특정 Snort 인스턴스에서 처리하는 트래픽 확인

목차

소개

이 문서에서는 Cisco FTD(Firepower Threat Defense) 환경에서 특정 Snort 인스턴스가 처리하는 트래픽을 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 제품에 대해 알고 있는 것이 좋습니다.

- FMC(Secure Firepower Management Center)
- FTD(Secure Firepower Threat Defense)
- Syslog 및 SNMP
- REST API

사용되는 구성 요소

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.

1. CLI 명령 사용

FTD 디바이스의 CLI(Command Line Interface)를 사용하여 Snort 인스턴스 및 해당 인스턴스가 처리하는 트래픽에 대한 자세한 정보에 액세스할 수 있습니다.

- 이 명령은 실행 중인 Snort 프로세스에 대한 세부 정보를 제공합니다.

show snort instances

다음은 명령 출력의 예입니다.

> show snort instances

Total number of instances available - 1 +----------+----------+ | INSTANCE | PID | +----------+----------+ | **1** | **4765** | <<< One instance available and its process ID +----------+----------+

- Snort 인스턴스에서 처리하는 트래픽 통계에 대한 자세한 내용을 보려면 이러한 명령을 사용할 수 있습니다. 여기에는 처리, 삭제된 패킷 수 및 각 Snort 인스턴스에서 생성된 알림을 비롯한 다양한 통계가 표시됩니다.

show snort statistics

다음은 명령 출력의 예입니다.

> show snort statistics Packet Counters: Passed Packets 3791881977 Blocked Packets 707722 Injected Packets 87 **Packets bypassed (Snort Down) 253403701** <<< Packets bypassed **Packets bypassed (Snort Busy) 0** Flow Counters: Fast-Forwarded Flows 294816 Blacklisted Flows 227 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 317032 Denied flow events 14230 Frames forwarded to Snort before drop 0 Inject packets dropped 0 TCP Ack bypass Packets 6412936 TCP Meta-Ack Packets 2729907 Portscan Events 0 Packet decode optimized 21608793 Packet decode legacy 6558642

show asp inspect-dp snort

다음은 명령 출력의 예입니다.

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid Cpu-Usage Conns Segs/Pkts Status tot (usr | sys) -- ----- ---------- ---------- ---------- -------- 0 16450 8% (7%| 0%) 2.2 K 0 READY 1 16453 9% (8%| 0%) 2.2 K 0 READY 2 16451 6% (5%| 1%) 2.3 K 0 READY 3 16454 5% (5%| 0%) 2.2 K 1 READY 4 16456 6% (6%| 0%) 2.3 K 0 READY 5 16457 6% (6%| 0%) 2.3 K 0 READY 6 16458 6% (5%| 0%) 2.2 K 1 READY 7 16459 4% (4%| 0%) 2.3 K 0 READY 8 16452 9% (8%| 1%) 2.2 K 0 READY **9 16455 100% (100%| 0%) 2.2 K 5 READY** <<<< High CPU utilization 10 16460 7% (6%| 0%) 2.2 K 0 READY -- ----- ---------- ---------- ---------- ---------- Summary 15% (14%| 0%) 24.6 K 7

2. FMC(Firepower 관리 센터) 사용

FMC를 통해 FTD 디바이스를 관리하는 경우 웹 인터페이스를 통해 트래픽 및 Snort 인스턴스에 대한 자세한 통찰력과 보고서를 얻을 수 있습니다.

- 모니터링

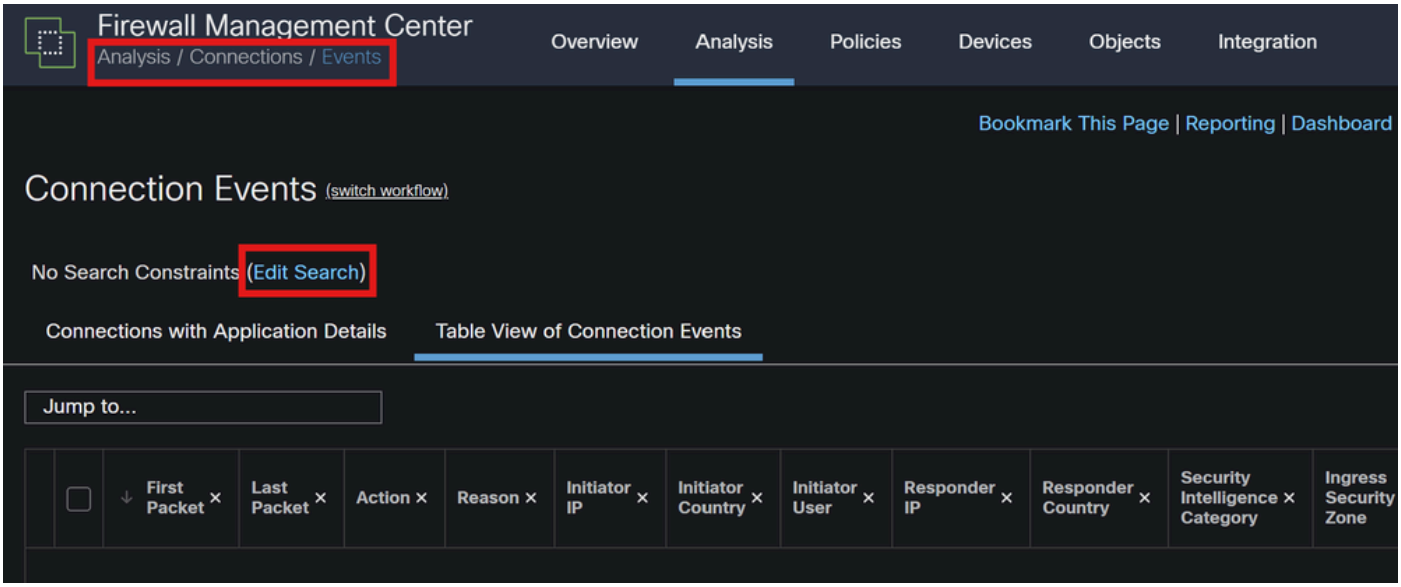
FMC Dashboard(FMC 대시보드): Snort 인스턴스를 비롯한 시스템 상태의 개요를 볼 수 있는 대시보드로 이동합니다.

Health Monitoring(상태 모니터링): health monitoring(상태 모니터링) 섹션에서는 처리된 트래픽을 포함하여 Snort 프로세스에 대한 자세한 통계를 확인할 수 있습니다.

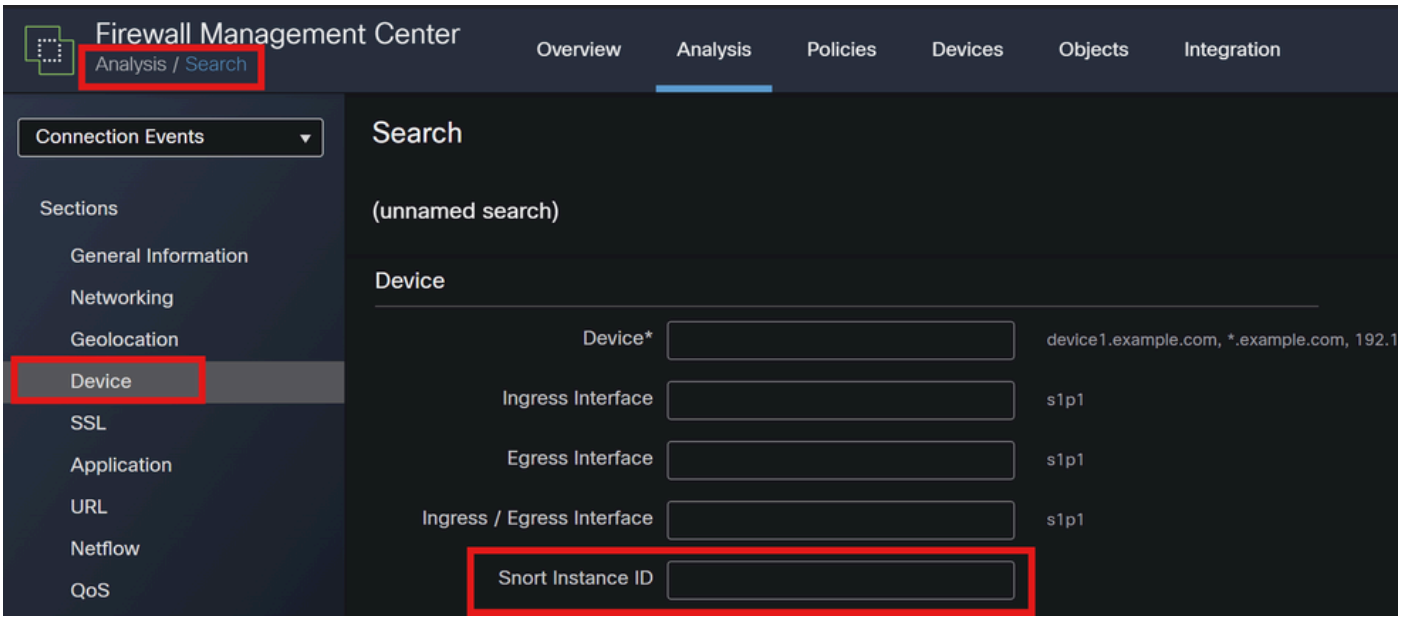
- 분석

Analysis(분석): Analysis(**분석) > Connection Events(연결 이벤트)로 이동합니다**.

Filters(필터): 필터를 사용하여 원하는 특정 Snort 인스턴스 또는 트래픽으로 데이터 범위를 좁힙니다.



연결 이벤트



Snort 인스턴스 *ID*

3. Syslog 및 SNMP 사용

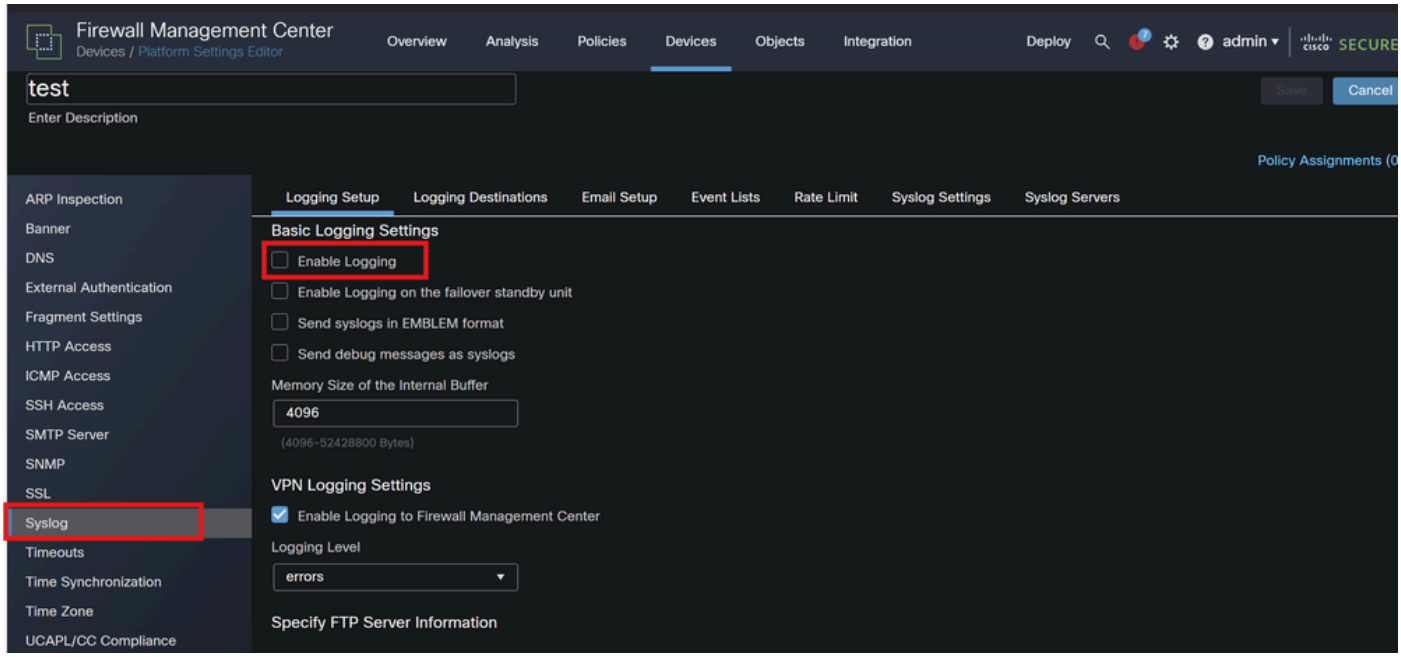
syslog 메시지 또는 SNMP 트랩을 트래픽 데이터를 분석할 수 있는 외부 모니터링 시스템으로 전송하도록 FTD를 구성할 수 있습니다.

- Syslog 컨피그레이션

Devices(디바이스): FMC에서 Devices(디바이스) > **Platform Settings(플랫폼 설정)로 이동합니다**.

정책 생성 또는 편집: 적절한 플랫폼 설정 정책을 선택합니다.

Syslog: Snort 알림 및 통계를 포함하도록 syslog 설정을 구성합니다.

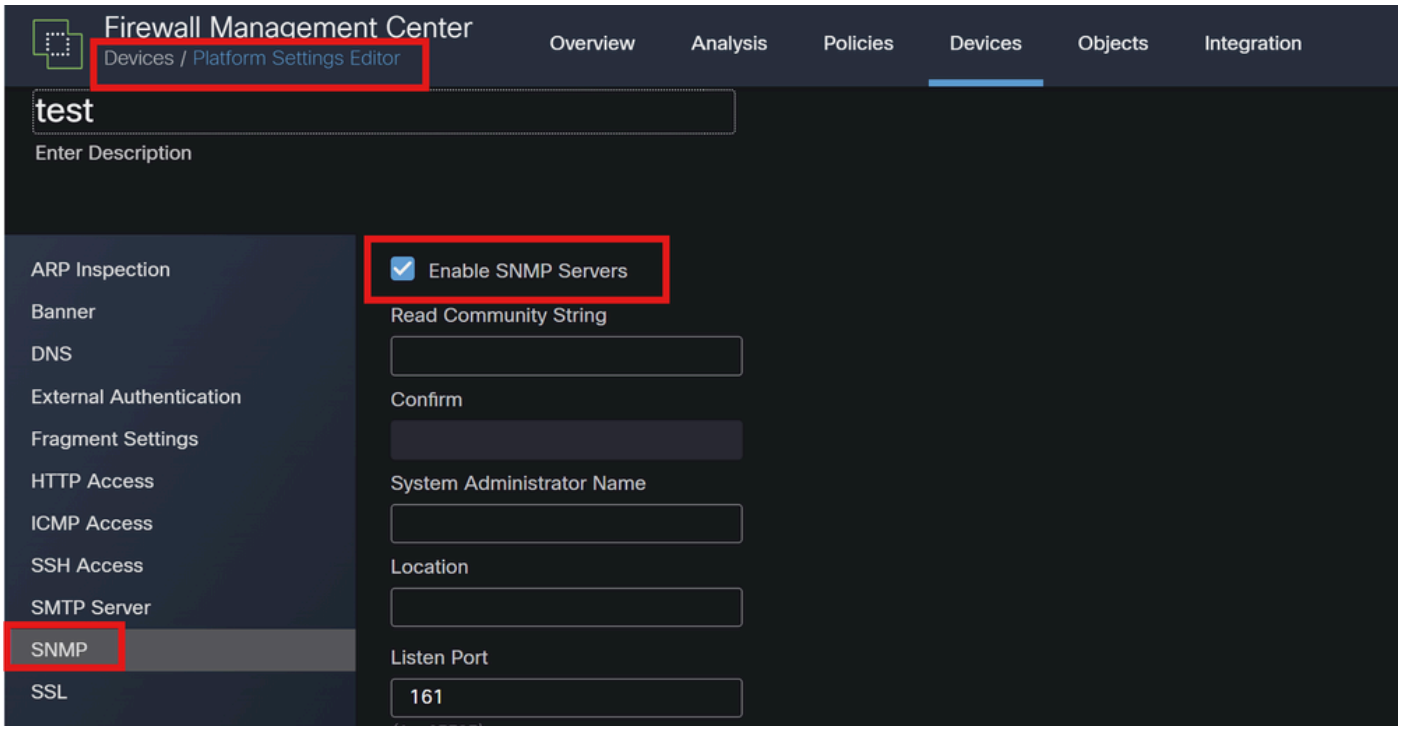


Syslog 컨피그레이션

- SNMP 컨피그레이션

SNMP Settings(SNMP 설정): syslog와 유사하게 Devices(디바이스) > **Platform Settings(플랫폼 설정)**에서 SNMP **설정을 구성합니다**.

Traps(트랩): Snort 인스턴스 통계에 필요한 SNMP 트랩이 활성화되어 있는지 확인합니다.



SNMP 컨피그레이션

4. 사용자 지정 스크립트 사용

고급 사용자의 경우 FTD REST API를 사용하여 Snort 인스턴스에 대한 통계를 수집하는 사용자 지정 스크립트를 작성할 수 있습니다. 이 접근 방식에서는 스크립팅 및 API 사용에 익숙해야 합니다.

- REST API

API 액세스: FMC에서 API 액세스가 활성화되었는지 확인합니다.

API 호출: 적절한 API 호출을 사용하여 Snort 통계 및 트래픽 데이터를 가져옵니다.

이는 특정 Snort 인스턴스에서 처리하는 트래픽을 확인하기 위해 구문 분석 및 분석할 수 있는 JSON 데이터를 반환합니다.

이러한 방법을 결합하면 Cisco FTD 구축에서 각 Snort 인스턴스가 처리하는 트래픽을 포괄적으로 파악할 수 있습니다.

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.