# Déterminer le trafic traité par une instance de Snort spécifique

## Table des matières

Introduction	
Conditions préalables	
Exigences	
Composants utilisés	
Utilisation des commandes CLI	
Utilisation de Firepower Management Center (FMC)	
Utilisation de Syslog et SNMP	

## 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 bypas	sed (Snort			
Down)	253403701	<	ckets bypassed (Snort Busy)	0 Flow Counters: Fast-			
Forwarded Flows		294816 Blacklisted Flows	227 Miscellan	eous Counters: Start-of-Flow			
events	0 End-of	F-Flow events	317032 Denied flow events 14				
Frames forwarded to	Snort before drop	0 Inject packets dropped	0 TCP Ack bypass	3			
Packets	6412936 TC	CP Meta-Ack Packets	2729907 Portscan Events	0			
Packet decode optim	ized	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 ------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 READY 3 16454 5% ( 5% | 0%) 2.2 K 1 READY 4 16456 6% ( 6% | 0%) 2.3 K 0 Κ 0 READY 5 16457 6% ( READY 6 16458 6% ( 5% | 0%) 2.2 K 1 6% 0%) 2.3 K 0 READY 7 16459 4% (4% 0%) 2.3 K 0 **READY 8** READY 9 16455 100% (100% 0%) 2.2 K 5 16452 9% (8% 1%) 2.2 K 0 READY <<<< High CPU utilization READY -- ---- Summary 15% (14% 0%) 24.6 K 7 10 16460 7% (6% 0%) 2.2 K 0

#### 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.

	Firewall Ma Analysis / Conn	anageme nections / Ev	ent Cent rents	ter	Overview	Analysis	Policie	s Devices	s Objects	Integratio	n
								Book	mark This Page	e   Reporting   D	ashboard
Con	nection E	vents 🛙	witch workflow	<u>n</u>							
No Se	earch Constraints	s (Edit Searc	ch)								
Con	nections with Ap	oplication D	etails	Table View o	of Connectio	n Events					
Jum	p to										
	〕 ↓ First Packet ×	Last Packet <sup>×</sup>	Action ×	Reason ×	Initiator × IP	Initiator Country ×	Initiator × User	Responder <sub>X</sub> IP	Responder <sub>×</sub> Country	Security Intelligence × Category	Ingress Security Zone

Événements de connexion

Firewall Managemer	nt Center	Overview	Analysis	Policies	Devices	Objects	Integration
Connection Events	Search						
Sections	(unnamed s	earch)					
General Information Networking	Device						
Geolocation		Device*				device1.examp	le.com, *.example.com, 192.1
Device SSL		Ingress Interface				s1p1	
Application		Egress Interface				s1p1	
URL	Ingress	/ Egress Interface				s1p1	
Netflow QoS		Snort Instance ID					

#### Utilisation de Syslog et 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.

Firewall Manageme	ent Center ove	erview Analysis	Policies	Devices Ob	jects Integ	ration	Deploy Q	e 🍳	admin
test									Save
Enter Description									
									Policy Assignments (0
ARP Inspection	Logging Setup	Logging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Servers		
Banner	Basic Logging Sett	tings							
DNS	Enable Logging								
External Authentication	Enable Logging o	on the failover standby u	nit						
Fragment Settings	Send syslogs in E	EMBLEM format							
HTTP Access	Send debug mes	sages as syslogs							
ICMP Access	Memory Size of the In	nternal Buffer							
SSH Access	4096								
SMTP Server									
SNMP									
SSL	VPN Logging Settin	ngs							
Syslog	Enable Logging to	o Firewall Management	Center						
Timeouts	Logging Level								
Time Synchronization	errors	▼							
Time Zone	Specify ETD Server	r Information							
UCAPL/CC Compliance	opeeny FTP Server	linomation							

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.

Firewall Management	t Center	Overview	Analysis	Policies	Devices	Objects	Integration
test							
Enter Description							
ARP Inspection	Enable SNN	IP Servers					
Banner	Read Communi	ty String					
DNS							
External Authentication	Confirm						
Fragment Settings							
HTTP Access	System Adminis	strator Name					
ICMP Access							
SSH Access	Location						
SMTP Server							
SNMP	Listen Port						
SSL	161						

#### 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.