Pare-feu Cisco IOS Classic/IPS : Configuration du contrôle d'accès basé sur contexte (CBAC) pour la protection contre les attaques de déni de service

Contenu

Introduction

Ce document décrit la procédure de réglage des paramètres de déni de service (DoS) dans le pare-feu classique Cisco IOS® avec CBAC.

CBAC fournit des fonctionnalités avancées de filtrage du trafic et peut être utilisé comme partie intégrante de votre pare-feu réseau.

Le DoS désigne généralement une activité réseau qui dépasse intentionnellement ou non les ressources réseau telles que la bande passante de liaison WAN, les tables de connexion de pare-feu, la mémoire d'hôte final, le processeur ou les fonctionnalités de service. Dans le pire des cas, l'activité de déni de service submerge la ressource vulnérable (ou ciblée) au point que la ressource devient indisponible et interdit la connectivité WAN ou l'accès au service aux utilisateurs légitimes.

Le pare-feu Cisco IOS peut contribuer à limiter l'activité DoS s'il gère des compteurs du nombre de connexions TCP “ semi-ouvertes ”, ainsi que le taux de connexion total via le pare-feu et le logiciel de prévention des intrusions dans les pare-feu classiques (**ip inspect**) et les pare-feu de stratégie basés sur des zones.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Les connexions semi-ouvertes sont des connexions TCP qui n'ont pas terminé la connexion SYN-SYN/ACK-ACK en trois étapes, toujours utilisée par les homologues TCP pour négocier les paramètres de leur connexion mutuelle. Un grand nombre de connexions semi-ouvertes peut indiquer une activité malveillante, telle que des attaques par déni de service distribué (DDoS) ou des attaques par déni de service distribué (DoS). Un exemple d'attaque par déni de service est mené par des logiciels malveillants et intentionnellement développés, tels que des vers ou des virus qui infectent plusieurs hôtes sur Internet et tentent de submerger des serveurs Internet spécifiques par des attaques SYN, où un grand nombre de connexions SYN sont envoyées à un serveur par plusieurs hôtes sur Internet ou au sein du réseau privé d'une organisation. Les attaques SYN représentent un danger pour les serveurs Internet, car les tables de connexion des serveurs peuvent être chargées avec “ tentatives de connexion SYN ” qui arrivent plus rapidement que le serveur ne peut gérer les nouvelles connexions. Il s'agit d'un type d'attaque DoS car le grand nombre de connexions dans la liste de connexions TCP du serveur victime empêche l'accès légitime des utilisateurs aux serveurs Internet victimes.

Le pare-feu Cisco IOS considère également les sessions UDP (User Datagram Protocol) avec le trafic dans une seule direction comme “ ” semi-ouvert, car de nombreuses applications qui utilisent UDP pour le transport reconnaissent la réception des données. Les sessions UDP sans trafic de retour indiquent probablement une activité DoS ou des tentatives de connexion entre deux hôtes, où l'un des hôtes ne répond plus. De nombreux types de trafic UDP, tels que les messages de journalisation, le trafic de gestion de réseau SNMP, les flux de données vocales et vidéo et le trafic de signalisation, utilisent le trafic dans une seule direction pour acheminer leur trafic. La plupart de ces types de trafic utilisent des informations spécifiques aux applications pour éviter que les modèles de trafic unidirectionnel n'affectent négativement le comportement du pare-feu et des déni de service IPS.

Avant les versions 12.4(11)T et 12.4(10) du logiciel Cisco IOS, Cisco IOS Stateful Packet Inspection offrait une protection contre les attaques DoS par défaut lorsqu'une règle d'inspection était appliquée. Les versions 12.4(11)T et 12.4(10) du logiciel Cisco IOS ont modifié les

paramètres DoS par défaut de sorte que la protection DoS n'est pas appliquée automatiquement, mais les compteurs d'activité de connexion sont toujours actifs. Lorsque la protection DoS est active, c'est-à-dire lorsque les valeurs par défaut sont utilisées sur les versions logicielles précédentes ou que les valeurs ont été ajustées à la plage qui affecte le trafic, la protection DoS est activée sur l'interface où l'inspection est appliquée, dans la direction dans laquelle le pare-feu est appliqué, pour que les protocoles de configuration de la stratégie de pare-feu puissent inspecter. La protection DoS n'est activée sur le trafic réseau que si le trafic entre dans une interface ou en sort avec une inspection appliquée dans la même direction du trafic initial (paquet SYN ou premier paquet UDP) pour une connexion TCP ou une session UDP.

L'inspection du pare-feu Cisco IOS fournit plusieurs valeurs réglables pour protéger contre les attaques DoS. Les versions du logiciel Cisco IOS antérieures aux versions 12.4(11)T et 12.4(10) ont des valeurs de déni de service par défaut qui peuvent interférer avec le bon fonctionnement du réseau si elles ne sont pas configurées pour le niveau approprié d'activité du réseau dans les réseaux où les débits de connexion dépassent les valeurs par défaut. Ces paramètres vous permettent de configurer les points où la protection DoS de votre routeur de pare-feu commence à prendre effet. Lorsque les compteurs DoS de votre routeur dépassent les valeurs par défaut ou configurées, le routeur réinitialise une ancienne connexion semi-ouverte pour chaque nouvelle connexion qui dépasse les valeurs maximales configurées incomplètes ou élevées d'une minute jusqu'à ce que le nombre de sessions semi-ouvertes tombe en dessous des valeurs minimales maximales incomplètes. Le routeur envoie un message syslog si la journalisation est activée et si un système de prévention des intrusions (IPS) est configuré sur le routeur, le routeur pare-feu envoie un message de signature DoS par le biais de l'échange d'événements SDEE (Security Device Event Exchange). Si les paramètres DoS ne sont pas ajustés au comportement normal de votre réseau, une activité réseau normale peut déclencher le mécanisme de protection DoS, qui entraîne des pannes d'applications, des performances réseau médiocres et une utilisation élevée du CPU sur le routeur Cisco IOS Firewall.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Réglage du déni de service pour le pare-feu et le système de prévention des intrusions de la plate-forme logicielle Cisco IOS classique (IP Inspect)

Le pare-feu Cisco IOS classique gère un ensemble global de compteurs DoS pour le routeur, et toutes les sessions de pare-feu pour toutes les stratégies de pare-feu sur toutes les interfaces sont appliquées au jeu global de compteurs de pare-feu.

L'inspection de pare-feu classique Cisco IOS offre une protection contre les attaques DoS par défaut lorsqu'un pare-feu classique est appliqué. La protection DoS est activée sur toutes les interfaces où l'inspection est appliquée, dans la direction dans laquelle le pare-feu est appliqué, pour chaque service ou protocole que la stratégie de pare-feu est configurée pour inspecter. Le pare-feu classique fournit plusieurs valeurs ajustables pour protéger contre les attaques DoS. Les paramètres par défaut hérités (des images logicielles antérieures à la version 12.4(11)T) indiqués dans le tableau 1 peuvent interférer avec le bon fonctionnement du réseau s'ils ne sont pas configurés pour le niveau approprié d'activité du réseau dans les réseaux où les débits de

connexion dépassent les valeurs par défaut. Les paramètres DoS peuvent être affichés à l'aide de la commande exec **show ip inspect config**, et les paramètres sont inclus avec le résultat de **sh ip inspect all**.

Le CBAC utilise des délais et des seuils pour déterminer la durée de gestion des informations d'état pour une session, ainsi que pour déterminer quand supprimer des sessions qui ne sont pas entièrement établies. Ces délais et seuils s'appliquent globalement à toutes les sessions.

Tableau 1 Limites de protection DoS par défaut des pare-feu classiques		
Valeur de protection DoS	**Avant 12.4(11)T/12.4(10) **	**12.4(11)T/12.4(10) et versions ultérieures**
max-incomplet haute *valeur*	500	Illimité
faible *valeur* max-incomplète	400	Illimité
valeur élevée d'une minute	500	Illimité
valeur basse d'une minute	400	Illimité
valeur d'hôte tcp max-incomplète	50	Illimité

Les routeurs configurés pour appliquer Cisco IOS VRF-Aware Firewall gèrent un ensemble de compteurs pour chaque VRF.

Le compteur “ ip inspect one minute high ” and “ ip inspect one minute low maintient une somme de toutes les tentatives de connexion TCP, UDP et ICMP (Internet Control Message Protocol) dans la minute précédente du fonctionnement du routeur, que les connexions aient réussi ou non. Une augmentation du débit de connexion peut être le signe d'une infection par un ver sur un réseau privé ou d'une tentative d'attaque DoS contre un serveur.

Bien que vous ne puissiez “ désactiver ” la protection DoS de votre pare-feu, vous pouvez ajuster la protection DoS de sorte qu'elle ne prenne pas effet, sauf si un très grand nombre de connexions semi-ouvertes sont présentes dans la table de session de votre routeur de pare-feu.

Protection par pare-feu DoS

Suivez cette procédure pour régler la protection DoS de votre pare-feu sur l'activité de votre réseau :

1. Assurez-vous que votre réseau n'est pas infecté par des virus ou vers qui peuvent conduire à des valeurs de connexion semi-ouvertes erronées ou à des tentatives de connexion. Si votre réseau n'est pas “ propre, ” il n'y a aucun moyen de régler correctement la protection DoS de votre pare-feu. Vous devez observer l'activité de votre réseau au cours d'une période d'activité typique. Si vous ajustez les paramètres de protection DoS de votre réseau dans une période d'activité réseau faible ou inactive, les niveaux d'activité normaux dépassent probablement les paramètres de protection DoS.
2. Définissez les valeurs maximales incomplètes sur des valeurs très élevées :

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

Cela empêche le routeur de fournir une protection DoS pendant que vous observez les modèles de connexion de votre réseau. Si vous souhaitez désactiver la protection DoS, arrêtez cette procédure maintenant.**Remarque :** si votre routeur exécute le logiciel Cisco IOS Version 12.4(11)T ou ultérieure, ou 12.4(10) ou ultérieure, vous n'avez pas besoin de relever les valeurs par défaut de protection DoS ; ils sont déjà définis sur leurs limites maximales par défaut.**Remarque :** si vous voulez activer la prévention plus agressive de refus de service spécifique à l'hôte TCP qui inclut le blocage de l'initialisation de la connexion à un hôte, vous devez définir la durée de blocage spécifiée dans la commande **ip inspect tcp max-incomplete host**

3. Effacez les statistiques du pare-feu Cisco IOS avec cette commande :

```
show ip inspect statistics reset
```

4. Laissez le routeur configuré dans cet état pendant un certain temps, peut-être jusqu'à 24 à 48 heures, afin que vous puissiez observer le modèle de réseau pendant au moins une journée complète du cycle d'activité réseau classique.**Remarque :** bien que les valeurs soient ajustées à des niveaux très élevés, votre réseau ne bénéficie pas de la protection DoS Cisco IOS Firewall ou IPS.
5. Après la période d'observation, vérifiez les compteurs DoS à l'aide de cette commande :

```
show ip inspect statistics
```

Les paramètres que vous devez observer pour régler votre protection DoS sont mis en surbrillance en **gras** :

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. Configurez **ip inspect max-incomplet** à une valeur supérieure de 25 % à la valeur semi-ouverte du compte de session maxever indiquée de votre routeur. Un multiplicateur de 1,25

offre une hauteur de tête supérieure de 25 % au comportement observé, par exemple :

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

Configuration:

```
router(config)
   #ip inspect max-incomplete high 70
```

Remarque : Ce document décrit l'utilisation d'un multiplicateur égal à 1,25 fois l'activité type de votre réseau pour définir des limites de protection DoS. Si vous observez votre réseau dans des pics d'activité réseau typiques, cela doit fournir une marge de sécurité suffisante pour éviter l'activation de la protection DoS du routeur dans toutes les circonstances sauf atypiques. Si votre réseau voit régulièrement de grandes rafales d'activité réseau légitime qui dépassent cette valeur, le routeur utilise les fonctionnalités de protection DoS, qui peuvent avoir un impact négatif sur une partie du trafic réseau. Vous devez surveiller les journaux de votre routeur pour détecter les activités DoS et ajuster les limites **ip inspect max-incomplete high** et/ou **ip inspect one minute high** limit pour éviter le déclenchement de DoS, après avoir déterminé que les limites ont été rencontrées en raison d'une activité réseau légitime. Vous pouvez reconnaître l'application de protection DoS en présence de messages de journal tels que :

7. Configurez **ip inspect max-incomplet low** à la valeur affichée par votre routeur pour sa valeur semi-ouverte de compte de session maxever, par exemple :

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   ```

   Configuration:

   ```
   router(config)
      #ip inspect max-incomplete low 56
   ```

8. Le compteur **ip inspect one minute high** and **one minute low** conserve une somme de toutes les tentatives de connexion TCP, UDP et ICMP (Internet Control Message Protocol) dans la minute précédente du fonctionnement du routeur, que les connexions aient réussi ou non. Une augmentation du débit de connexion peut être le signe d'une infection par un ver sur un réseau privé ou d'une tentative d'attaque DoS contre un serveur. Une statistique d'inspection supplémentaire a été ajoutée à la sortie **show ip inspect statistics** dans les paragraphes 12.4(11)T et 12.4(10) afin de révéler la limite supérieure du taux de création de session. Si vous exécutez une version du logiciel Cisco IOS antérieure à 12.4(11)T ou 12.4(10), les statistiques d'inspection ne contiennent pas cette ligne :

   ```
   Maxever session creation rate [value]
   ```

   Les versions du logiciel Cisco IOS antérieures aux versions 12.4(11)T et 12.4(10) ne conservent pas de valeur pour le débit de connexion maximal d'une minute d'inspection. Vous devez donc calculer la valeur que vous appliquez en fonction des valeurs ” de nombre de sessions maximum observées “. Les observations de plusieurs réseaux qui utilisent l'inspection dynamique du pare-feu Cisco IOS version 12.4(11)T en production ont montré que les taux de création de sessions de Maxever ont tendance à dépasser de près de dix pour cent la somme des trois valeurs (établies, semi-ouvertes et terminées) dans “ nombre de sessions de maximum ”. Afin de calculer la valeur minimale d'une minute d'inspection ip, multipliez la valeur ” établie “ indiquée par 1,1, par exemple :

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   (207 + 56 + 35) * 1.1 = 328
   ```

   Configuration:

```
ip inspect one-minute low 328
```

Si le routeur exécute le logiciel Cisco IOS Version 12.4(11)T ou ultérieure, ou 12.4(10) ou ultérieure, vous pouvez simplement appliquer la valeur indiquée dans la statistique d'inspection " taux de création de session " Maxever :

```
Maxever session creation rate 330
```

Configuration:

```
ip inspect one-minute low 330
```

9. Calculer et configurer **ip inspect une minute de haut**. La valeur élevée d'une minute ip inspect doit être supérieure de 25 % à la valeur inférieure d'une minute calculée, par exemple :

```
ip inspect one-minute low (330) * 1.25 = 413
```

Configuration:

```
ip inspect one-minute high 413
```

Remarque : Ce document décrit l'utilisation d'un multiplicateur égal à 1,25 fois l'activité type de votre réseau pour définir des limites de protection DoS. Si vous observez votre réseau dans des pics d'activité réseau typiques, cela doit fournir une marge de sécurité suffisante pour éviter l'activation de la protection DoS du routeur dans toutes les circonstances sauf atypiques. Si votre réseau voit régulièrement de grandes rafales d'activité réseau légitime qui dépassent cette valeur, le routeur utilise les fonctionnalités de protection DoS, qui peuvent avoir un impact négatif sur une partie du trafic réseau. Vous devez surveiller les journaux de votre routeur pour détecter les activités DoS et ajuster les limites **ip inspect max-incomplete high** et/ou **ip inspect one minute high** limit pour éviter le déclenchement de DoS, après avoir déterminé que les limites ont été rencontrées en raison d'une activité réseau légitime. Vous pouvez reconnaître l'application de protection DoS en présence de messages de journal tels que :

10. Vous devez définir une valeur pour **ip inspect tcp max-incomplete host** conformément à votre connaissance de la capacité de vos serveurs. Ce document ne peut pas fournir de directives pour la configuration de la protection DoS par hôte, car cette valeur varie considérablement en fonction des performances matérielles et logicielles de l'hôte final. Si vous n'êtes pas certain des limites appropriées à configurer pour la protection DoS, vous avez effectivement deux options pour définir les limites DoS :L'option préférable est de configurer la protection DoS basée sur routeur par hôte à une valeur élevée (inférieure ou égale à la valeur maximale de 4 294 967 295) et d'appliquer la protection spécifique à l'hôte offerte par le système d'exploitation de chaque hôte ou un système de protection contre les intrusions basé sur hôte externe tel que Cisco Security Agent (CSA).Examinez les journaux d'activité et de performances de vos hôtes réseau et déterminez leur taux de connexion maximal durable. Puisque le pare-feu classique ne propose qu'un seul compteur global, vous devez appliquer la valeur maximale que vous déterminez après avoir vérifié les débits de connexion maximaux de tous vos hôtes réseau. Il est toujours conseillé d'utiliser des limites d'activité spécifiques au système d'exploitation et un système de prévention des intrusions basé sur l'hôte, tel que CSA.**Remarque :** Cisco IOS Firewall offre une protection limitée contre les attaques dirigées contre des vulnérabilités spécifiques des systèmes d'exploitation et des applications. La protection DoS du pare-feu Cisco IOS n'offre aucune garantie de protection contre les attaques sur les services d'hôte final exposés à des environnements potentiellement hostiles.
11. Surveillez l'activité de protection DoS de votre réseau. Idéalement, vous devez utiliser un serveur syslog ou, idéalement, une station MARS (Cisco Monitoring and Reporting Stations) pour enregistrer les occurrences de détection d'attaque DoS. Si la détection se produit très fréquemment, vous devez surveiller et ajuster vos paramètres de protection DoS.Pour plus d'informations sur les attaques DoS SYN TCP, référez-vous à Définition de

stratégies de protection contre les attaques par déni de service SYN TCP.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems