Déterminer le trafic traité par une instance de Snort spécifique

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)
- [1. Utilisation des commandes CLI](#)
- [2. Utilisation de Firepower Management Center (FMC)](#)
- [3. Utilisation de Syslog et de SNMP](#)
- [4. Utilisation des scripts personnalisés](#)

Introduction

Ce document décrit comment déterminer le trafic traité par une instance Snort spécifique dans un environnement Cisco Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des produits suivants :

- Centre de gestion Firepower sécurisé (FMC)
- Défense contre les menaces Firepower (FTD)
- Syslog et SNMP
- API REST

Composants utilisés

The information in this document was created from the devices in a specific lab environment. Tous les dispositifs utilisés dans ce document ont démarré par une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

1. Utilisation des commandes CLI

L'interface de ligne de commande (CLI) de votre périphérique FTD vous permet d'accéder à des informations détaillées sur les instances Snort et le trafic qu'elles gèrent.

- Cette commande fournit des détails sur les processus Snort en cours d'exécution.

show snort instances

Voici un exemple pour le résultat de la commande.

> show snort instances

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

- Pour obtenir des informations plus détaillées sur les statistiques de trafic traitées par les instances Snort, ces commandes peuvent être utilisées. Cela affiche diverses statistiques, y compris le nombre de paquets traités, abandonnés et les alertes générées par chaque instance Snort.

show snort statistics

Voici un exemple pour le résultat de la commande.

> 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

Voici un exemple pour le résultat de la commande.

> 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. Utilisation de Firepower Management Center (FMC)

Si vous gérez vos périphériques FTD via FMC, vous pouvez obtenir des informations et des rapports détaillés sur le trafic et les instances Snort via l'interface Web.

- Surveillance

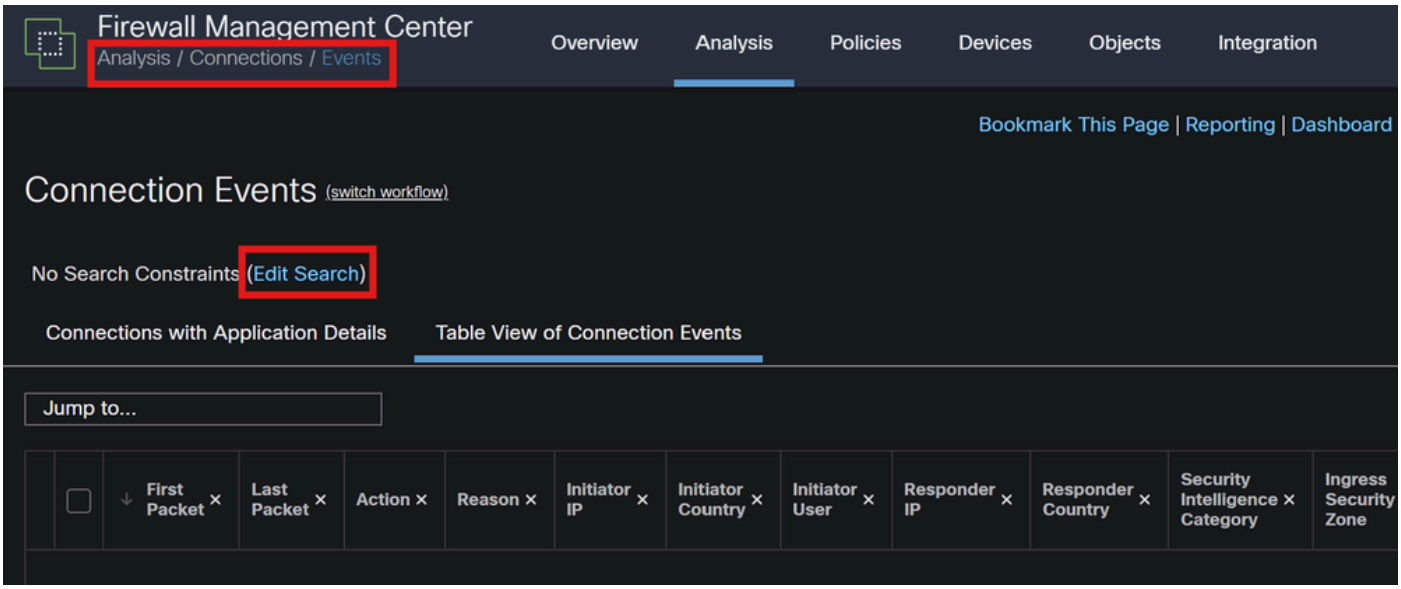
Tableau de bord FMC : accédez au tableau de bord où vous pouvez voir une vue d'ensemble de l'état du système, y compris les instances Snort.

Health Monitoring : dans la section Health Monitoring, vous pouvez obtenir des statistiques détaillées sur les processus Snort, y compris le trafic traité.

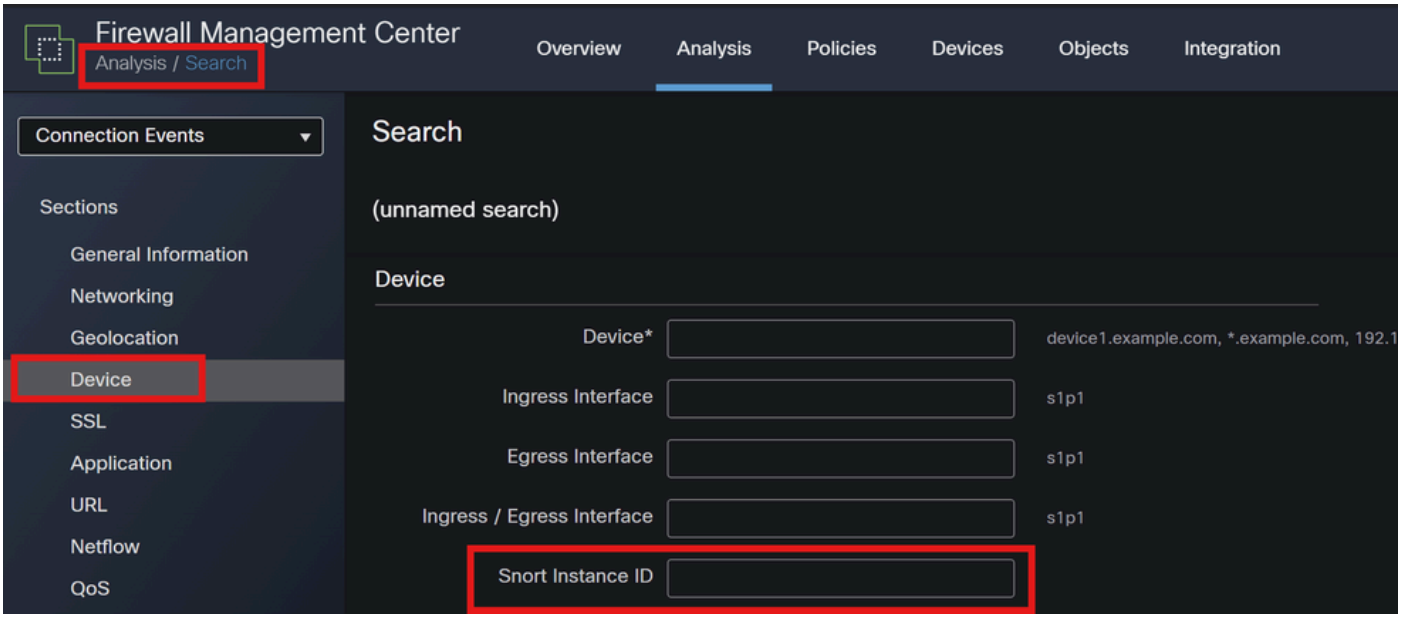
- Analyse

Analyse : accédez à **Analyse > Événements de connexion**.

Filtres : utilisez des filtres pour restreindre les données à l'instance ou au trafic Snort spécifique qui vous intéresse.



Événements de connexion



ID d'instance Snort

3. Utilisation de Syslog et de SNMP

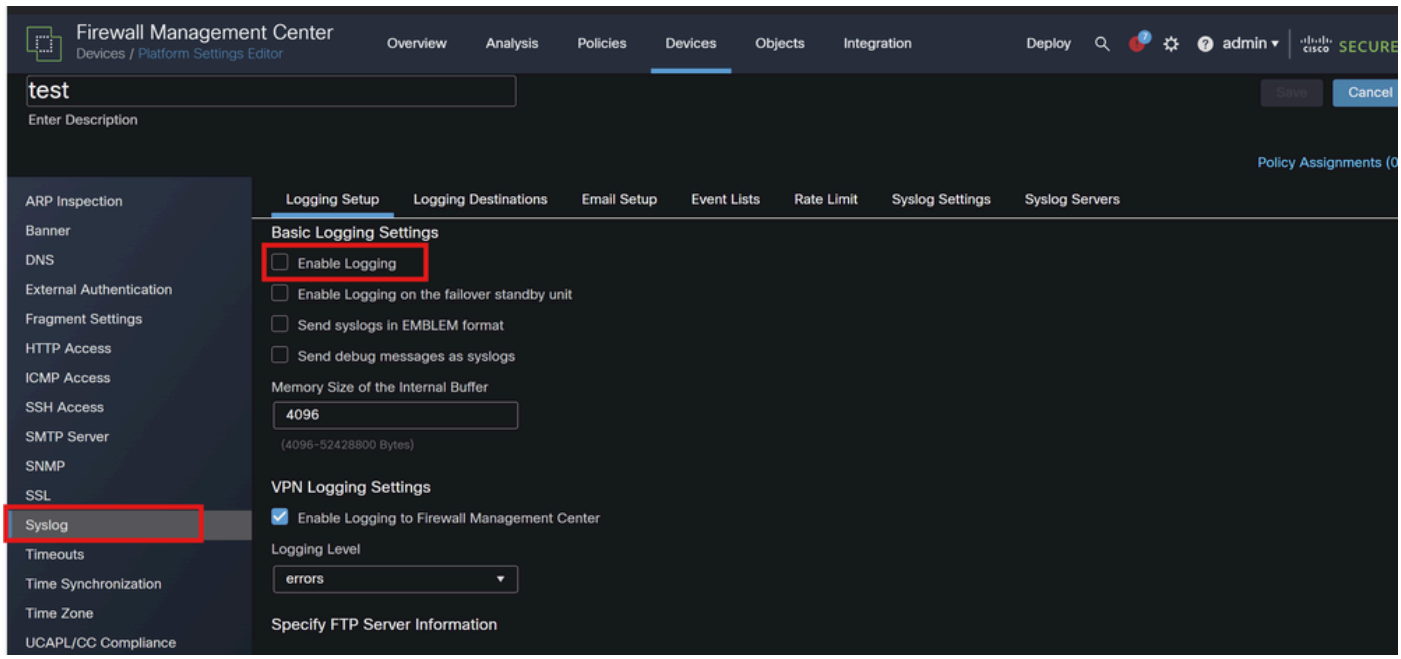
Vous pouvez configurer votre FTD pour envoyer des messages syslog ou des déroutements SNMP à un système de surveillance externe où vous pouvez analyser les données de trafic.

- Configuration Syslog

Périphériques : dans FMC, accédez à **Périphériques > Paramètres de la plate-forme**.

Create or Edit a Policy : choisissez la stratégie de paramètres de plate-forme appropriée.

Syslog : configurez les paramètres syslog pour inclure les alertes et les statistiques Snort.

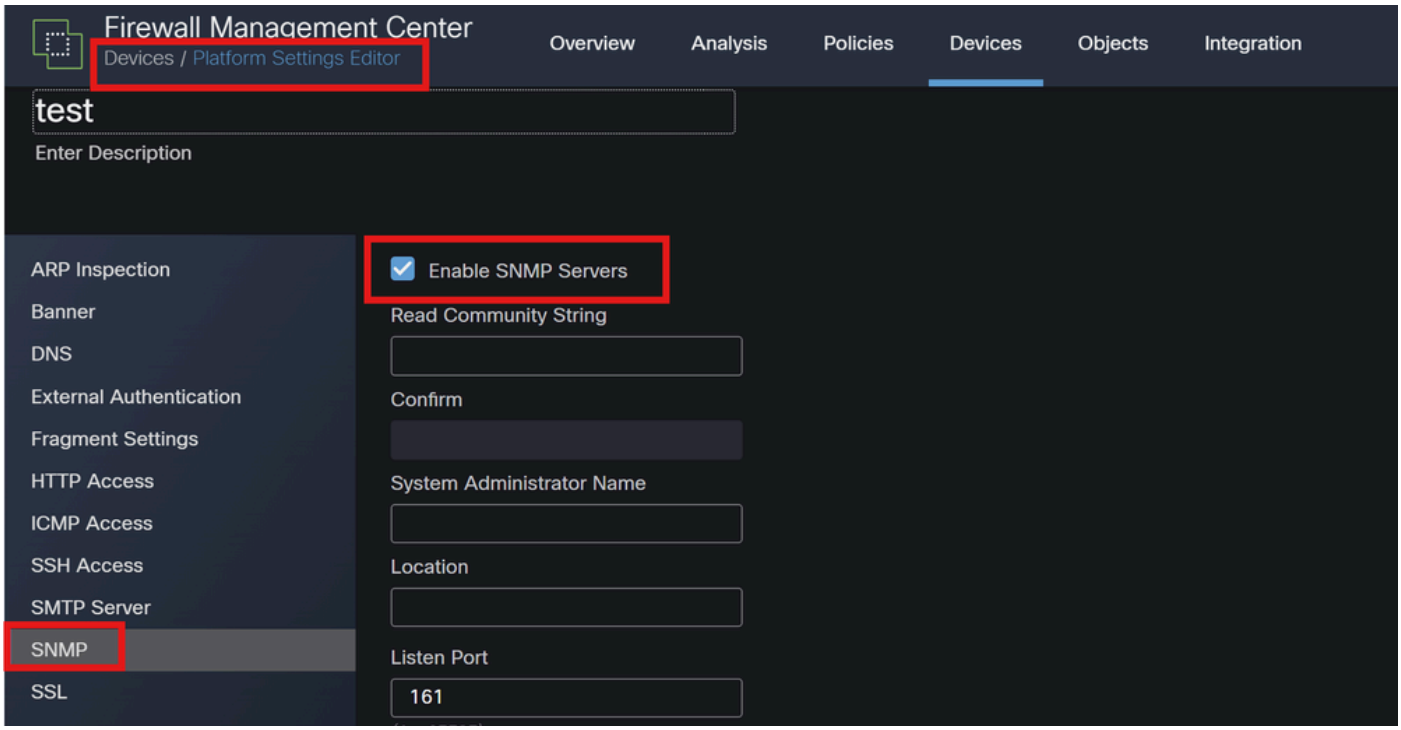


Configuration Syslog

- Configuration SNMP

SNMP Settings : comme pour syslog, configurez les paramètres SNMP sous **Devices > Platform Settings**.

Traps : assurez-vous que les déroutements SNMP nécessaires sont activés pour les statistiques d'instance Snort.



Configuration SNMP

4. Utilisation des scripts personnalisés

Pour les utilisateurs avancés, vous pouvez écrire des scripts personnalisés qui utilisent l'API REST FTD pour collecter des statistiques sur les instances Snort. Cette approche nécessite une bonne connaissance des scripts et de l'utilisation des API.

- API REST

Accès à l'API : assurez-vous que l'accès à l'API est activé sur votre FMC.

Appels API : utilisez les appels API appropriés pour récupérer les statistiques Snort et les données de trafic.

Cela renvoie des données JSON que vous pouvez analyser pour déterminer le trafic traité par des instances Snort spécifiques.

En combinant ces méthodes, vous pouvez obtenir une compréhension complète du trafic géré par chaque instance Snort dans votre déploiement Cisco FTD.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.