Utilisation de CAR lors d'attaques par déni de service (DoS)

Contenu

Introduction

Parfois, un réseau reçoit un flot des paquets d'attaque du Déni de service (DOS) avec le trafic réseau régulier. Dans de telles situations, vous pouvez employer un mécanisme appelé la « limitation de débit » afin de permettre aux performances du réseau pour dégrader, de sorte que le réseau demeure. Vous pouvez employer le logiciel de Cisco IOS® pour réaliser la limitation de débit par ces schémas :

- Fonction Committed Access Rate (CAR)
- Formation du trafic
- Formation et maintien de l'ordre par la qualité de service modulaire d'interface de ligne de commande (QoS CLI)

Ce document discute le CAR pour l'usage dans les attaques DoS. Les autres schémas sont juste des variantes du concept de base.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Mainline 11.1CC et 12.0 de version du logiciel Cisco IOS, qui prennent en charge le CAR.
- Logiciel Cisco IOS version 11.2 et plus tard, qui prennent en charge la formation du trafic.
- Versions du logiciel Cisco IOS 12.0XE, 12.1E, 12.1T, qui prennent en charge QoS modulaire CLI.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Raté limit ICMP/Smurf

Configurez ces Listes d'accès :

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

```
interface <interface> <interface #>
  rate-limit input access-group 102 256000 8000 8000 conform-action transmit
  exceed-action drop
```

Afin d'activer le CAR, vous devez activer le Technologie Cisco Express Forwarding (CEF) sur la case. En outre, vous devez configurer une interface CEF-commutée pour le CAR.

Les valeurs de bande passante d'utilisations de sortie témoin pour le DS3 tapent des bandes passantes. Choisissez les valeurs basées sur la bande passante d'interface et le débit auxquels vous voulez limiter un type de trafic particulier. Pour de plus petites interfaces d'entrée, vous pouvez configurer des débits inférieurs.

Paquets de synchronisation de TCP de raté limit

11.1(X)CC

Si vous connaissez quel hôte est soumis aux attaques, configurez ces Listes d'accès :

```
access-list 103 deny tcp any host 10.0.0.1 established
!--- Let sessions in progress run. access-list 103 permit tcp any host 10.0.0.1 !--- Rate limit
the initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 103
8000 8000 8000 conform-action transmit exceed-action drop
```

Remarque: Dans cet exemple, l'hôte sous l'attaque est 10.0.0.1.

Si vous ne vous savez pas quel hôte est soumis à l'attaque DoS, et voulez protéger un réseau, configurez ces Listes d'accès :

```
access-list 104 deny tcp any any established
!--- Let sessions in progress run. access-list 104 permit tcp any any !--- Rate limit the
initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 104
64000 8000 8000 conform-action transmit exceed-action drop
```

Remarque: Raté limit à 64000 bps pour tous les paquets de synchronisation de TCP.

12.0(X)[S/T/M]

Si vous connaissez quel hôte est soumis aux attaques, configurez ces Listes d'accès :

```
access-list 105 permit tcp any host 10.0.0.1 syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 105 8000 8000 8000 conform-action transmit exceed-action drop
```

Remarque: Dans cet exemple, 10.0.0.1 est soumis l'hôte aux attaques.

Si vous n'êtes pas sûr qui l'hôte est soumis aux attaques, et vous voulez protéger un réseau, configurez ces Listes d'accès :

```
access-list 106 permit tcp any any syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 106 64000 8000 8000 conform-action transmit exceed-action drop
```

Remarque: Raté limit à 64000 bps pour tous les paquets de synchronisation de TCP.

Forums aux questions de CAR

Comment identifier les valeurs pour utiliser pour le CAR ordonne aux paquets de synchronisation de raté limit ?

Comprenez votre réseau. Le type de trafic détermine le nombre de sessions TCP actives pour une quantité déterminée de données.

- Le trafic de WWW a un mélange beaucoup plus élevé de paquets de synchronisation de TCP que le trafic serveur ftp de ferme.
- Les piles de client PC tendent à reconnaître au moins chaque autre paquet TCP. D'autres piles peuvent reconnaître moins ou plus souvent.
- Vérifiez si vous devez appliquer ces règles de CAR sur la périphérie d'utilisateur résidentiel ou à la périphérie de réseau client.

```
users ---- { ISP } --- web farm
```
Pour WWW, voici le mélange du trafic :

Pour chaque fichier 5k que vous téléchargez de la batterie de serveurs Web, la batterie de serveurs Web reçoit 560 octets, comme affiché ici :

- 80 octets [synchronisation, ACK]
- 400 structure de HTTP d'octet des octets [320, 2 Acks]
- 80 octets [FIN, ACK]

Supposez que le rapport au trafic en sortie de la batterie de serveurs Web du trafic entrant de la batterie de serveurs Web is10:1. Le niveau de trafic qui compose des paquets de synchronisation est 120:1.

Si vous avez un lien OC3, vous limitez le débit de paquets de synchronisation de TCP à 155 mbps/120 mbps du == 1.3.

Sur l'interface d'entrée au routeur de batterie de serveurs Web, configurez :

```
rate-limit input access-group 105 1300000 256000 256000 conform-action transmit
exceed-action drop
```
Le débit de paquets de synchronisation de TCP obtient plus petit pendant que la longueur de vos sessions TCP obtiennent plus long.

```
users ---- { ISP } --- MP3/FTP Farm
```
Les fichiers MP3 tendent à être 4 à 5 mgbps dans la taille sur une moyenne. Le téléchargement d'un fichier de 4 mgbps génère le trafic entrant ces quantités à 3160 octets :

- 80 octets [synchronisation, ACK]
- 3000 octets [Acks + ftp get]
- 80 octets [FIN, ACK]

Le débit de synchronisations de TCP au trafic en sortie est == 155 mbps/120000 1.3 Kbps.

Configurez :

```
 rate-limit input access-group 105 1300 1200 1200 conform-action transmit
exceed-action drop
```
Comment est-ce que je sais si je limite trop de paquets de synchronisation ?

Si vous connaissez votre vitesse de connexion habituelle sur vos serveurs, vous pouvez comparer les figures avant et après que vous activiez le CAR. La comparaison vous aide à identifier l'occurrence d'une baisse dans votre vitesse de connexion. Si vous trouvez une baisse dans le débit, incrémentez vos paramètres de CAR pour laisser plus de sessions.

Vérifiez si les utilisateurs peuvent établir des sessions TCP facilement. Si vos limites de CAR sont trop restrictives, besoin de l'utilisateur de faire des tentatives de multiple d'établir une session TCP.

Est-ce que je peux activer le CAR sur un routeur de commutateur de gigabit (GSR)

?

Oui. Les linecards de l'engine 0 et de l'engine 1 prennent en charge le CAR. La version du logiciel Cisco IOS 11.2(14)GS2 et fournissent plus tard le support de CAR. L'incidence des performances du CAR dépend du nombre de CAR vous ordonne s'appliquent.

L'incidence des performances est également plus grande sur des linecards de l'engine 1 que sur des linecards de l'engine 0. Si vous voulez activer le CAR sur des linecards de l'engine 0, vous devez se rendre compte de l'ID de bogue Cisco CSCdp80432 (clients enregistrés seulement). Si vous voulez activer le CAR au trafic de multidiffusion de rate-limit, assurez-vous que l'ID de bogue Cisco CSCdp32913 (clients enregistrés seulement) ne vous affecte pas. L'ID de bogue Cisco CSCdm56071 (clients enregistrés seulement) est une autre bogue que vous devez se rendre compte de avant que vous activiez le CAR.

Est-ce que je peux activer le CAR distribué (DCAR) sur un Cisco 7500 ?

Oui, le DCAR de supports de plate-forme RSP/VIP dans le Logiciel Cisco IOS version 11.1(20)CC, et tous 12.0 versions logicielles.

Le CAR affecte des performances dans une certaine mesure. Basé sur la configuration du CAR, vous pouvez réaliser la ligne débit [pour le trafic de mélange d'Internet] avec un VIP2-50 [par le DCAR] sur un OC3. Assurez-vous que l'ID de bogue Cisco CSCdm56071 (clients enregistrés seulement) ne vous affecte pas. Si vous voulez utiliser pour sortir le CAR, l'ID de bogue Cisco CSCdp52926 (clients enregistrés seulement) peut affecter votre Connectivité. Si vous activez le DCAR, l'ID de bogue Cisco CSCdp58615 (clients enregistrés seulement) peut entraîner une panne de VIP.

Est-ce que je peux activer le CAR sur un Cisco 7200 ?

Oui. Le NPE prend en charge le CAR dans le Logiciel Cisco IOS version 11.1(20)CC, et chacune des 12.0 versions logicielles.

Le CAR affecte des performances dans une certaine mesure, basé sur la configuration du CAR. Obtenez les difficultés pour ces bogues : ID de bogue Cisco CSCdm85458 (clients enregistrés seulement) et ID de bogue Cisco CSCdm56071 (clients enregistrés seulement).

Remarque: Un grand nombre d'entrées de CAR dans une interface/sous-interface dégrade des performances parce que le routeur doit exécuter une recherche Linéaire sur les déclarations de CAR pour trouver la déclaration de « CAR » qui apparie.

D'autres caractéristiques et solutions de rechange

L'IP reçoivent l'ACL

Le Logiciel Cisco IOS version 12.0(22)S contient l'IP reçoivent la fonctionnalité d'ACL sur le Routeur Internet de la série Cisco 12000.

L'IP reçoivent la fonctionnalité d'ACL fournit les filtres de base pour le trafic destiné pour atteindre le routeur. Le routeur peut protéger le trafic prioritaire de protocole de routage contre une attaque parce que la caractéristique filtre toute la liste de contrôle d'accès d'entrée (ACL) sur l'interface

d'entrée. L'IP reçoivent des filtres de fonctionnalité d'ACL trafiquent sur les linecards distribués avant que le processeur d'artère reçoive des paquets. Cette caractéristique permet à des utilisateurs pour filtrer des inondations du Déni de service (DOS) contre le routeur. Par conséquent, cette caractéristique empêche la dégradation de représentation du processeur d'artère.

Référez-vous à l'IP reçoivent l'APL pour plus de détails.

Fonction IP Source Tracker

Le Logiciel Cisco IOS version 12.0(21)S prend en charge la caractéristique de Fonction IP Source Tracker sur le Routeur Internet de la série Cisco 12000. Le Logiciel Cisco IOS version 12.0(22)S prend en charge cette caractéristique sur le routeur de gamme Cisco 7500.

La caractéristique de Fonction IP Source Tracker te permet pour recueillir des informations au sujet du trafic qui circule à un hôte que vous suspectez est soumis aux attaques. Cette caractéristique te permet également pour tracer facilement une attaque de nouveau au point d'entrée dans le réseau. Quand vous identifiez le point d'entrée du réseau par cette caractéristique, vous pouvez utiliser ACLs ou CAR pour bloquer l'attaque efficacement.

Référez-vous au pour en savoir plus de Fonction IP Source Tracker.

Informations connexes

- Comment protéger votre réseau contre le virus Nimda
- L'IP reçoivent l'APL
- Fonction IP Source Tracker
- Support et documentation techniques - Cisco Systems