Afficher les flux actifs dans Snort

Table des matières

Introduction

Ce document décrit comment utiliser la commande show snort flows pour afficher les flux actifs dans Snort.

Comparaison antérieure à cette version

In Secure Firewall 7.4 and Below		New to Secure Firewall 7.6
• No way to look at active flows in Snort		• New CLI `show snort flows` can be used to view active flows in Snort

Présentation des fonctionnalités

- La nouvelle interface de ligne de commande show snort flows permet d'afficher les flux actifs dans le cache de flux Snort 3.
- Ceci fournit des détails sur les flux actifs dans l'exécution du processus Snort 3.
- Le résultat fournit l'état du flux de Snort, l'adresse IP source et de destination et le port.
- Il permet d'isoler et de déboguer les problèmes dans les environnements de production.

Déflecteur (Surligner pour lire)

NOTE: Cette fonctionnalité est présentée pour avoir une capacité à examiner les flux Snort actifs et le client, les états de flux du serveur, le délai d'attente, et plus encore.

NOTE: Cette fonctionnalité est présentée pour avoir une capacité à examiner les flux Snort actifs et le client, les états de flux du serveur, le délai d'attente, et plus encore.

Plates-formes logicielles et matérielles minimales

Manager(s) and Version (s)	Application (FTD) and Minimum Version of Application	Supported Platforms
• (CLI only)	FTD 7.6.0	All platforms running FTD and Snort 3

Prise en charge de Snort 3, IPv6, Multi-Instance et HA/Clustering

- Fonctionne avec IPv4 et IPv6.
- Requiert que Snort 3 soit le moteur de détection

FTD	
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes

Autres aspects du soutien

Platforms	
FTD	
Licenses Required	Essentials
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

Description des fonctionnalités et procédure pas à pas

Cette section fournit une procédure pas à pas, y compris le délai d'expiration du flux et des détails sur d'autres fonctionnalités.

Nouvelle CLI Show Snort Flows

<#root>

```
> show snort flows
```

```
TCP 0: x1.x1.x1.2/38148 x1.x1.x1.1/22 pkts/bytes client 9/2323 server 6/2105 idle 7s, uptime 7s, timeou
ICMP 0: x1.x1.x1.2 type 8 x1.x1.x1.1 pkts/bytes client 1/98 server 1/98 idle 0s, uptime 0s, timeout 3m0
UDP 0: x1.x1.x1.1/40101 x1.x1.x1.1/12345 pkts/bytes client 3/141 server 0/0 idle 19s, uptime 58s, timeo
```

Cet exemple illustre trois flux : TCP, ICMP et UDP.

Pour le flux TCP, les valeurs sont les suivantes :

- Protocole - TCP/ICMP/UDP/IP
- ID d'espace d'adressage - ID VRF de l'interface
- SourceIP / Port : x1.x1.x1.2/38148
- Adresse IP/port de destination : x1.x1.x1.1/2
- Paquets client/octets - 9/2323
- Paquets/octets serveur - 6/2015
- Inactif - Temps écoulé depuis le dernier paquet dans le flux
- Temps de disponibilité - Temps écoulé depuis la configuration du flux
- Timeout - Dépassement du délai de flux
- État du client (flux TCP uniquement) - EST

- État du serveur (flux TCP uniquement) - EST

États de flux client et serveur

- L'état du client et l'état du serveur dans le résultat n'apparaissent que si le protocole est TCP.
- Voici les valeurs possibles et ce que chaque acronyme signifie, pour chaque état :

State Acronym	Description
LST	Listen
SYS	SYN Sent
SYR	SYN received
EST	Established
MDS	Midstream Sent
MDR	Midstream Received
FW1	Final Wait 1
FW2	Final Wait 2
CLW	Close Wait
CLG	Closing
LAK	Last ACK
TWT	Time wait
CLD	Closed

Options de filtre

La commande show snort flows prend en charge les options de filtrage où seuls les flux qui correspondent aux filtres sont affichés. La syntaxe est la suivante

show snort flows <option de filtre> <valeur>

Les options de filtre sont les suivantes :

- proto -TCP/UDP/IP/ICMP

- src_ip - filtre les flux par adresse ip source
- dst_ip - filtre les flux par adresse ip de destination
- src_port - filtre les flux par port source
- dst_port - filtre les flux par port de destination

La commande > show snort flows proto TCP répertorie uniquement les flux TCP :

```
TCP 0: x1.x1.x1.2/45508 x1.x1.x1.1/22 pkts/bytes client 10/2389 server 7/2171 idle
30s, uptime 150s, timeout 59m30s state client CLW server FW2
```

Déflecteur (Surligner pour lire)

NOTE: vous pouvez également utiliser plusieurs filtres dans la commande. Exemple :

> show snort flows proto TCP src_ip x1.x1.x1.2 - affiche les flux TCP qui ont l'adresse src ip x1.x1.x1.2

NOTE: vous pouvez également utiliser plusieurs filtres dans la commande. Par exemple, > show snort flows proto TCP src_ip x1.x1.x1.2 - affiche les flux TCP qui ont l'adresse src ip x1.x1.x1.2

Réponse aux erreurs potentielles

- L'utilisateur de l'interface de ligne de commande a obtenu la réponse « Impossible de traiter la commande, veuillez réessayer ultérieurement ».
- Cela se produit lorsque, par exemple, Snort 3 est en panne, lorsque Snort 3 est occupé ou lorsque Snort 3 ne traite pas les commandes de socket de contrôle (telles que les threads à l'état bloqué).
- Conditions d'exécution de l'interface CLI :
    - Snort 3 est en cours d'exécution.
    - Snort 3 répond aux commandes de contrôle sur socket de domaine UNIX.

Arrêt CLI/Sortie

- Comme toute commande CLI, vous pouvez obtenir l'invite de commande en appuyant sur CTRL +C , mais la commande a déjà été passée à tous les threads de paquets et elle s'exécute jusqu'à la fin dans Snort.
- La commande se termine lorsque les deux conditions s'appliquent :
    - Tous les flux du cache de flux ont été affichés
    - Tous les flux qui correspondent aux filtres de la commande CLI ont été écrits dans les fichiers qui servent d'entrée pour la sortie de la commande dans la CLI.

Impact sur les performances

- Ceci est une CLI de débogage. Pour chaque paquet que nous traversons, nous examinons environ 100 flux de la table de flux et imprimons les flux qui correspondent aux critères.
- L'exécution de show snort flows a un impact sur les performances.

Références

FAQ

Q : Pouvons-nous utiliser plusieurs filtres dans « show snort flows » ?

A : Oui, l'interface CLI prend en charge la fourniture de plusieurs filtres à la fois et génère des flux correspondant aux deux filtres.

Q : Quels protocoles sont pris en charge ?

A : IP/TCP/UDP/ICMP

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.