# 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 accord pour des paramètres du Déni de service (DOS) dans le Pare-feu classique de Cisco IOS® avec CBAC.

CBAC fournit la fonctionnalité de filtrage du trafic avancé et peut être utilisé en tant que partie intégrante de votre pare-feu réseau.

Le DOS se rapporte généralement à l'activité réseau qu'accable intentionnellement ou involontairement des ressources de réseau telles que la bande passante de lien WAN, les tables de connexion de Pare-feu, la mémoire de fin-hôte, la CPU, ou les capacités de services. Dans un pire scénario, l'activité DOS accable (ou visé) la ressource vulnérable au point que la ressource devient indisponible, et elle interdit l'accès de connectivité WAN ou de service aux utilisateurs légitimes.

Le Pare-feu Cisco IOS peut contribuer à la réduction de l'activité DOS s'il met à jour des compteurs du nombre de « entrouvrent » des connexions TCP, aussi bien que toute la vitesse de connexion par le logiciel de Pare-feu et de prévention des intrusions dans le Pare-feu classique (**ip inspect**) et le Pare-feu basé sur zone de stratégie.

# Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

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

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

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-duplex sont des connexions TCP qui ne se sont pas terminées la prise de contact à trois voies SYN-SYN/ACK-ACK qui est toujours utilisée par des pairs de TCP pour négocier les paramètres de leur connexion mutuelle. Un grand nombre de connexions semi-duplex peuvent être indicatives de l'action malveillante, telle que des attaques DOS ou de déni de service distribué (DDoS). Un exemple d'un type d'attaque DoS est conduit par le logiciel malveillant et intentionnel-développé, tel que des vers ou les virus qui infectent de plusieurs hôtes sur l'Internet et la tentative d'accabler les serveurs Internet spécifiques avec la synchronisation attaque, où un grand nombre de connexions de synchronisation sont envoyées à un serveur par de plusieurs hôtes sur l'Internet ou dans le réseau privé d'une organisation. Les attaques de synchronisation représentent un risque aux serveurs Internet puisque les tables de connexion des serveurs peuvent être chargées avec les tentatives « factices » de connexion de synchronisation qui arrivent plus rapide que le serveur peuvent traiter les nouvelles connexions. C'est un type d'attaque DoS parce que le grand nombre de connexions dans la liste de connexion TCP du serveur de victime empêchent l'accès d'utilisateur légitime aux serveurs Internet de victime.

Le Pare-feu Cisco IOS considère également des sessions de Protocole UDP (User Datagram Protocol) avec le trafic dans seulement une direction comme « entrouvrent » parce que beaucoup d'applications qui utilisent l'UDP pour le transport reconnaissent la réception des données. Les sessions d'UDP sans trafic de retour sont vraisemblablement indicatives de l'activité ou des tentatives DOS de se connecter entre deux hôtes, où un des hôtes est devenu insensible. Beaucoup de types de trafic UDP, tels que les messages de log, le trafic de gestion du réseau SNMP, coulant les medias de Voix et de vidéo, et le trafic de signalisation, seulement le trafic d'utilisation dans une direction pour porter leur trafic. Plusieurs de ces types de trafic appliquent l'intelligence spécifique à l'application d'empêcher des modèles de trafic unidirectionnel de compromettre le Pare-feu et l'IPS de comportement DOS.

Avant le Logiciel Cisco IOS version 12.4(11)T et 12.4(10), l'inspection de Stateful Packet de Cisco IOS a assuré la protection contre des attaques DOS comme par défaut quand une règle

d'inspection était appliquée. Le Logiciel Cisco IOS version 12.4(11)T et 12.4(10) ont modifié les configurations DOS de par défaut de sorte que la protection DOS ne soit pas automatiquement appliquée, mais les compteurs d'activité de connexion sont encore en activité. Quand la protection DOS est en activité, c.-à-d., quand les valeurs par défaut sont utilisées sur des versions logicielles plus anciennes, ou les valeurs ont été ajustés à la plage qui affectent 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 politique de Pare-feu examinent. La protection DOS est seulement activée sur le trafic réseau si le trafic écrit ou part d'une interface avec l'inspection appliquée dans la même direction du trafic initial (paquet de synchronisation ou premier paquet UDP) pour une connexion TCP ou une session d'UDP.

L'inspection de Pare-feu Cisco IOS fournit plusieurs valeurs réglables pour se protéger contre des attaques DoS. Les versions logicielles de Cisco IOS avant 12.4(11)T et 12.4(10) ont des valeurs par défaut DOS qui peuvent gêner l'exploitation réseau appropriée s'ils ne sont pas configurés pour le niveau approprié de l'activité réseau dans les réseaux où les vitesses de connexion dépassent les par défaut. Ces paramètres te permettent pour configurer les points auxquels la protection DOS de votre routeur de Pare-feu commence à la prendre effet. Quand les compteurs DOS de votre routeur dépassent le par défaut ou les valeurs configurées, le routeur remet à l'état initial une vieille connexion semi-duplex pour chaque nouvelle connexion qui dépasse les valeurs élevées configurées max-incomplete ou d'one-minute jusqu'au nombre de baisses entrouvertes de sessions au-dessous des faibles valeurs max-incomplete. Le routeur envoie un message de Syslog si se connecter est activé, et si un Système de prévention d'intrusion (IPS) est configuré sur le routeur, le routeur de Pare-feu envoie un message de signature DOS par l'échange d'événement de périphérique de sécurité (SDEE). Si les paramètres DOS ne sont pas ajustés au comportement normal de votre réseau, l'activité réseau normale peut déclencher le mécanisme de protection DOS, qui entraîne des pannes d'application, des performances du réseau pauvres, et l'utilisation du CPU élevé sur le routeur de Pare-feu Cisco IOS.

# Configurez

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

**Remarque:** Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Déni de service accordant pour le Pare-feu et le système de prévention des intrusions classiques de logiciel de Cisco IOS (ip inspect)

Le Pare-feu de Cisco IOS classique met à jour 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 à l'ensemble global de compteurs de Pare-feu.

L'inspection classique de Pare-feu de Cisco IOS assure la protection contre l'attaque DoS par défaut quand 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 examiner. Le Pare-feu classique fournit plusieurs valeurs réglables pour se protéger contre des attaques DoS. Les valeurs par défaut existantes (des images logicielles avant release 12.4(11)T) affichées dans le tableau 1 peuvent gêner l'exploitation réseau appropriée si elles ne sont pas configurées pour le niveau approprié de l'activité réseau dans les réseaux où les vitesses de connexion dépassent les

par défaut. Les configurations DOS peuvent être visualisées avec le **config de show ip inspect de** commande EXEC, et les configurations sont incluses avec **toute la** sortie de l'**ip inspect SH**.

CBAC emploie des délais d'attente et des seuils pour déterminer combien de temps gérer les informations d'état pour une session, aussi bien que déterminer quand relâcher les sessions qui ne deviennent pas entièrement établies. Ces délais d'attente et seuils s'appliquent globalement à toutes les sessions.

| **Limites classiques de protection DOS de par défaut de Pare-feu du tableau 1** | | |
|---|---|---|
| **Valeur de protection DOS** | **Avant 12.4(11)T/12.4(10)** | **12.4(11)T/12.4(10) et plus tard** |
| valeur élevée max-incomplete | 500 | Illimité |
| faible valeur max-incomplete | 400 | Illimité |
| valeur élevée d'one-minute | 500 | Illimité |
| faible valeur d'one-minute | 400 | Illimité |
| *valeur d'*hôte de tcp max-incomplete | 50 | Illimité |

Les Routeurs configurés pour appliquer le Pare-feu Vrf-averti de Cisco IOS mettent à jour un ensemble de compteurs pour chaque VRF.

Le compteur pour le « ip inspect one-minute high » et le « ip inspect one-minute low » met à jour une somme de tous les TCP, UDP, et tentatives de connexion de Protocole ICMP (Internet Control Message Protocol) dans la minute antérieure du fonctionnement du routeur, que les connexions aient été réussies ou pas. Une vitesse de connexion étant en hausse peut être indicative d'une infection de ver sur un réseau privé ou d'une attaque DoS tentée contre un serveur.

Tandis que vous ne pouvez pas « désactiver » la protection DOS de votre Pare-feu, vous pouvez ajuster la protection DOS de sorte qu'elle ne la prenne pas effet à moins qu'un très grand nombre de connexions semi-duplex soient présentes dans la table de session de votre routeur de Pare-feu.

## Protection pare-feu DOS

Suivez cette procédure pour accorder la protection DOS de votre Pare-feu à l'activité de votre réseau :

1. Soyez sûr que votre réseau n'est pas infecté par les virus ou vers qui peuvent mener aux valeurs incorrectement grandes de connexion semi-duplex ou aux vitesses de connexion tentées. Si votre réseau n'est pas « propre, » il n'y a aucune manière d'ajuster 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 accordez les configurations de protection DOS de

votre réseau au cours d'une période de bas ou d'activité réseau d'inactif, les niveaux d'activité normaux dépassent vraisemblablement les configurations de protection DOS.

2. Placez les valeurs élevées max-incomplete très aux valeurs élevées : **ip inspect max-incomplete high 20000000 ip inspect one-minute high 100000000 ip inspect tcp max-incomplete host 100000 block-time 0** Ceci empêche le routeur d'assurer la protection DOS tandis que vous observez les modèles de connexion de votre réseau. Si vous souhaitez laisser la protection DOS désactivée, arrêtez cette procédure maintenant.**Remarque:** Si votre routeur exécute le Logiciel Cisco IOS version 12.4(11)T ou plus tard, ou 12.4(10) ou plus tard, vous n'avez pas besoin de soulever les valeurs de protection DOS de par défaut ; ils sont déjà placés à leurs limites maximum par défaut.**Remarque:** Si vous voulez activer la prévention plus agressive de déni de service d'hôte-particularité de TCP qui inclut le blocage de la demande de connexion à un hôte, vous devez placer la bloc-heure spécifiée dans la commande d'**ip inspect tcp max-incomplete host**
3. Effacez les statistiques de Pare-feu Cisco IOS avec cette commande : **show ip inspect statistics reset**
4. Laissez le routeur configuré dans cet état pendant quelque temps, peut-être tant que 24 à 48 heures, ainsi vous peuvent observer le modèle de réseau plus d'au moins un jour complet du cycle d'activité de réseau ordinaire.**Remarque:** Tandis que les valeurs sont ajustées aux très hauts niveaux, votre réseau ne tire pas bénéfice du Pare-feu Cisco IOS ou de l'IPS de protection DOS.
5. Après la période d'observation, vérifiez les compteurs DOS avec cette commande : **show ip inspect statistics** Les paramètres que vous devez observer avec ce que pour accorder votre protection DOS sont mis en valeur 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 l'**ip inspect max-incomplete high à un** supérieur à de la valeur 25-percent la valeur entrouverte indiquée de comptage des sessions de maxever de votre routeur. 1.25 un comportement observé ci-dessus de marge des offres 25-percent de multiplicateur, par exemple :`Maxever session counts`
   `(estab/half-open/terminating) [207:56:35]`
`56 * 1.25 = 70`

   Configurez :`router(config)`

   `#ip inspect max-incomplete high 70`**Remarque:** Ce document décrit l'utilisation d'un multiplicateur de 1.25 fois l'activité typique de votre réseau de fixer des limites pour engager la protection DOS. Si vous observez votre réseau dans des crêtes d'activité de réseau ordinaire, ceci doit fournir la marge adéquate pour éviter le lancement de la protection DOS du routeur sous presque des circonstances atypiques. Si votre réseau voit périodiquement les grandes rafales de l'activité réseau légitime qui dépassent cette valeur, le routeur engage

les capacités de protection DOS, qui peuvent entraîner une incidence négative sur une partie du trafic réseau. Vous devez surveiller vos journaux du routeur pour des détections d'activité DOS et ajuster l'**ip inspect max-incomplete high** et/ou les limites d'**ip inspect one-minute high** pour éviter de déclencher le DOS, après que vous déterminiez que les limites ont été produites en raison de l'activité réseau légitime. Vous pouvez identifier l'application de protection DOS par la présence des messages de log de ce type :

7. Configurez l'**ip inspect max-incomplete low à la** valeur votre routeur affiché pour sa valeur entrouverte de comptage des sessions de maxever, par exemple :`Maxever session counts (estab/half-open/terminating) [207:56:35]`Configurez :`router(config) #ip inspect max-incomplete low 56`
8. Le compteur pour l'**ip inspect one-minute high** et le **bas d'one-minute** met à jour une somme de tous les TCP, UDP, et tentatives de connexion de Protocole ICMP (Internet Control Message Protocol) dans la minute antérieure de l'exécution de routeur, que les connexions aient été réussies ou pas. Une vitesse de connexion étant en hausse peut être indicative d'une infection de ver sur un réseau privé, ou d'une attaque DoS tentée contre un serveur. Une statistique supplémentaire d'inspection a été ajoutée à la sortie de **statistiques de show ip inspect** dans 12.4(11)T et 12.4(10) pour indiquer la marque des grandes marées pour le débit de création de session. Si vous exécutez une version du logiciel Cisco IOS plus tôt que 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 avant 12.4(11)T et 12.4(10) ne mettent pas à jour une valeur pour la vitesse de connexion d'one-minute de maxever d'inspection, ainsi vous devez calculer la valeur que vous vous appliquez basé sur des valeurs observées « de comptage des sessions de maxever ». Les observations de plusieurs réseaux qui utilisent l'inspection avec état de la release 12.4(11)T de Pare-feu Cisco IOS dans la production ont prouvé que les débits de création de session de Maxever tendent à dépasser la somme des trois valeurs (établi, entrouvert, et se terminant) dans le « comptage des sessions de maxever » par approximativement dix pour cent. Afin de calculer la valeur d'ip inspect one-minute low, 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`
   Configurez :`ip inspect one-minute low 328`Si le routeur exécute le Logiciel Cisco IOS version 12.4(11)T ou plus tard, ou 12.4(10) ou plus tard, vous pouvez simplement appliquer la valeur affichée dans la statistique d'inspection « de débit de création de session de Maxever » :`Maxever session creation rate 330`Configurez :`ip inspect one-minute low 330`
9. Calculez et configurez l'**ip inspect one-minute high**. La valeur d'ip inspect one-minute high doit être 25-percent plus grand que la faible valeur calculée d'one-minute, par exemple :`ip inspect one-minute low (330) * 1.25 = 413` Configurez :`ip inspect one-minute high 413`**Remarque:** Ce document décrit l'utilisation d'un multiplicateur de 1.25 fois l'activité typique de votre réseau de fixer des limites pour engager la protection DOS. Si vous observez votre réseau dans des crêtes d'activité de réseau ordinaire, ceci doit fournir la marge adéquate pour éviter le lancement de la protection DOS du routeur sous presque des circonstances atypiques. Si votre réseau voit périodiquement les grandes rafales de l'activité réseau légitime qui dépassent cette valeur, le routeur engage les capacités de protection DOS, qui peuvent entraîner une incidence négative sur une partie du trafic réseau. Vous devez surveiller vos journaux du routeur pour des détections d'activité DOS et ajuster l'**ip inspect max-incomplete high** et/ou les limites d'**ip inspect one-minute high** pour éviter de déclencher le DOS, après que vous déterminiez que les limites ont été produites en raison de l'activité

réseau légitime. Vous pouvez identifier l'application de protection DOS par la présence des messages de log de ce type :

10. Vous devez définir une valeur pour l'**ip inspect tcp max-incomplete host** selon votre connaissance de la capacité de vos serveurs. Ce document ne peut pas fournir des instructions pour la configuration de protection DOS de par-hôte puisque cette valeur varie largement basé sur la représentation de matériel et de logiciel de fin-hôte. Si vous êtes incertain au sujet des limites appropriées pour configurer pour la protection DOS, vous avez efficacement deux options avec lesquelles définir le DOS limite :L'option préférable est de configurer la protection basée sur routeur DOS de par-hôte à une valeur élevée (inférieur ou égal à la valeur maximale de 4,294,967,295), et applique la protection d'hôte-particularité offerte par le système d'exploitation de chaque hôte ou un système de protection contre les intrusions géré par le système central externe tel que le Cisco Security Agent (CSA).Examinez l'activité et la représentation ouvre une session vos hôtes réseau et détermine leur vitesse de connexion viable maximale. Puisque le Pare-feu classique offre seulement un compteur global, vous devez appliquer la valeur maximale que vous déterminez après que vous vérifiiez tous vos hôtes réseau pour leurs débits de nombre maximal de connexions. Il est encore recommandé que vous utilisiez des limites d'activité de Système d'exploitation-particularité et un IPS géré par le système central tel que CSA.**Remarque:** Le Pare-feu Cisco IOS offre la protection limitée contre des attaques dirigées sur des vulnérabilités spécifiques de système d'exploitation et d'application. La protection DOS du Pare-feu Cisco IOS n'offre aucune garantie de la protection contre la compromission sur des services de fin-hôte qui sont exposés aux environnements potentiellement hostiles.
11. Surveillez l'activité de protection DOS votre réseau. Dans le meilleur des cas, vous devez utiliser un serveur de Syslog, ou idéalement, Cisco surveillant et signalant des stations (MARS) aux occurrences d'article de la 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 des attaques DoS de synchronisation de TCP, référez-vous à définir des stratégies pour se protéger contre des attaques par déni de service de synchronisation de TCP.

## Vérifiez

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** .

## Dépannez

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