Dépannage des problèmes de trafic sur CSF CLI

Table des matières

Introduction

Ce document décrit comment utiliser l'interface CLI de Cisco Secure Firewall pour résoudre les problèmes de trafic en validant le routage, le flux de paquets et le comportement de Snort.

Conditions préalables

Aucune exigence spécifique n'est associée à ce document.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Stratégies et configuration d'objets de Firepower Management Center (FMC)
- Routage Cisco Secure Firewall (CSF) et logique d'interface
- Inspection des paquets et dépannage des pare-feu

Composants utilisés

Ce document n'est pas limité à des versions logicielles et matérielles spécifiques pour CSF. Le périphérique utilisé dans le document exécute le code 7.6.5.

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.

Produits associés

Ce document peut également être utilisé avec les versions matérielles et logicielles suivantes :

- Centre de gestion du pare-feu sécurisé (FMC)
- Cisco Secure Firewall (CSF)
- Outils CLI Firepower Threat Defense

Informations importantes

Lorsqu'un périphérique est soumis à une utilisation élevée du processeur, de la mémoire ou des E/S, l'exécution de commandes de dépannage peut aggraver la dégradation des performances. Il est recommandé d'examiner et de résoudre d'abord la condition d'épuisement des ressources, puis de procéder au diagnostic des problèmes de trafic. Les commandes de diagnostic consomment des ressources système supplémentaires, ce qui peut dégrader davantage la disponibilité et prolonger le temps de récupération.

Informations générales

Le dépannage du trafic sur CSF commence souvent par la confirmation du chemin logique qu’un paquet doit emprunter à travers le pare-feu. Une fois que le mappage de route et d’interface est compris, l’étape suivante consiste à comparer le chemin attendu au flux de paquets réel. Cette opération peut être effectuée à l’aide de recherches de route, de simulations Packet Tracer, de captures de paquets et du suivi du moteur Snort.

Chaque outil offre une couche de visibilité différente :

- show route confirme le chemin de routage du paquet et l'identité de l'interface.
- packet-tracer simule le flux de trafic et identifie les décisions relatives aux listes de contrôle

d’accès, à la NAT et aux interfaces.
- les captures de paquets inspectent le trafic en direct qui traverse le pare-feu.
- system support trace expose la prise de décision de Snort pour les blocs liés aux politiques ou les événements d'inspection.

Conseil : Commencez par valider le routage et le traceur de paquets avant de capturer le trafic, afin de pouvoir vérifier si les décisions de chemin et de contrôle d’accès attendues sont correctes avant d’analyser le trafic actif.

Problème

Un flux de trafic ne fonctionne pas comme prévu, et l'administrateur doit déterminer si le paquet emprunte le chemin correct, si le pare-feu autorise ou refuse la connexion, et si Snort ou l'inspection des politiques bloque le trafic.

Étape 1: Trouver la route

Identifiez le chemin de routage et déterminez les noms d’interface logique associés aux adresses IP source et de destination. Les noms d’interface logique sont requis par la plupart des commandes de dépannage. Il doit donc s’agir de la première étape du workflow de dépannage.

Exécutez la commande pour l'adresse IP source et de destination :

```
show route <IP>
```

Le trafic destiné à Internet qui repose sur la route par défaut nécessite l'identification de l'interface de sortie logique. Le nom de l'interface logique peut être déterminé en exécutant cette étape :

```
show route 0.0.0.0
```

Exemple de rapport :

```
FTD1# show route 192.168.0.11
```

```
Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

Dans cet exemple, l'interface d'entrée logique est Interne et l'interface de sortie est Externe.

Mise en garde : La traduction d'adresses de réseau (NAT) peut rediriger le trafic via différentes interfaces que la table de routage indique lorsque les stratégies NAT correspondent au flux de trafic. Lors du dépannage de la connectivité, vérifiez que votre configuration NAT s'aligne sur le chemin de trafic attendu.

Conseil : Les noms d'interface logique sont utilisés dans les commandes de dépannage CLI. Veuillez prendre note du nom logique pour référence ultérieure.

Étape 2: Exécuter Packet-Tracer

Utilisez packet-tracer pour simuler la manière dont le pare-feu évalue un flux de trafic spécifique. Cet outil permet de vérifier quelles interfaces sont utilisées, si une stratégie NAT est appliquée et si une liste de contrôle d'accès autorise ou refuse le trafic.

Utilisez la syntaxe de commande suivante :

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

Exemple de commande :

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

Examinez le résultat pour confirmer que le paquet suit le chemin prévu et qu'il est autorisé pendant la simulation. Cela est utile lorsque vous devez déterminer si le problème est lié au routage, à la NAT ou à la mise en correspondance des politiques avant d'effectuer une analyse de paquets en direct.

Le mot clé transmit dans packet-tracer provoque l'injection du paquet simulé à l'interface d'entrée, lui permettant de traverser toutes les phases de traitement du pare-feu plutôt que de rester comme une simulation.

Exemple de commande :

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

Étape 3: Exécuter les captures

Utilisez les captures de paquets pour inspecter le trafic en direct lorsqu'il traverse le pare-feu. Les captures de paquets sont différentes de packet-tracer car elles capturent le trafic réel et doivent donc correspondre au flux réel qui traverse le pare-feu au moment où la capture est active. Les captures de paquets sont bidirectionnelles et documentent les deux côtés de la connexion.

Pour la plupart des scénarios de dépannage du trafic, configurez les captures suivantes :

- Ingress Capture : capture le trafic arrivant sur l'interface côté source
- Capture de sortie : capture le trafic sortant sur l'interface côté destination
- ASP Drop Capture : capture les paquets abandonnés par le pare-feu et correspondant aux critères configurés

Syntaxe générale de capture :

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

Exemple de capture d'entrée :

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

Exemple de capture de sortie :

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

Exemple de capture de dépôt ASP :

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

Les captures de paquets sont bidirectionnelles, ce qui signifie que le trafic entrant et le trafic de retour peuvent être capturés en fonction des critères de correspondance définis. La fonction de trace permet de visualiser les décisions prises par le pare-feu sur le trafic réel.

⚠ Mise en garde : Si la NAT est exécutée, la capture de sortie doit utiliser l'IP source traduite, et non l'IP source d'origine, pour capturer correctement le trafic post-NAT.

Étape 4: Exécuter la trace de support système

Utilisez la commande system support trace pour afficher le processus d'inspection Snort en temps réel pour un flux de trafic spécifique. Ceci est particulièrement utile lorsque le trafic correspond à une règle d'autorisation de liste de contrôle d'accès mais est toujours bloqué par l'inspection de stratégie. Les captures de paquets standard indiquent qu'un paquet a été bloqué, mais le suivi de la prise en charge du système fournit une visibilité sur la raison pour laquelle le paquet a été traité de cette manière. La trace de prise en charge du système est bidirectionnelle, ce qui signifie qu'elle reçoit le trafic des deux côtés. Cela signifie que l'ordre dans lequel les adresses IP sont ajoutées à l'outil n'a pas d'importance.

Exécutez cette commande et répondez aux invites :

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
```

```
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

Cet outil est particulièrement utile lorsque l'environnement utilise des règles d'application ou d'URL, des règles basées sur l'identité, des stratégies de fichiers ou des stratégies d'intrusion. Ces fonctionnalités sont évaluées après la correspondance de la liste de contrôle d'accès, de sorte qu'un paquet peut être autorisé par la stratégie de contrôle d'accès, mais toujours bloqué par l'inspection Snort.

Remarque : Le port client peut être laissé vide si le port source exact est inconnu.

Vérifier

Utilisez les résultats de la recherche de route, de la simulation Packet Tracer, des captures de paquets et du suivi de la prise en charge du système pour confirmer le comportement du flux de trafic. L'objectif est de déterminer si le paquet emprunte le chemin correct, si le pare-feu l'autorise ou le refuse, et si Snort le bloque sur la base d'une inspection plus approfondie.

Un flux de dépannage complet confirme généralement :

- La recherche de route affiche les interfaces logiques d'entrée et de sortie.
- Packet-Tracer confirme le chemin de transfert prévu et l’évaluation de la stratégie.
- Les captures de paquets confirment si le trafic arrive et sort comme prévu.
- Le suivi du support système confirme si Snort ou l'inspection des politiques est à l'origine du blocage.

Dépannage

Lorsqu'un problème de trafic persiste, passez en revue les zones suivantes :

- Vérifiez si la recherche de route correspond aux interfaces source et de destination attendues.
- Vérifiez si le résultat du traceur de paquets indique que le trafic est refusé à l’étape de la liste de contrôle d’accès ou de la NAT.
- Passez en revue les captures de paquets d’entrée et de sortie pour vérifier que le trafic atteint le pare-feu et qu’il part sur l’interface appropriée.
- Utilisez les captures d'abandon ASP pour confirmer si le pare-feu abandonne le trafic en

interne.
- Utilisez la commande system support trace pour déterminer si Snort bloque le trafic après la décision d'autorisation de la liste de contrôle d'accès.

Informations connexes

- Analyser les captures du pare-feu Firepower pour résoudre les problèmes réseau
- Utiliser les captures Firepower Threat Defense et Packet Tracer

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.