FMC GUI에서 Snort 3 규칙 프로파일링 및 CPU 프로파일링 이해

목차

소개

이 문서에서는 FMC 7.6에 추가된 Snort 3 규칙 및 CPU 프로파일링 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

· Snort 지식 3
· FMC(Secure Firepower Management Center)
· 보안 Firepower 위협 방어(FTD)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 문서는 모든 Firepower 플랫폼에 적용됩니다
- 소프트웨어 버전 7.6.0을 실행하는 FTD(Secure Firewall Threat Defense Virtual)
- 소프트웨어 버전 7.6.0을 실행하는 FMC(Secure Firewall Management Center Virtual)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 개요

- 규칙 및 CPU 프로파일링은 Snort에 이미 존재했지만 FTD CLI를 통해서만 액세스할 수 있었습니다. 이 기능의 목적은 프로파일링 기능을 확장하여 더 간단하게 만드는 것입니다.
- 트러블슈팅 지원을 받기 위해 TAC에 연락하기 전에 디버그 침입 규칙 성능 문제를 활성화하고 규칙 컨피그레이션을 자체적으로 조정합니다.
- Snort 3에서 높은 CPU를 소비하는 경우 어떤 모듈의 성능이 만족스럽지 않은지 파악하십시오.
- 더 나은 성능을 위해 침입 및 네트워크 분석 정책을 디버깅하고 세부적으로 조정할 수 있는 사용자 친화적인 방법을 만듭니다.

프로파일링

- 규칙 프로파일링과 CPU 프로파일링 모두 FTD에서 실행되며 그 결과는 디바이스에 저장되고 FMC에 의해 풀링됩니다.
- 서로 다른 디바이스에서 여러 프로파일링 세션을 동시에 실행할 수 있습니다.
- Rules Profiling(규칙 프로파일링)과 CPU Profiling(CPU 프로파일링)을 동시에 실행할 수 있습니다.
- 고가용성의 경우 세션 시작 시 활성 상태인 디바이스에서만 프로파일링을 시작할 수 있습니다.
  클러스터링된 설정의 경우 클러스터의 각 노드에서 프로파일링을 실행할 수 있습니다.
- 프로파일링 세션이 진행 중인 동안 구축이 트리거되면 사용자에게 경고가 표시됩니다.

사용자가 경고를 무시하고 구축하도록 선택하면 현재 프로파일링 세션이 취소되고 프로파일러 결과에 이에 대한 메시지가 표시됩니다.

실제 프로파일링 결과를 얻으려면 구축에 의해 중단되지 않고 새 프로파일링 세션을 시작해야 합니다.

규칙 프로파일러

- Snort 3 규칙 프로파일러는 Snort 3 침입 규칙 집합을 처리하는 데 걸린 시간에 대한 데이터를 수집하여 잠재적인 문제를 강조 표시하여 성능이 만족스럽지 않은 규칙을 표시합니다.
- Rule Profiler(규칙 프로파일러)는 확인하는 데 가장 많은 시간이 걸린 100개의 IPS 규칙을 표시합니다.
- 규칙 프로파일러를 트리거할 때 Snort 3을 다시 로드하거나 다시 시작할 필요가 없습니다.
- 규칙 프로파일링 결과는 /ngfw/var/sf/sync/snort_profiling/ 디렉터리에 JSON 형식으로 저장되며 FMC에서 동기화됩니다.
- 규칙 프로파일러는 Snort 3 내에 상주하며 Snort 3 침입 탐지 메커니즘으로 트래픽을 검사합

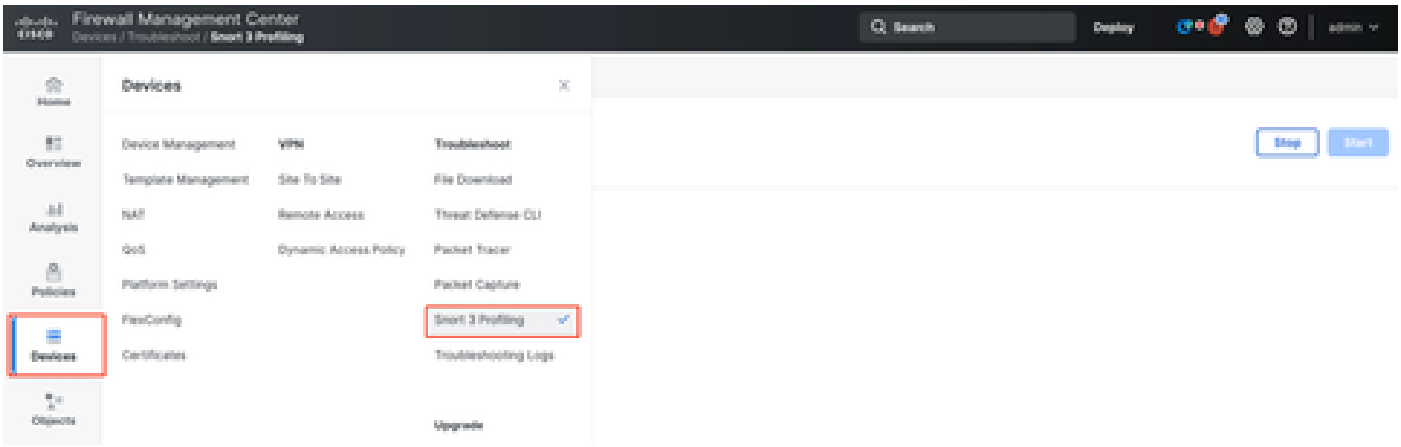
니다. 규칙 프로파일링을 활성화해도 성능에 눈에 띄는 영향을 미치지 않습니다.

운영 규칙 프로파일링

- 트래픽이 디바이스를 통과해야 함
- 디바이스를 선택한 다음 Start(시작) 버튼을 클릭하여 규칙 프로파일링을 시작합니다.
  - 프로파일링 세션을 시작하면 Tasks(작업) 아래의 Notifications(알림)에서 모니터링할 수 있는 작업이 생성됩니다
- 규칙 프로파일링 세션의 기본 지속 시간은 120분입니다
  - 규칙 프로파일링 세션은 완료 전에 Stop 버튼을 눌러 더 빨리 중지할 수 있습니다
- GUI에서 결과를 보고 다운로드할 수 있습니다
- Profiling History(프로파일링 기록)에는 이전 프로파일링 세션 결과가 표시됩니다. 사용자는 Profiling History 왼쪽 패널에서 카드를 클릭하여 특정 프로파일링 결과를 검사할 수 있습니다.

Snort 3 프로파일링 메뉴

Profiling(프로파일링) 페이지는 Devices(디바이스) > Snort 3 Profiling(Snort 3 프로파일링) 메뉴에서 액세스할 수 있습니다. 이 페이지에는 규칙 및 CPU 프로파일링이 두 개의 탭으로 구분되어 있습니다.



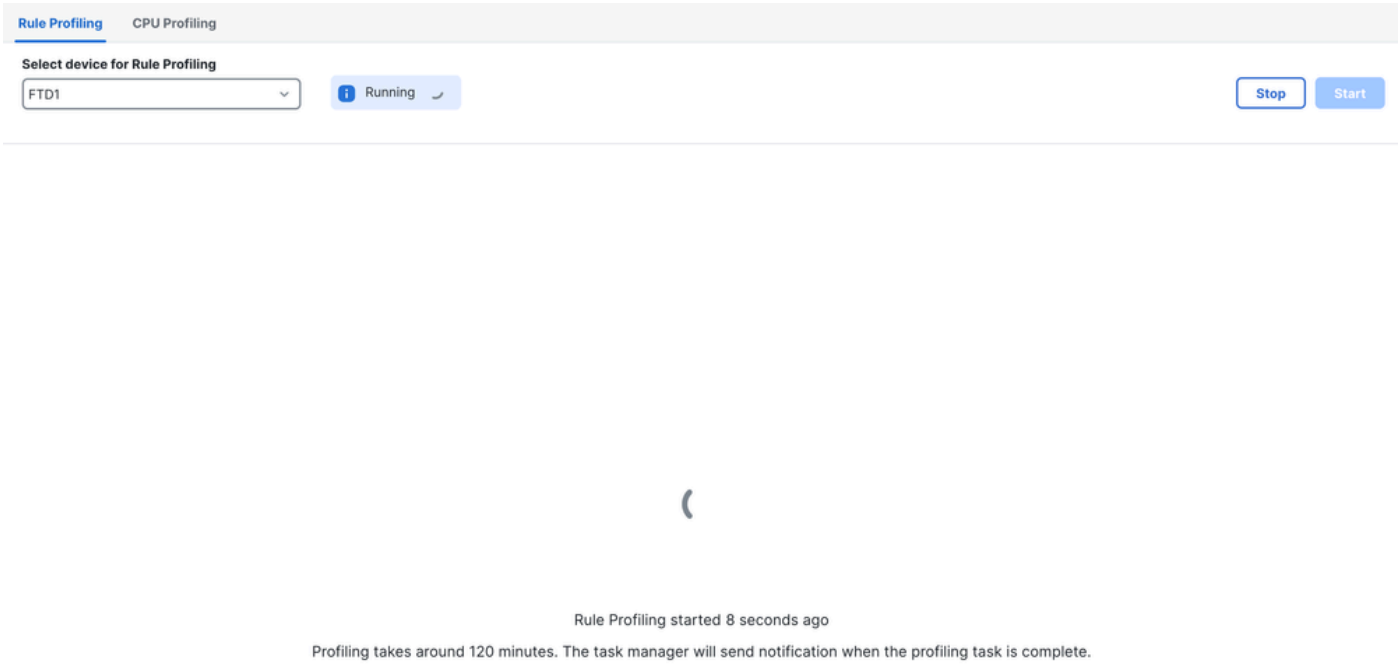
디바이스

규칙 프로파일링 시작

규칙 프로파일링 세션을 시작하려면 Start를 클릭합니다. 120분 후에 세션이 자동으로 중지됩니다.

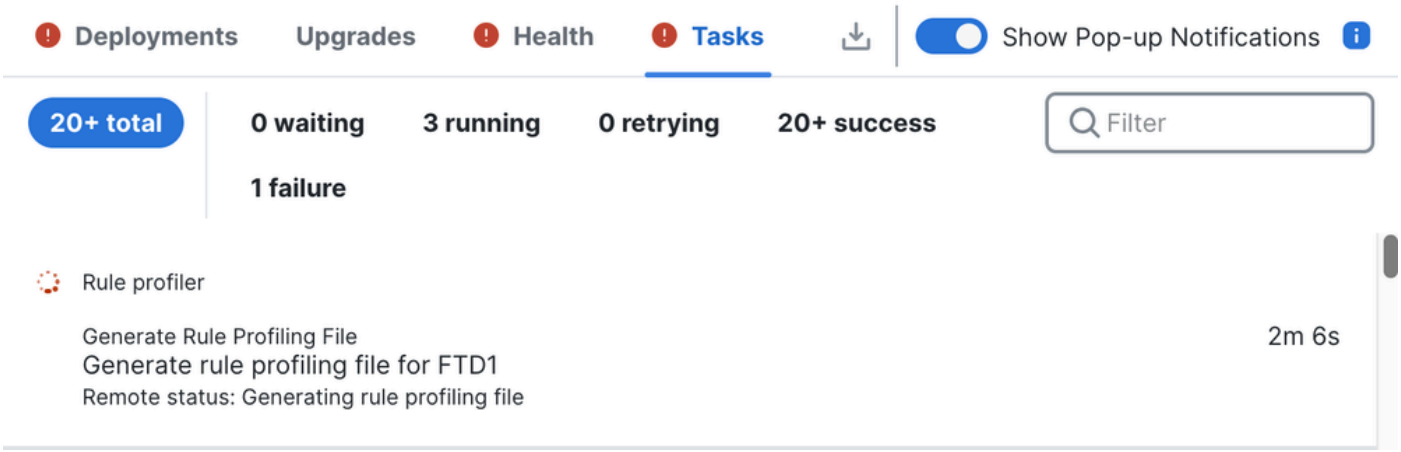
사용자는 프로파일링 세션의 길이를 구성할 수 없지만 2시간이 경과하기 전에 중지할 수 있습니다.

규칙 프로파일링



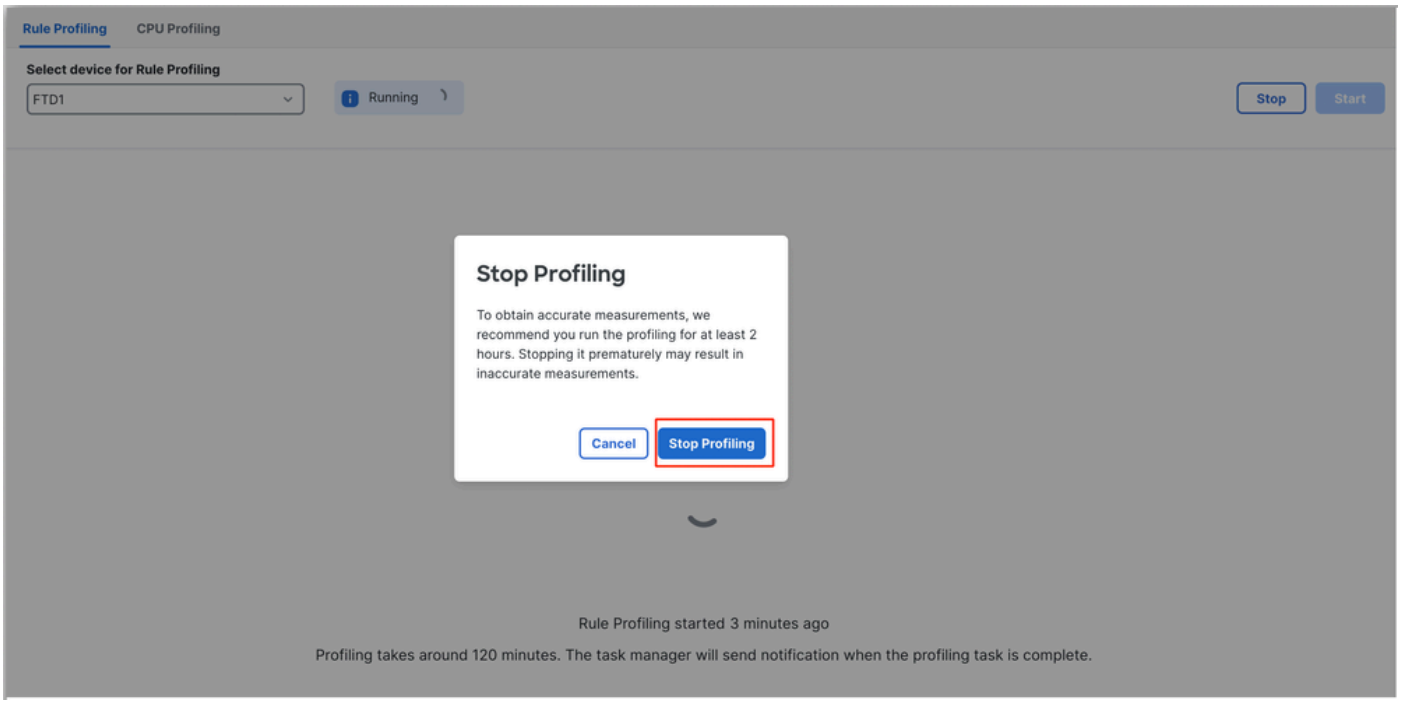
실행 중

규칙 프로파일링 세션이 시작되면 작업이 생성됩니다. 이는 Notifications(알림) > Tasks(작업)에서 확인할 수 있습니다.



작업

진행 중인 규칙 프로파일링 세션을 중지하려면 자동 중지 전에 중단해야 하는 경우 Stop(중지)을 클릭하고 확인을 클릭합니다.



프로파일링 중지

디바이스를 선택하면 최신 프로파일링 결과가 Rule Profiling Results 섹션에 자동으로 표시됩니다.

이 테이블에는 처리에 가장 많은 시간이 걸린 규칙에 대한 통계가 내림차순으로 정렬되어 소요된 총 시간(마이크로초(µs))을 기준으로 합니다.

결과

규칙 프로파일러 결과

IPS 규칙에 대한 규칙 프로파일러 출력에는 다음 필드가 포함됩니다.

- Snort 시간의 % - Snort 3 작업 시간을 기준으로 규칙을 처리하는 데 걸린 시간
- Checks(검사) - IPS 규칙이 실행된 횟수
- Matches(일치) - IPS 규칙이 완전히 일치하는 횟수
- Alerts(알림) - IPS 규칙이 IPS 알림을 트리거한 횟수
- 시간(µs) - Snort가 IPS 규칙 확인에 보낸 시간(마이크로초)
- 평균/검사 - Snort가 규칙의 단일 검사에 보낸 평균 시간
- Avg/Match - Snort가 일치 결과를 가져온 한 번의 검사에 소요된 평균 시간
- 평균/일치하지 않음 - Snort가 일치하는 결과가 발생하지 않은 한 검사에 보낸 평균 시간
- Timeouts - 규칙이 Rule Handling - Threshold(규칙 처리 - 임계값을 초과한 횟수)를 AC 정책의 Latency-Based Performance Settings(레이턴시 기반 성능 설정)에 구성합니다.
- Suspends(일시 중단) - 일부 연속 임계값 위반으로 인해 규칙이 일시 중단된 횟수

결과 다운로드

- 사용자는 "Download Snapshot(스냅샷 다운로드)" 버튼을 클릭하여 프로파일링 결과("스냅샷")를 다운로드할 수 있습니다. 다운로드한 파일은 .csv 형식이며 프로파일링 결과 페이지의 모든 필드를 포함합니다.
- 스냅샷 .csv 파일에서 추출:

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

스냅샷 .csv 파일 보기:

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 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

스냅샷

CPU 프로파일링

Snort 3 CPU 프로파일러 개요

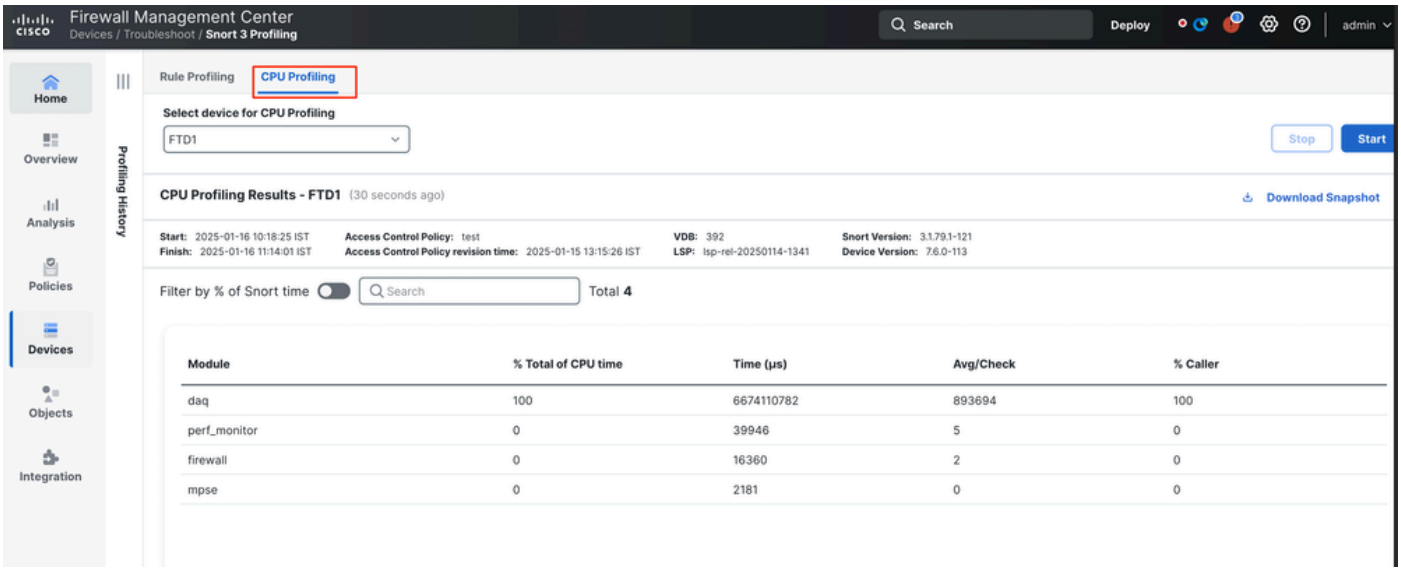
- CPU 프로파일러는 지정된 시간 간격으로 패킷을 처리하기 위해 Snort 3의 모듈/검사기가 소요한 CPU 시간을 프로파일링합니다. Snort 3 프로세스에서 소비한 총 CPU와 관련하여 각 모듈에서 어느 정도의 CPU를 소비하고 있는지 파악할 수 있습니다.
- CPU 프로파일러를 사용하면 컨피그레이션을 다시 로드하거나 Snort 3을 다시 시작할 필요가 없으므로 다운타임을 방지할 수 있습니다.
- CPU 프로파일러 결과는 마지막 프로파일링 세션 동안 모든 모듈에서 소요한 처리 시간을 표시합니다.
- CPU 프로파일링 결과는 /ngfw/var/sf/sync/cpu_profiling/ 디렉토리 아래에 JSON 형식으로 저장되며 FMC /var/sf/peers/<device UUID>/sync/cpu_profiling 디렉토리에서 동기화됩니다.

- 새 Snort 3 프로파일링 페이지가 FMC UI에 추가되었습니다
- 이 페이지는 Devices(디바이스) > Snort 3 Profiling(Snort 3 프로파일링) 메뉴 > CPU Profiling(CPU 프로파일링) 탭에서 액세스할 수 있습니다
- CPU 프로파일링 탭에서 스냅샷 다운로드를 사용하여 CSV 형식의 프로파일링 결과 스냅샷을 다운로드합니다.

CPU 프로파일링 탭

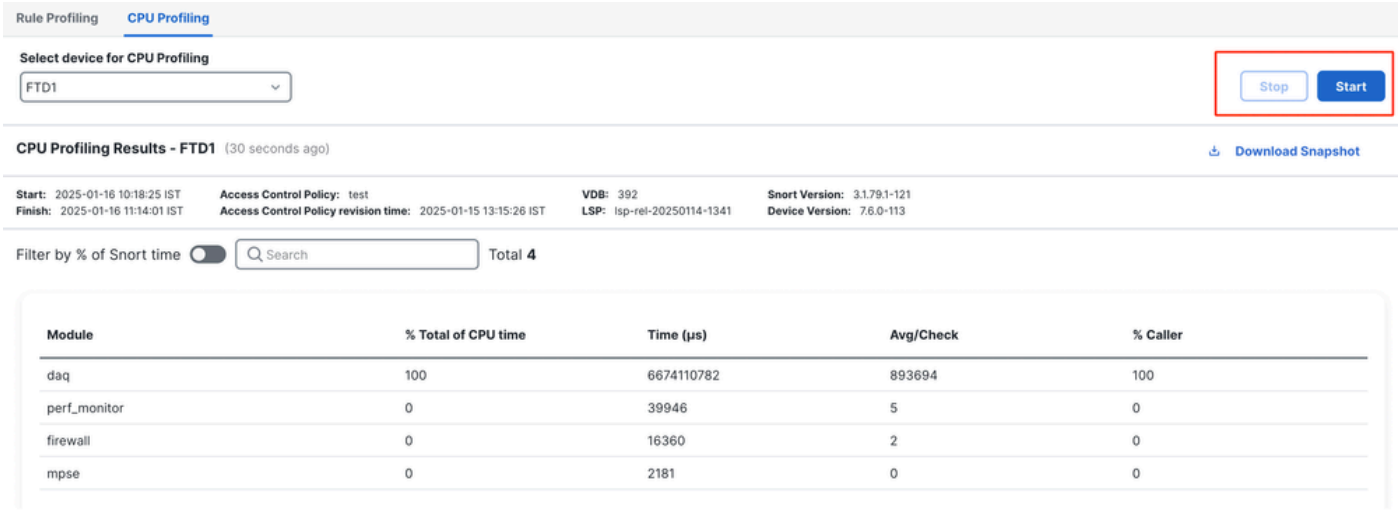
CPU Profiling(CPU 프로파일링) 페이지는 Devices(디바이스) > Snort 3 Profiling(Snort 3 프로파일링) 메뉴 > CPU Profiling(CPU 프로파일링) 탭에서 액세스합니다.

여기에는 디바이스 선택기, 시작/중지 버튼, 스냅샷 다운로드 버튼, 프로파일링 결과 섹션 및 왼쪽의 프로파일링 기록 섹션이 포함되어 있으며 이 섹션을 클릭하면 확장됩니다.

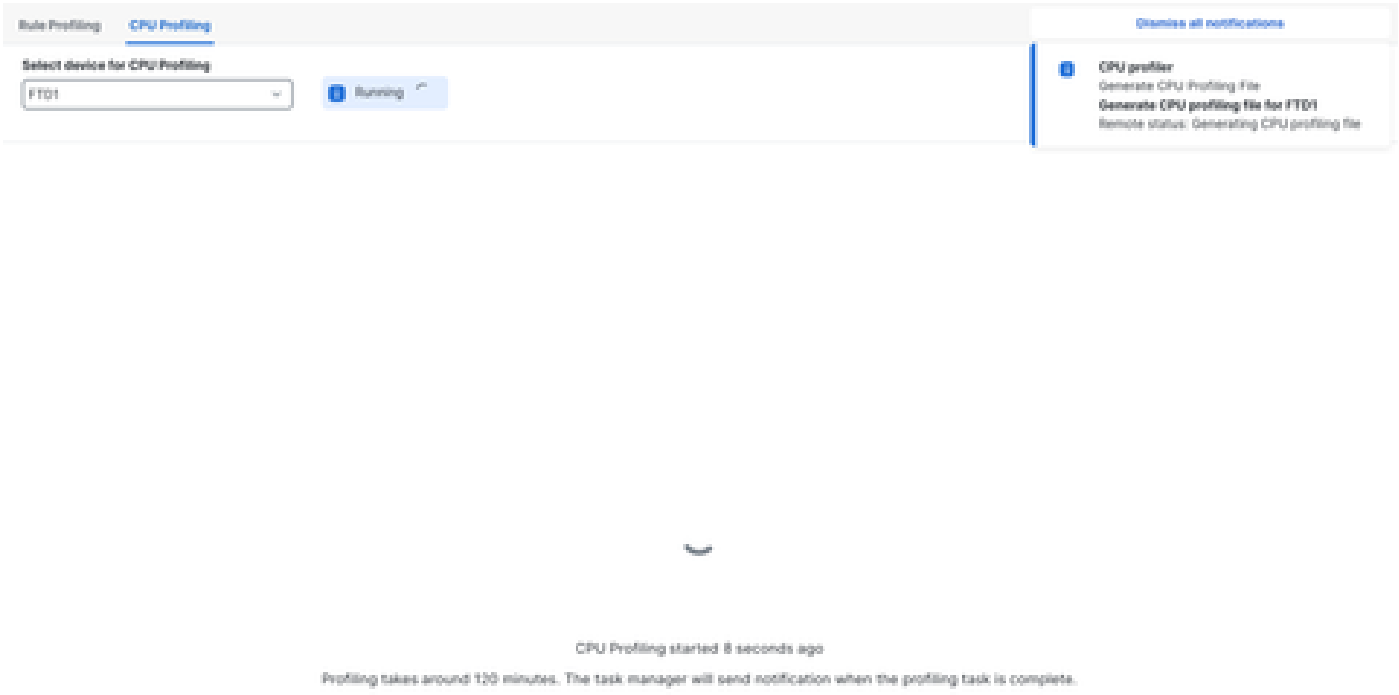


Cpu 프로파일링

CPU 프로파일링 세션을 시작하려면 Start(시작)를 클릭합니다. 이 페이지는 세션이 시작될 때 표시됩니다.

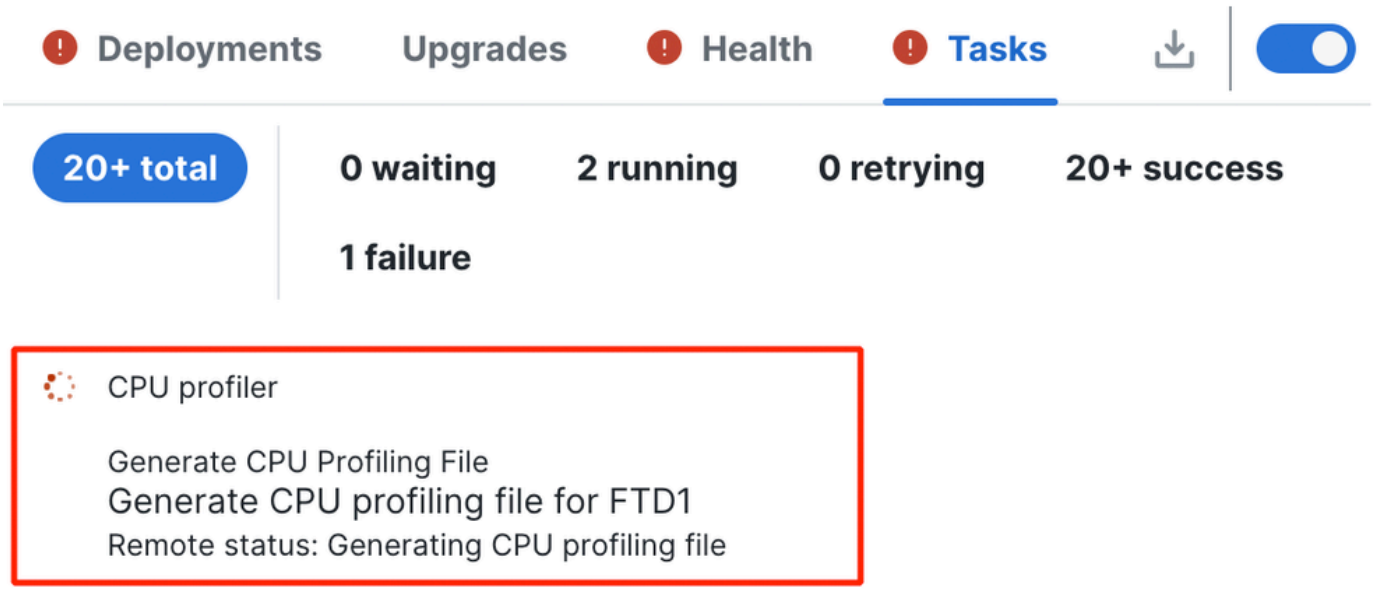


시작하기



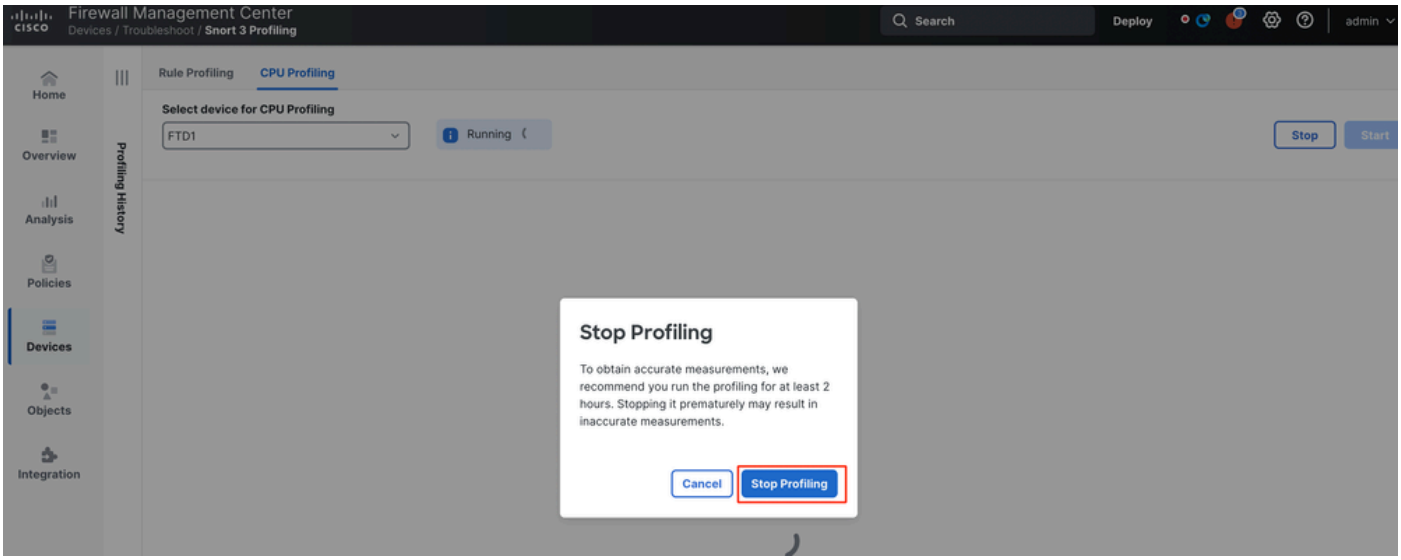
실행 중

CPU 프로파일링 세션이 시작되면 작업이 생성됩니다. Notifications(알림) > Tasks(작업)에서 이 옵션을 선택할 수 있습니다.



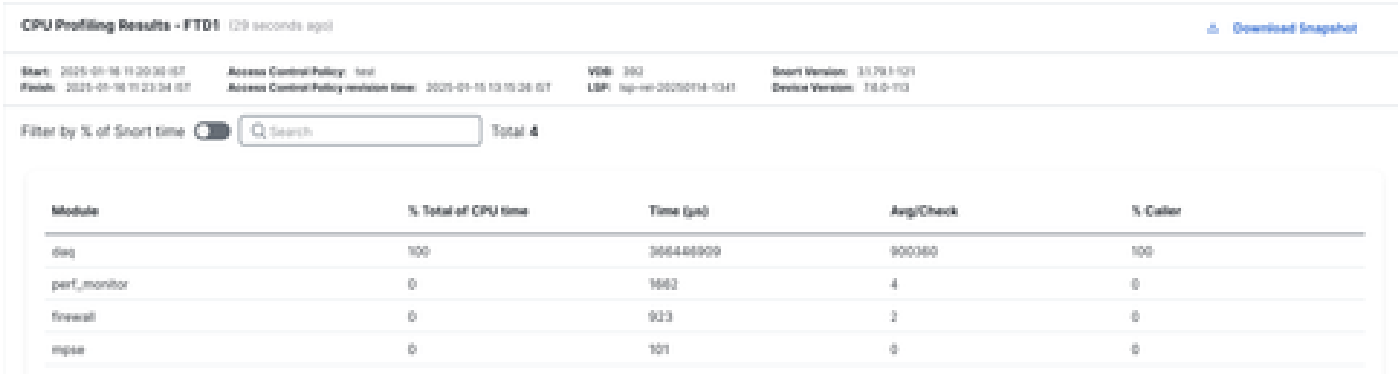
작업

- 진행 중인 CPU 프로파일링 세션을 중지하려면 Stop을 클릭합니다.
- 확인 대화 상자가 나타납니다. Stop Profiling(프로파일링 중지)을 클릭합니다.



실행 중지

최신 프로파일링 결과는 CPU Profiling Results 섹션에 표시됩니다.



결과

CPU 프로파일러 결과 설명

- "Module" 열은 모듈/검사기의 이름을 나타냅니다.
- "% Total of CPU Time" 열은 처리 트래픽에서 Snort 3이 소요한 전체 시간과 관련하여 모듈이 소요한 시간의 백분율을 나타냅니다. 이 값이 다른 모듈보다 상당히 클 경우 모듈은 Snort 3의 불만족스러운 성능에 더 크게 기여합니다.
- "시간(µs)"은 각 모듈이 취한 총 시간(마이크로초)을 나타냅니다.
- "Avg/Check"는 모듈이 호출될 때마다 모듈이 소요한 평균 시간을 나타냅니다.
- "% Caller"는 기본 모듈과 관련하여 하위 모듈(구성된 경우)이 소요한 시간을 나타냅니다. 주로 개발자 디버깅 용도로 사용됩니다.

CPU 프로파일러 결과 - 스냅샷 다운로드

- 사용자는 Download Snapshot(스냅샷 다운로드)을 클릭하여 프로파일링 결과 스냅샷을 다운로드할 수 있습니다. 다운로드한 파일은 .csv 형식이며 이 예에 표시된 대로 프로파일링 결과 페이지의 모든 필드가 포함되어 있습니다.
- 스냅샷 .csv 파일에서 추출:

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

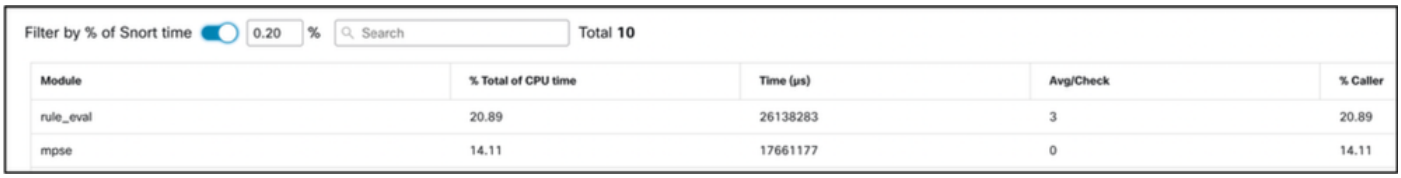
스냅샷

CPU 프로파일링 결과 필터링

프로파일링 결과는 다음을 사용하여 필터링할 수 있습니다.

- "Filter by % of Snort time(Snort 시간의 %로 필터링)" - 실행 시간이 프로파일링 시간의 n%를 초과하는 모듈을 필터링할 수 있습니다.
- 검색 - 결과 테이블에 있는 필드를 통해 텍스트 검색을 수행할 수 있습니다.

"Module"을 제외한 모든 열은 해당 헤더를 클릭하여 정렬할 수 있습니다.



결과

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.