警告。

如果用户选择忽略警告并进行部署，则会取消当前分析会话，分析器结果会显示有关此问题的消息。

新的分析会话需要在不被部署中断的情况下启动，才能获得实际的分析结果。

规则分析器

- Snort 3规则分析器收集有关处理一组Snort 3入侵规则所花费时间的数据，从而突出显示潜在问题，显示性能不令人满意的规则。
- Rule Profiler显示100条检查时间最长的IPS规则。
- 触发规则分析器不需要重新加载或重新启动Snort 3。
- 规则分析结果以JSON格式保存在/ngfw/var/sf/sync/snort_profiling/目录中，并在FMC上同步。
- 规则分析器位于Snort 3中，并使用Snort 3入侵检测机制检查流量；启用规则分析不会显着影响性能。

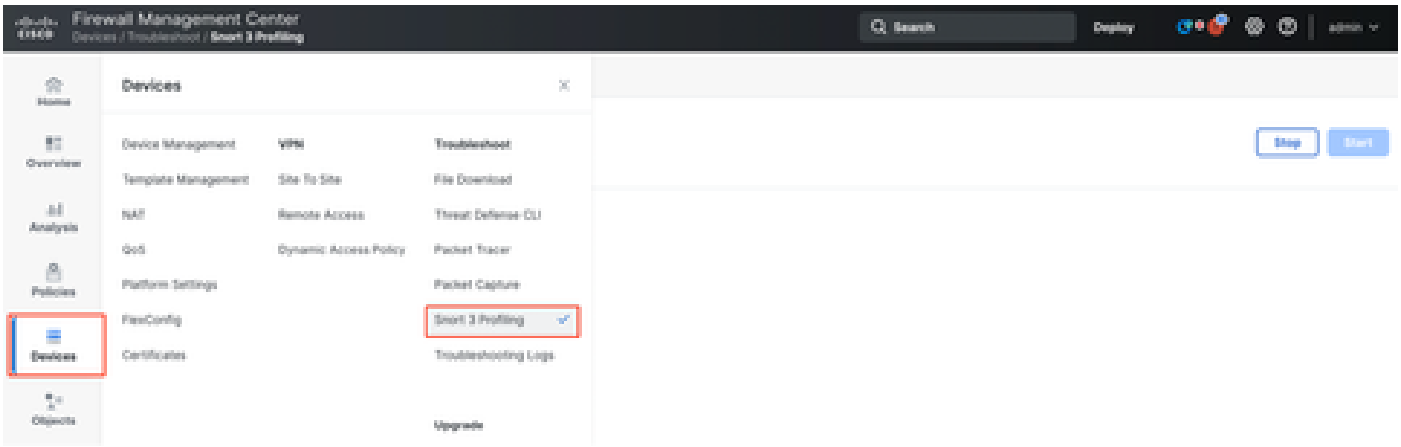
运行规则分析

- 流量必须流经设备
- 通过选择设备，然后点击Start按钮启动规则分析
  - 启动性能分析会话将创建一个任务，该任务可在“任务”下的“通知”中进行监控
- 规则分析会话的默认持续时间为120分钟
  - 通过按Stop按钮，规则分析会话可以在完成之前提前停止
- 结果可在GUI中查看并下载

- Profiling History显示先前的分析会话结果。用户可以通过单击Profiling History左侧面板中的卡来检查特定的分析结果。

Snort 3分析菜单

可以从Devices > Snort 3 Profiling菜单访问Profiling页面。该页面包含规则和CPU分析，分为两个选项卡。



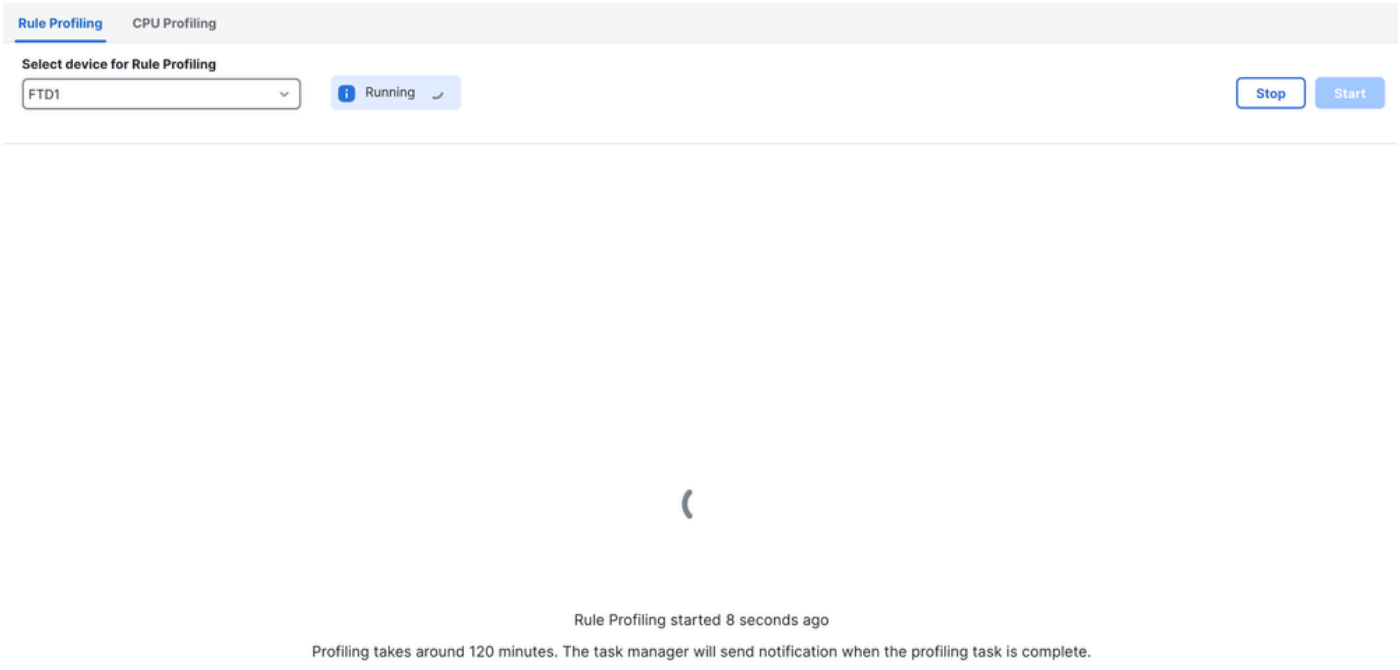
设备

启动规则分析

要启动规则分析会话，请单击Start。会话将在120分钟后自动停止。

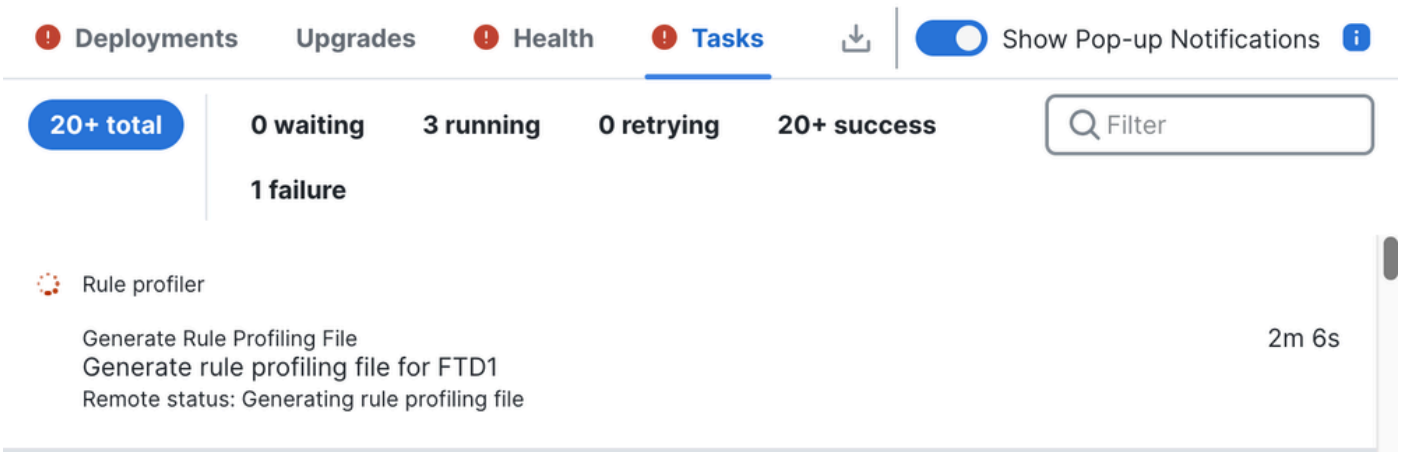
用户无法配置分析会话的长度，但可以在两小时过去之前将其停止。

规则分析



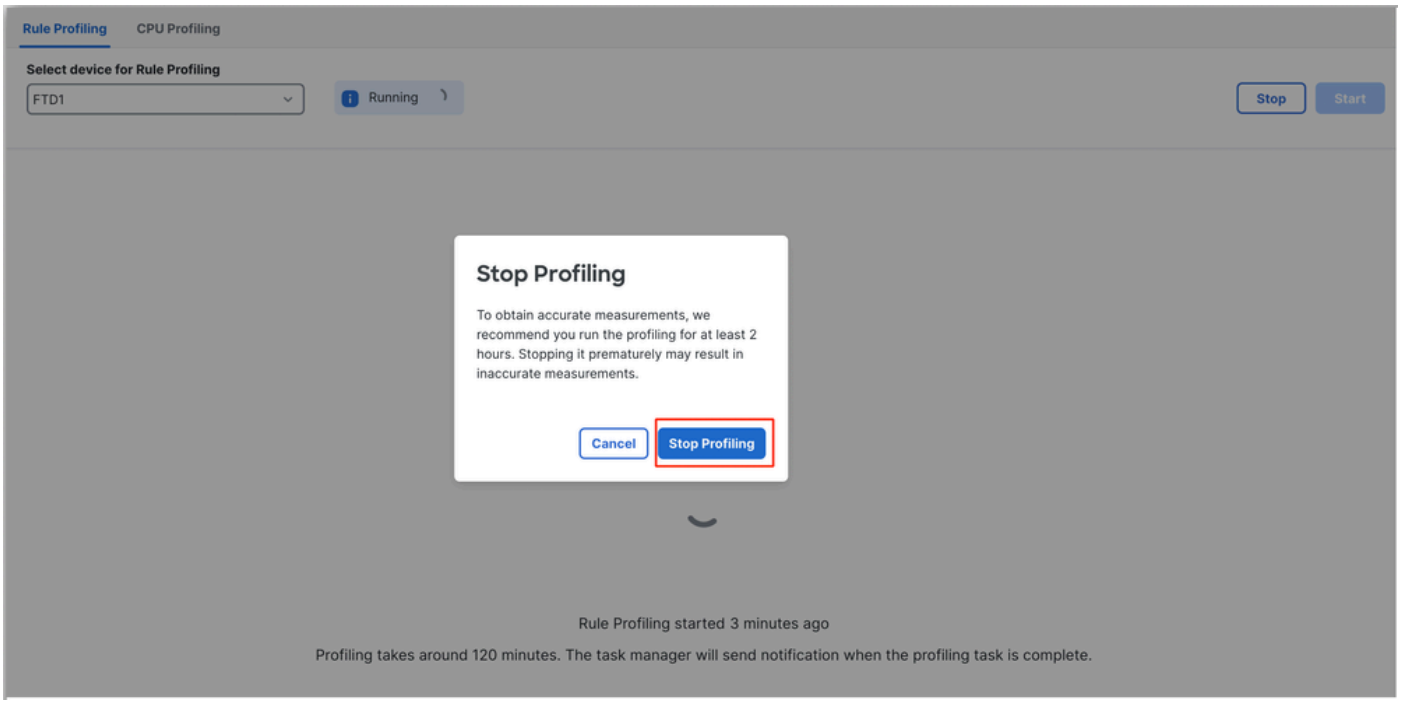
正在运行

启动规则分析会话后，将创建一个任务。可以在Notifications > Tasks中选中此项。



任务

要停止正在进行的规则分析会话（如果您需要在自动停止之前中断它），请单击Stop并确认。



停止分析

选择设备后，最新分析结果会自动显示在Rule Profiling Results部分中。

该表包含按总时间(以微秒(µs)为单位)降序排序的处理时间最长的规则的统计信息。

结果

规则分析器结果

IPS规则的规则分析器输出包括以下字段：

- Snort时间的百分比 — 处理规则所花费的时间，相对于Snort 3的操作时间
- Checks - IPS规则执行的次数
- Matches - IPS规则完全匹配的次数
- Alerts - IPS规则触发IPS警报的次数
- Time(µs)- Snort检查IPS规则所用的时间（以微秒为单位）
- Avg/Check - Snort对规则的一次检查所花费的平均时间
- Avg/Match - Snort在一次检查中导致匹配所花费的平均时间
- Avg/Non-Match - Snort执行一次未导致匹配的检查所花费的平均时间
- 超时 — 规则超出规则处理的次数 — 在AC策略的基于延迟的性能设置中配置的阈值
- Suspends — 由于某些连续阈值违规而暂停规则的次数

下载结果

- 用户可以通过点击“Download Snapshot”按钮下载分析结果(“snapshot”)。下载的文件是.csv格

式，包含分析结果页面中的所有字段。
- 从快照.csv文件中提取：

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

快照.csv文件视图：

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 CTF font head 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

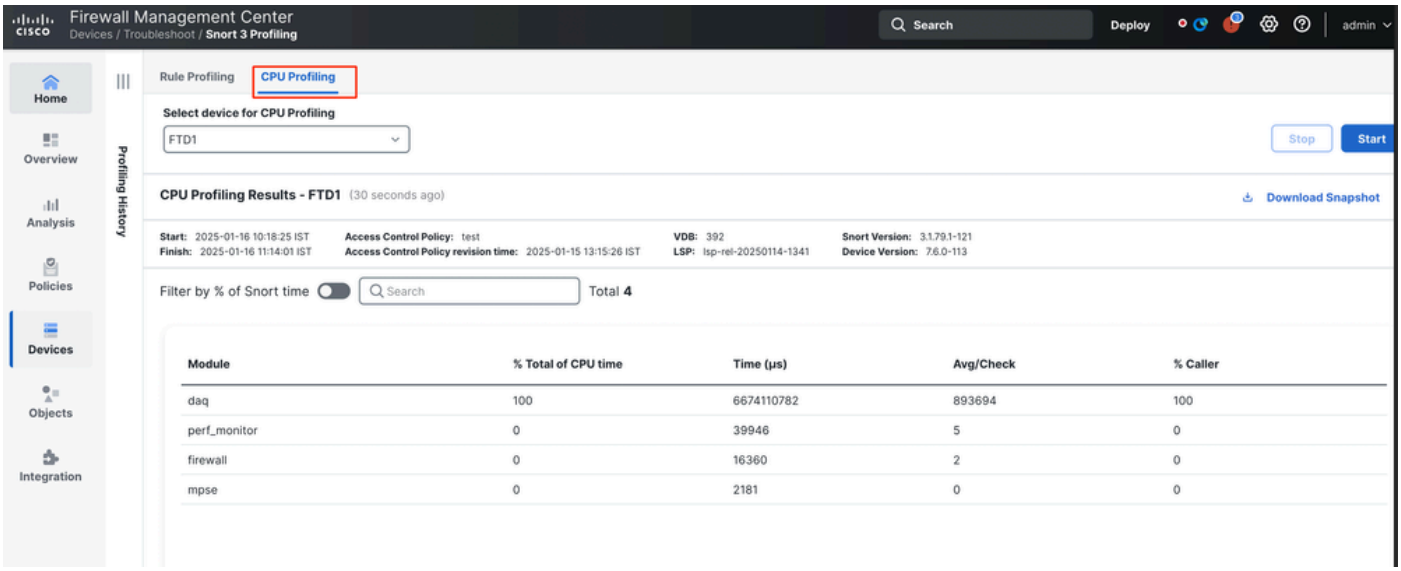
- CPU分析器会分析Snort 3的模块/检查器在特定时间间隔内处理数据包所花费的CPU时间。它可提供有关每个模块消耗的CPU数量（相对于Snort 3进程消耗的CPU总数）的信息。
- 使用CPU分析器不需要重新加载配置或重新启动Snort 3，从而避免了停机时间。
- CPU分析器结果显示所有模块在上次分析会话期间所用的处理时间。
- CPU分析结果以JSON格式保存在/ngfw/var/sf/sync/cpu_profiling/目录下，并在FMC /var/sf/peers/<device UUID>/sync/cpu_profiling目录上同步。

- 在FMC UI中添加了新的Snort 3分析页面
- 可以从Devices > Snort 3 Profiling菜单> CPU Profiling选项卡访问此页
- 使用CPU分析选项卡上的Download Snapshot以CSV格式下载分析结果的快照。

CPU分析选项卡

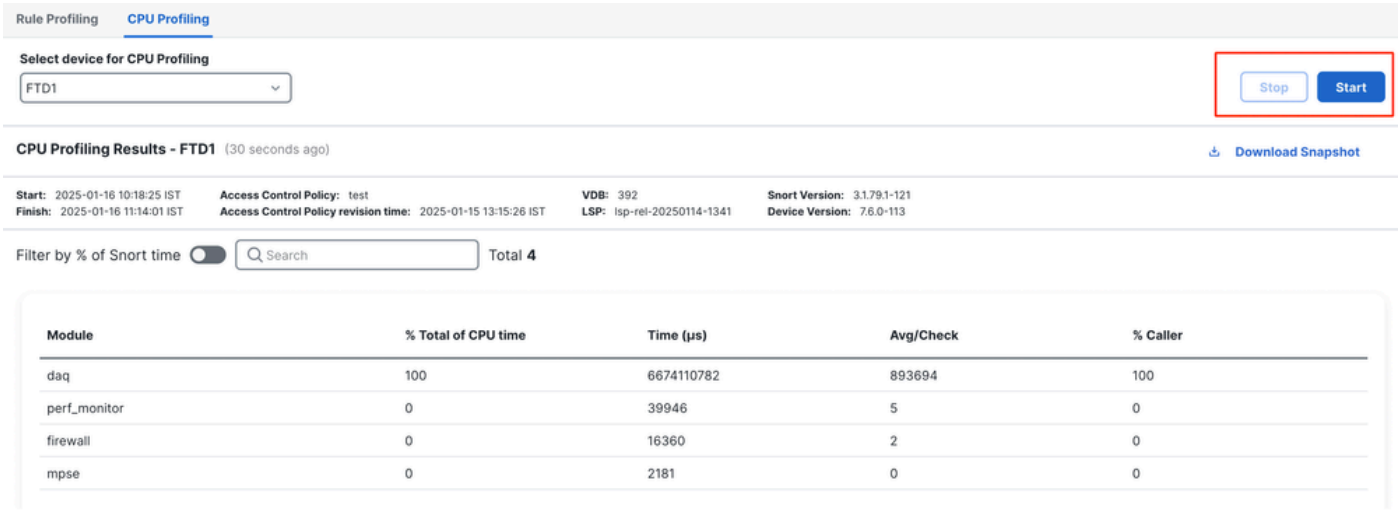
可以从设备 > Snort 3分析菜单> CPU分析选项卡访问“CPU分析”页。

它包含设备选择器、开始/停止按钮、下载快照按钮、性能分析结果部分以及左侧的性能分析历史记录部分（单击该部分时将展开该部分）。

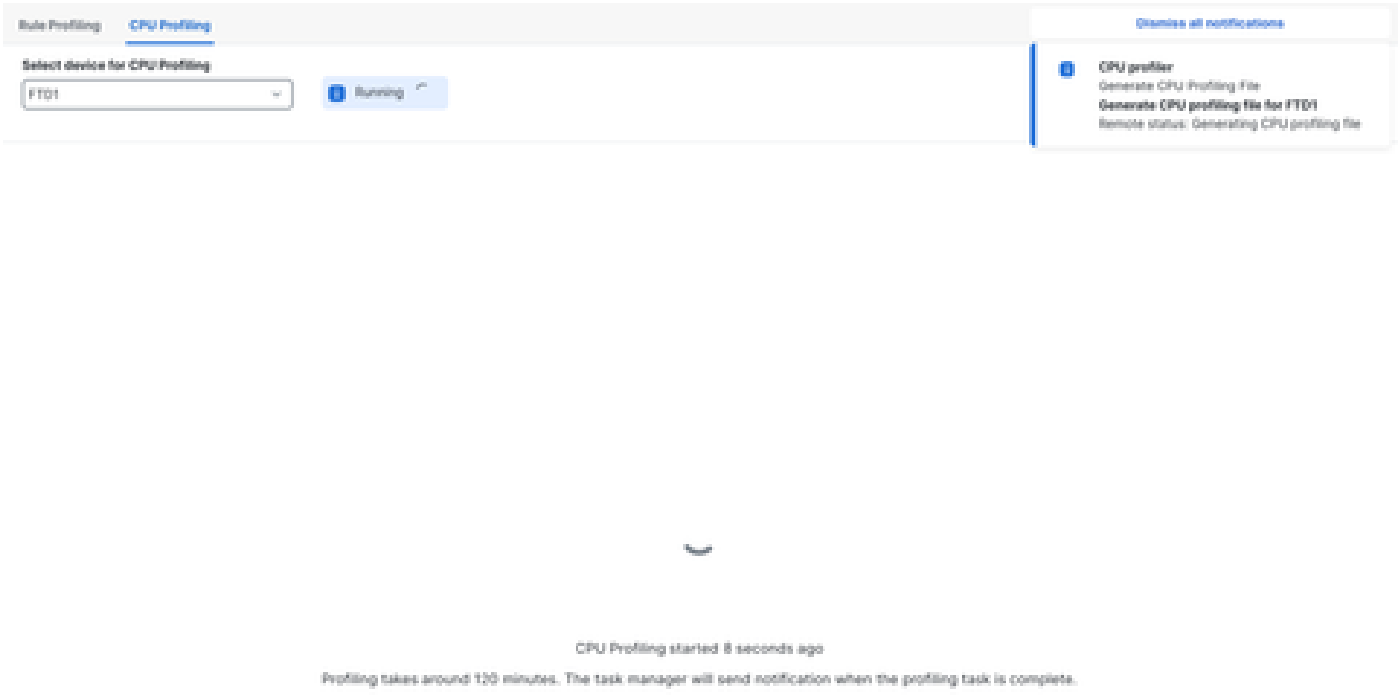


CPU 分析

要启动CPU分析会话，请单击Start。启动会话时显示此页面。

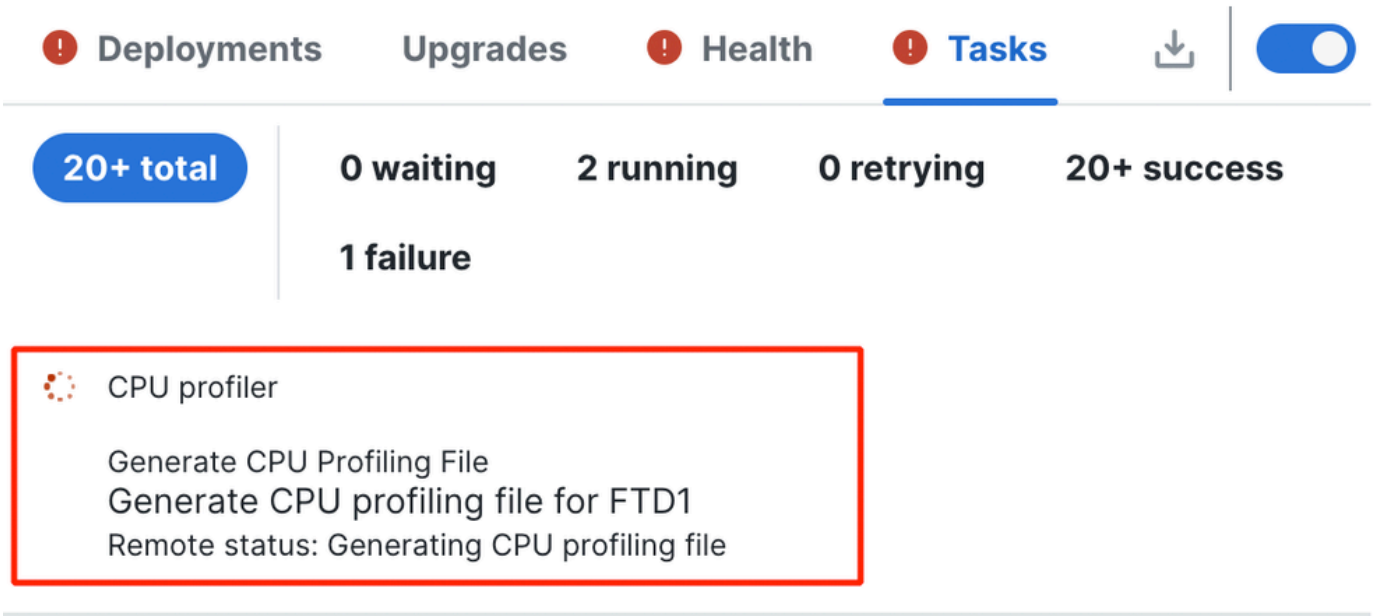


开始



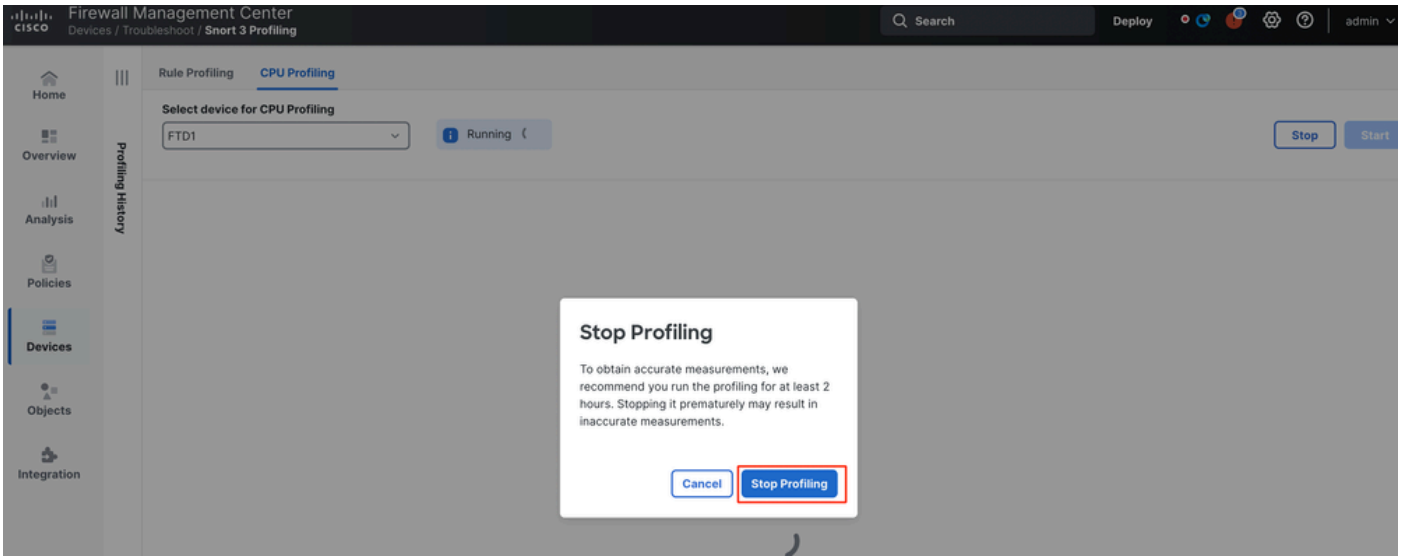
正在运行

启动CPU分析会话后，会创建一个任务。可以在Notifications > Tasks中选中此选项。



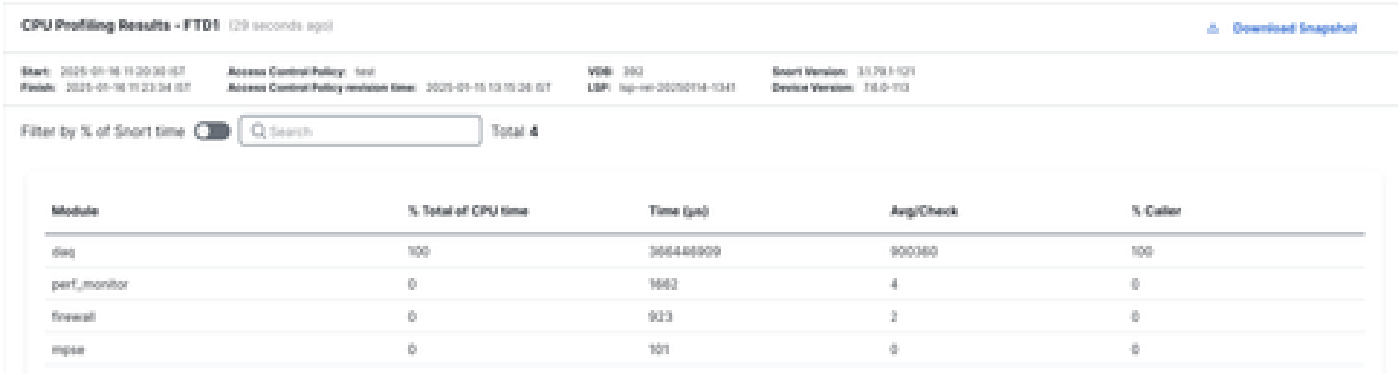
任务

- 要停止正在进行的CPU分析会话，请单击停止。
- 系统将显示确认对话框。单击停止分析。



停止运行

最新的分析结果显示在“CPU Profiling Results（CPU分析结果）”部分。



结果

CPU分析器结果说明

- “模块”列表示模块/检查器的名称。
- “CPU时间总百分比”列表示模块在处理流量时占用的时间相对于Snort 3总时间的百分比。如果该值明显大于其他模块的值，则模块对Snort 3性能不满意的贡献更大。
- “时间(µs)”表示每个模块花费的总时间（以微秒为单位）。
- “Avg/Check”表示模块每次调用模块时所用的平均时间。
- “%调用方”表示子模块（如果已配置）相对于主模块花费的时间。主要用于开发者调试的目的。

CPU分析器结果 — 下载快照

- 用户可以通过点击Download Snapshot下载分析结果快照。下载的文件是.csv格式，包含分析结果页面中的所有字段，如本示例所示。
- 从快照.csv文件中提取：

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

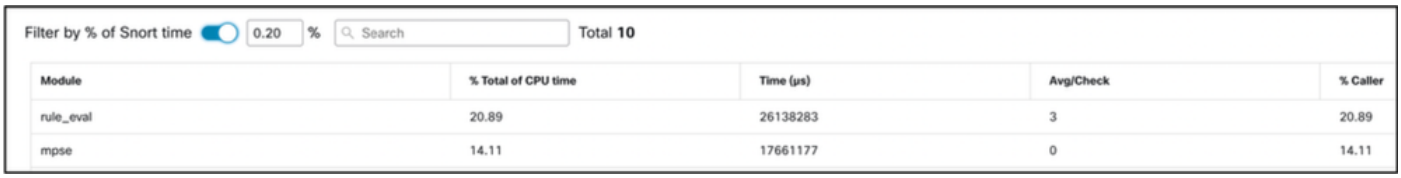
快照

CPU分析结果过滤

分析结果可以使用以下内容进行过滤：

- “按Snort时间的%过滤” — 允许您过滤执行时间超过分析时间n%的模块。
- 搜索(Search) — 允许您通过结果表中存在的任何字段执行文本搜索。

除“Module”以外的任何列均可单击其标题进行排序。



结果

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。