Bepaal verkeer dat door een specifiek gesorteerd exemplaar wordt verwerkt

Inhoud

Inleiding

Dit document beschrijft hoe u het verkeer kunt bepalen dat door een specifieke instantie in een Cisco Firepower Threat Defence (FTD)-omgeving wordt verwerkt.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze producten:

- Secure Firepower Management Center (FMC)
- Secure Firepower Threat Defence (FTD)
- Syslog en SNMP
- REST API

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een uitgeschakelde (standaard) configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

1. CLI-opdrachten gebruiken

Met behulp van de Command Line Interface (CLI) op uw FTD-apparaat kunt u toegang krijgen tot

gedetailleerde informatie over Snortinstanties en het verkeer dat ze verwerken.

- Deze opdracht geeft de details over de lopende gesorteerde processen.

show snort instances

Hier is een voorbeeld voor de opdrachtoutput.

> show snort instances

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

- Voor gedetailleerdere informatie over de verkeersstatistieken die worden verwerkt door Snort-instanties, kunnen deze opdrachten worden gebruikt. Dit geeft verschillende statistieken weer, waaronder het aantal verwerkte pakketten, dat is gevallen en het aantal waarschuwingen dat door elke gescande instantie wordt gegenereerd.

show snort statistics

Hier is een voorbeeld voor de opdrachtoutput.

> 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

Hier is een voorbeeld voor de opdrachtoutput.

> 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. Gebruik van Firepower Management Center (FMC)

Als u uw FTD-apparaten beheert via FMC, kunt u gedetailleerde inzichten en rapporten over verkeer en Snort-instanties krijgen via de webinterface.

- Bewaking

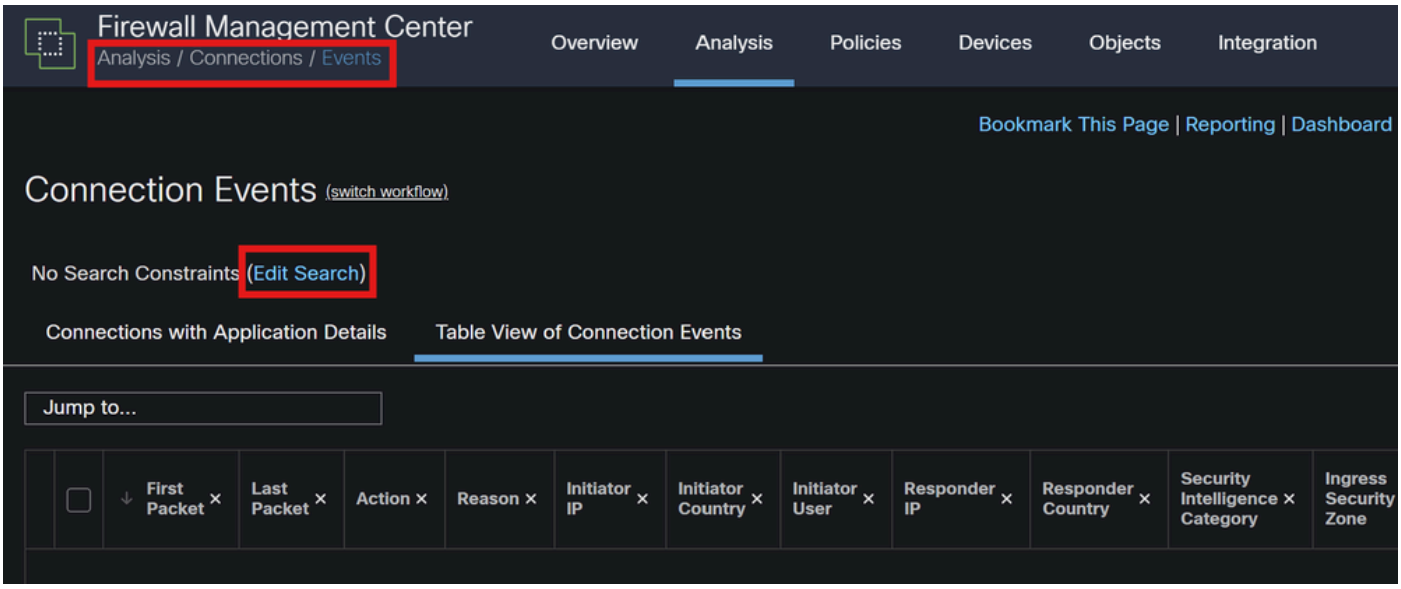
FMC Dashboard: Navigeer naar het dashboard waar u een overzicht kunt zien van de systeemstatus, inclusief Snort-instanties.

Gezondheidsbewaking: In de sectie voor gezondheidsbewaking kunt u gedetailleerde statistieken krijgen over Snortprocessen, waaronder het verkeer dat wordt verwerkt.

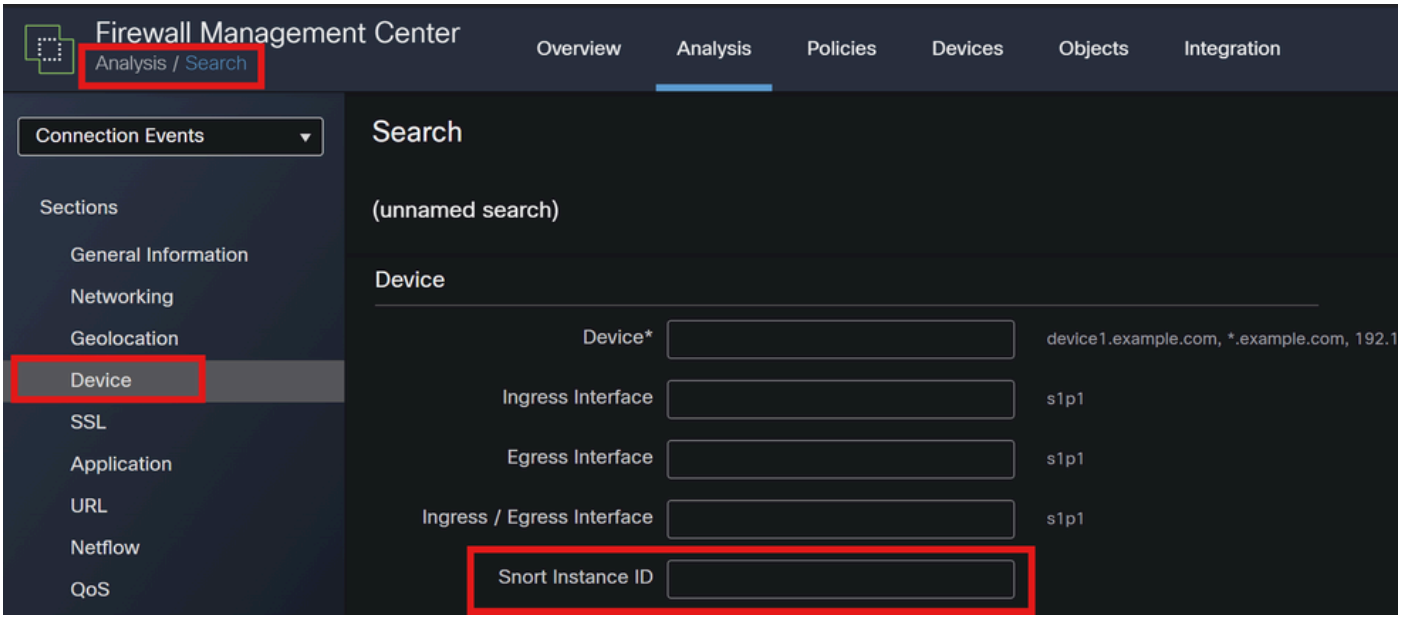
- Analyse

Analyse: Navigeren naar **Analyse > Verbindingsgebeurtenissen**.

Filters: Gebruik filters om de gegevens te beperken tot de specifieke instantie of het verkeer waarin u geïnteresseerd bent.



Verbindingsgebeurtenissen



ID gesorteerde instantie

3. Syslog en SNMP gebruiken

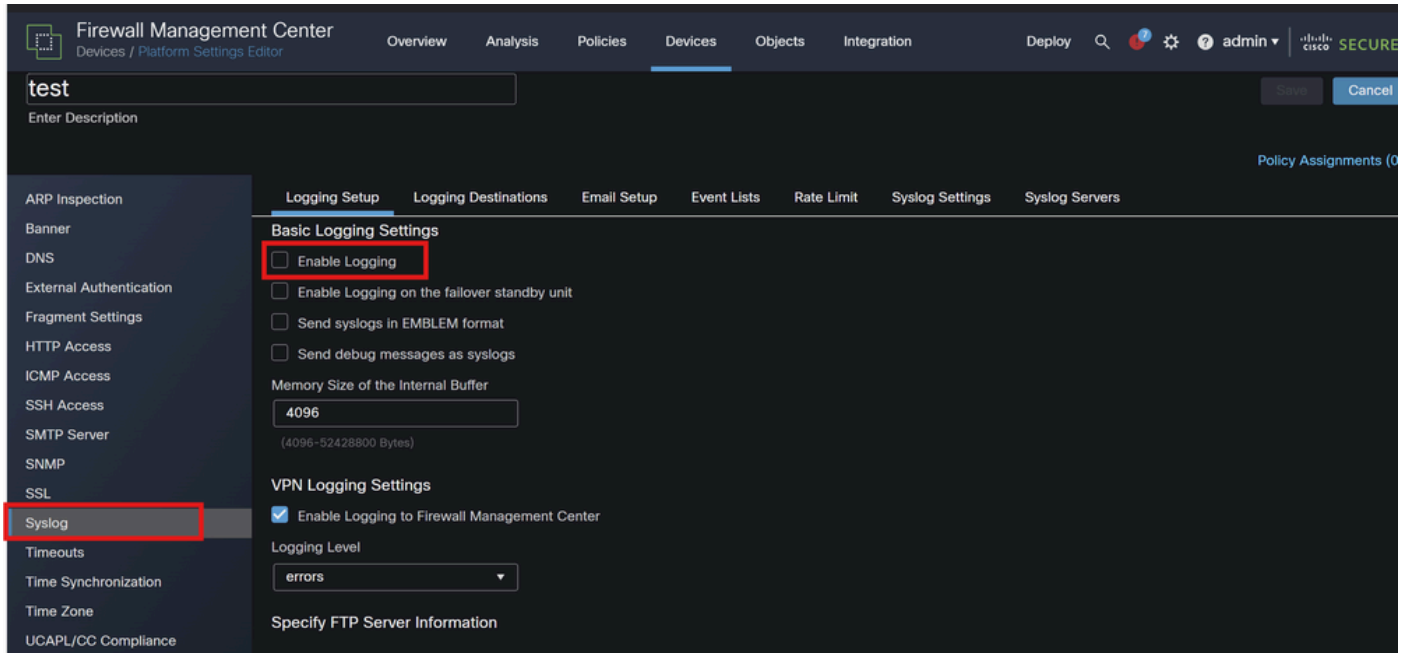
U kunt uw FTD configureren om syslog-berichten of SNMP-traps naar een extern monitoringsysteem te sturen waar u de verkeersgegevens kunt analyseren.

- Syslog-configuratie

Apparaten: Ga in FMC naar **Apparaten > Platform-instellingen**.

Een beleid maken of bewerken: kies het juiste beleid voor platforminstellingen.

Syslog: Syslog-instellingen configureren voor snelmeldingen en statistieken.

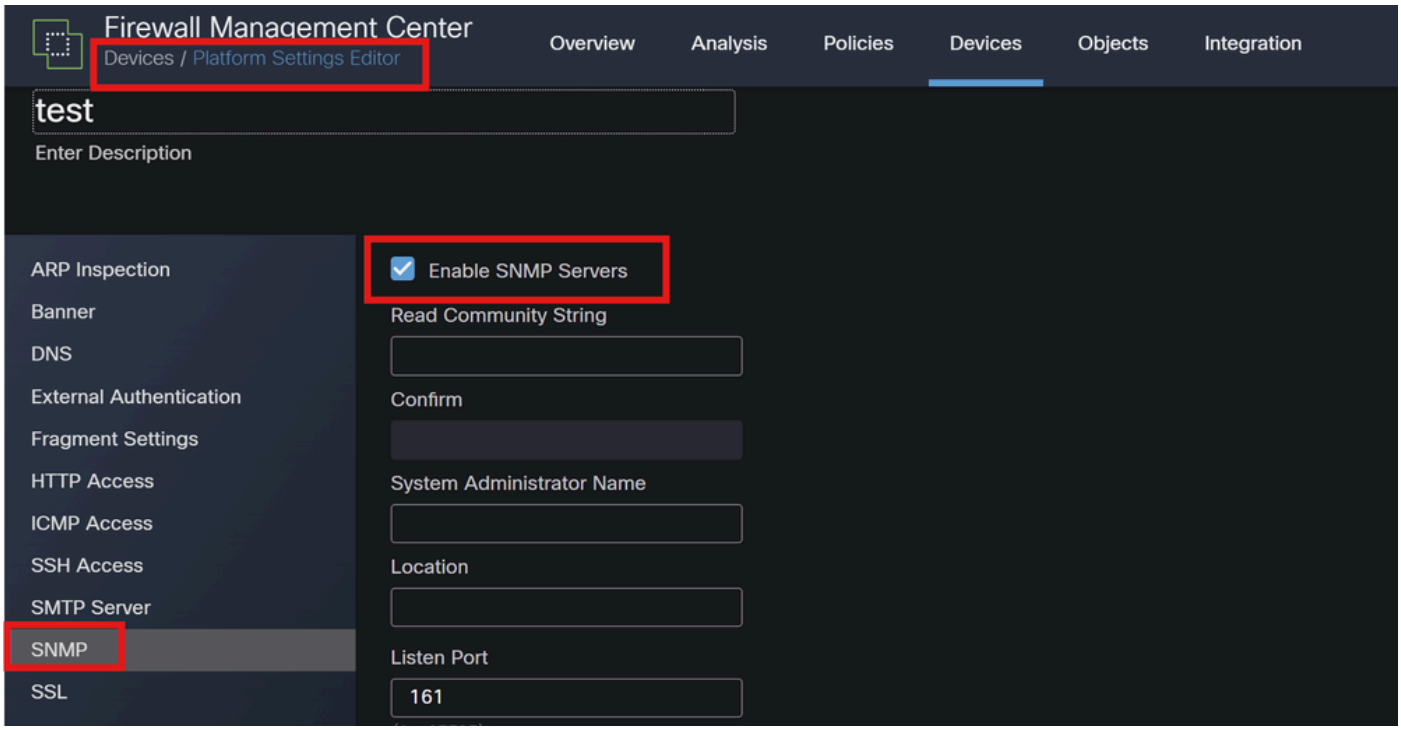


Syslog-configuratie

- SNMP-configuratie

SNMP-instellingen: Net als syslog, configureer SNMP-instellingen onder **Apparaten > Platform-instellingen**.

Traps: Zorg ervoor dat de benodigde SNMP-traps zijn ingeschakeld voor snurk-instantiestatistieken.



SNMP-configuratie

4. De aangepaste scripts gebruiken

Voor geavanceerde gebruikers kunt u aangepaste scripts schrijven die de FTD REST API gebruiken om statistieken te verzamelen over gescande instanties. Deze benadering vereist vertrouwdheid met scripting en API gebruik.

- REST API

API Access: Zorg ervoor dat API-toegang is ingeschakeld op uw FMC.

API-oproepen: Gebruik de juiste API-oproepen om gesorteerde statistieken en verkeersgegevens op te halen.

Dit retourneert JSON-gegevens die u kunt parseren en analyseren om verkeer te bepalen dat wordt verwerkt door specifieke Snort-instanties.

Door deze methodes te combineren, kunt u een uitvoerig begrip van het verkeer krijgen dat door elke instantie van de Snort in uw plaatsing van Cisco FTD wordt behandeld.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.