Comprendre la protection DNS dans Secure Firewall 7.7.0

Table des matières

Introduction

Ce document décrit la fonction DNS Guard de Secure Firewall 7.7.0, en se concentrant sur sa fonctionnalité et son dépannage.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Présentation du protocole DNS et des sessions UDP
- Connaissance de Snort 3 et de sa gestion de session

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Protection pare-feu contre les menaces (FTD) version 7.7.0
- Firepower Management Center (FMC) version 7.7.0

- Snort version 3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le protocole DNS est un protocole basé sur la requête-réponse UDP avec des sessions de courte durée. Contrairement à Lina, les sessions DNS dans Snort 3 ne sont pas effacées immédiatement après la réponse DNS. Au lieu de cela, les sessions DNS sont élaguées sur la base d'un délai d'attente de flux de 120 secondes ou plus. Cela entraîne une accumulation inutile de sessions, qui pourraient autrement être utilisées pour d'autres connexions TCP ou UDP.

Comparaison avec la version précédente

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		• DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

Nouvelle fonctionnalité de la version 7.7

Nouvelles fonctionnalités

- Cette fonction de « protection DNS » efface le flux UDP immédiatement après la réception et l'inspection du paquet de réponse DNS.
- Il s'agit d'une amélioration spécifique au protocole par rapport à la conception et à l'architecture actuelles de Snort 3.

Notions de base Plates-formes prises en charge, licences

Plates-formes et gestionnaires FTD

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

Plates-formes prises en charge

Autres aspects du support

FTD	
Licenses Required	Essentials, URL, Threat, Malware
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

Licences et compatibilité

Problème

Dans les versions précédentes, en particulier Secure Firewall 7.6 et versions ultérieures, la session DNS reste un flux Snort 3 obsolète jusqu'à ce qu'elle soit élaguée par le délai d'attente UDP. Cela entraîne des problèmes de gestion des sessions et peut entraîner une utilisation inefficace des ressources à mesure que les sessions DNS s'accumulent inutilement.

Étapes de recréation du problème

Pour observer le problème, exécutez la commande Lina pour vérifier les connexions DNS actives du côté Lina :

```
show conn detail
```

Dans Secure Firewall 7.6 et versions ultérieures, les sessions DNS restent actives jusqu'à l'expiration du délai UDP, ce qui entraîne une inefficacité des ressources.

Solution

La fonction DNS Guard de Secure Firewall 7.7.0 résout ce problème en supprimant immédiatement le flux UDP après réception et inspection du paquet de réponse DNS. Cette amélioration spécifique au protocole garantit que les sessions DNS dans Snort 3 sont libérées immédiatement, ce qui empêche l'accumulation inutile de sessions et améliore l'efficacité des ressources.

Présentation des fonctionnalités

La fonction DNS Guard efface le flux UDP immédiatement après la réception et l'inspection du paquet de réponse DNS. Le flux Snort n'a pas besoin d'attendre que le délai UDP expire.

- Lorsqu'il y a suffisamment de trafic DNS sur la boîte, cette fonctionnalité conduit à moins de flux actifs en raison du nettoyage en temps opportun des flux Snort correspondants.
- Davantage de connexions TCP/UDP peuvent être gérées par le boîtier sans élaguer les connexions actives, ce qui améliore l'efficacité globale du boîtier.

Dépannage

Pour vérifier le fonctionnement de la fonction de protection DNS, utilisez la commande Lina pour vous assurer que les sessions UDP sont libérées lors de la réception d'une réponse DNS :

<#root>

>

show snort counters | begin stream_udp

Exemple de résultat sans fonctionnalité de protection DNS :

```
stream_udp sessions: 755
 max: 12
created: 755
released: 0
total_bytes: 124821
```

<#root>

>

show snort counters | begin stream_udp

Exemple de résultat avec la fonction de protection DNS :

```
stream_udp sessions: 899
max: 14
created: 899
released: 899
total_bytes: 135671
```

Les résultats indiquent que toutes les sessions créées sont libérées à temps, ce qui confirme le bon fonctionnement de la fonction de protection DNS.

Informations connexes

- Assistance technique de Cisco et téléchargements

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.