

Paramètres de connexion

Ce chapitre décrit comment configurer les paramètres de connexion pour les connexions qui passent par l'ASA ou pour les connexions de gestion, qui vont à l'ASA.

- Que sont les paramètres de connexion ?, à la page 1
- Configurer les paramètres de connexion, à la page 2
- Supervision des connexions, à la page 24
- Historique des paramètres de connexion, à la page 25

Que sont les paramètres de connexion ?

Les paramètres de connexion comprennent une variété de fonctionnalités liées à la gestion des connexions de trafic, telles qu'un flux TCP dans ASA. Certaines fonctionnalités sont des composants nommés que vous configurez pour fournir des services spécifiques.

Les paramètres de connexion sont les suivants :

- **Délais d'expiration globaux pour divers protocoles** : Tous les délais d'expiration globaux ont des valeurs par défaut, vous devez donc les modifier uniquement si vous subissez une perte de connexion prématurée.
- **Délai d'expiration de la connexion par classe de trafic** : vous pouvez remplacer les délais d'expiration globaux pour des types de trafic spécifiques à l'aide des politiques de service. Tous les délais d'expiration de classes de trafic ont des valeurs par défaut, vous n'avez donc pas besoin de les définir.
- **Limites de connexion et interception TCP** : par défaut, il n'y a aucune limite au nombre de connexions pouvant passer par (ou vers) l'ASA. Vous pouvez définir des limites pour des classes de trafic particulières en utilisant des règles de politique de service pour protéger les serveurs contre les attaques par déni de service (DoS). En particulier, vous pouvez définir des limites sur les connexions amorces (celles qui n'ont pas terminé la prise de contact TCP), ce qui protège contre les attaques par inondation SYN. Lorsque les limites amorces sont dépassées, le composant TCP Intercept intervient pour les connexions mandataires et s'assure que les attaques sont limitées.
- **Détection des connexions mortes (DCD)** : si vous avez des connexions persistantes qui sont valides, mais souvent inactives, de sorte qu'elles sont fermées parce qu'elles dépassent les paramètres de délai d'inactivité, vous pouvez activer la détection des connexions mortes pour identifier les connexions inactives, mais valides, et les maintenir actives (en réinitialisant leurs temporisateurs d'inactivité). Chaque fois que les durées d'inactivité sont dépassées, la DCD sonde les deux côtés de la connexion pour voir si les deux côtés s'entendent pour dire que la connexion est valide. La sortie de la commande **show**

service-policy comprend des compteurs pour afficher le volume d'activité du DCD. Vous pouvez utiliser la commande **show conn detail** pour obtenir des renseignements sur l'initiateur et le répondeur, et indiquer la fréquence à laquelle chacun a envoyé des sondes.

- **Randomisation de la séquence TCP** : chaque connexion TCP possède deux numéros de séquence initial (ISN) : un généré par le client et l'autre par le serveur. Par défaut, ASA rend aléatoire l'ISN du SYN TCP passant à la fois dans les sens entrant et sortant. La gestion aléatoire empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session. Cependant, la répartition aléatoire des séquences TCP rompt en pratique les SACK TCP (accusé de réception sélectif), car les numéros de séquence que voit le client sont différents de ce que le serveur voit. Vous pouvez désactiver la répartition aléatoire par classe de trafic si vous le souhaitez.
- **Normalisation TCP** : le normaliseur TCP offre une protection contre les paquets anormaux. Vous pouvez configurer le traitement de certains types d'anomalies de paquets par classe de trafic.
- **Contournement d'état TCP** : vous pouvez contourner la vérification de l'état TCP si vous utilisez le routage dissymétrique dans votre réseau.
- **Contournement d'état SCTP** : vous pouvez contourner l'inspection avec état du protocole SCTP (Stream Control Transmission Protocol) si vous ne souhaitez pas de validation du protocole SCTP.
- **Décharge de flux** : vous pouvez identifier le trafic à décharger vers un chemin super rapide, où les flux sont commutés dans la carte réseau elle-même. Le déchargement peut vous aider à améliorer les performances des applications exigeantes en données, telles que les transferts de fichiers volumineux.
- **Décharge de flux IPsec** : après la configuration initiale d'une association de sécurité (SA) IPsec de site à site ou d'accès à distance, les connexions IPsec sont déchargées vers le réseau portail programmable sur site (FPGA) dans le périphérique, ce qui devrait améliorer les performances du périphérique . Cette fonctionnalité est activée par défaut sur les plateformes qui la prennent en charge.

Configurer les paramètres de connexion

Les limites de connexion, les délais d'expiration, la normalisation TCP, l'aléatorisation de séquence TCP et le décrément de la durée de vie (TTL) ont des valeurs par défaut qui sont appropriées à la plupart des réseaux. Vous ne devez configurer ces paramètres de connexion que si vous avez des exigences hors du commun, si votre réseau dispose de types de configuration spécifiques ou si vous subissez des pertes de connexion anormales en raison d'un délai d'inactivité prématuré.

Les autres fonctionnalités liées à la connexion ne sont pas activées. Vous configurez ces services sur des classes de trafic spécifiques uniquement, et non en tant que service général. Ces fonctionnalités comprennent les éléments suivants : interception TCP, contournement de l'état TCP, détection de connexion inactive (DCD), contournement de l'état SCTP, déchargement de flux.

La procédure générale suivante couvre la gamme des configurations possibles des paramètres de connexion. Choisissez et sélectionnez les éléments à mettre en œuvre en fonction de vos besoins.

Avant de commencer

Lorsqu'un paquet entre dans le périphérique, le pare-feu évalue d'abord les règles de contrôle d'accès et le NAT pour déterminer si une entrée de connexion doit être créée. Une entrée de connexion est créée, qu'une entrée ARP existe pour le prochain saut. Ainsi, l'existence d'une connexion ne signifie pas qu'un paquet dans la portée de la connexion l'a fait par l'intermédiaire du périphérique. Les paramètres de connexion tels que

les délais d'inactivité garantissent que les connexions indésirables ne persistent pas et n'utilisent pas les ressources du système.

Procédure

Étape 1 Configurer les délais d'expiration globaux, à la page 3. Ces paramètres modifient les délais d'inactivité par défaut pour divers protocoles pour tout le trafic qui passe par le périphérique. Si vous rencontrez des problèmes avec la réinitialisation des connexions en raison d'un délai d'expiration prématuré, essayez d'abord de modifier les délais d'expiration globaux.

Étape 2 Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 6. Utilisez cette procédure pour configurer l'interception TCP.

Étape 3 Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP), à la page 8, si vous souhaitez modifier le comportement de normalisation TCP par défaut pour des classes de trafic spécifiques.

Étape 4 Contourner les vérifications de l'état TCP pour le routage asymétrique (TCP State Bypass), à la page 11, si vous disposez de ce type d'environnement de routage.

Étape 5 Désactiver la gestion aléatoire de la séquence TCP, à la page 13, si l'aléatorisation par défaut brouille les données pour certaines connexions.

Étape 6 Délester les flux volumineux, à la page 15, si vous devez améliorer les performances dans un centre de données exigeant en informatique.

Étape 7 Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services), à la page 19. Il s'agit d'une procédure « fourre-tout » pour les paramètres de connexion. Ces paramètres peuvent remplacer les valeurs globales par défaut pour des classes de trafic spécifiques à l'aide de règles de politique de service. Vous utilisez également ces règles pour personnaliser le normalisateur TCP, modifier l'aléatoire de séquence TCP, décrémenter la durée de vie des paquets et mettre en œuvre d'autres fonctionnalités facultatives.

Étape 8 Configurer les options TCP, à la page 23, si vous devez forcer les réinitialisations ou modifier un autre comportement TCP standard.

Configurer les délais d'expiration globaux

Vous pouvez définir les durées d'inactivité globales pour la connexion et les intervalles de traduction de divers protocoles. Si l'emplacement n'a pas été utilisé pendant la durée d'inactivité spécifiée, la ressource est remise dans le groupement (pool) libre.

La modification du délai d'expiration global définit un nouveau délai d'expiration par défaut, qui, dans certains cas, peut être remplacé pour des flux de trafic particuliers par le biais des politiques de service.

Pour les protocoles qui n'ont pas de paramètre de délai d'expiration configurable, comme GRE, le délai d'inactivité est de 2 minutes.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.

Étape 2 Configurez les délais d'expiration en cochant les cases des délais d'expiration que vous souhaitez modifier et en saisissant la nouvelle valeur.

Toutes les durées sont affichées au format *hh*:*mm*:*ss*, avec une durée maximale de 1193:0:0 dans la plupart des cas. Dans tous les cas, à l'exception de Authentication absolute (Authentification absolue) et de Authentication inactivity (Inactivité de l'authentification), le fait de décocher les cases ramène le délai d'expiration à la valeur par défaut. Dans ces deux cas, le fait de décocher la case signifie une réauthentification à chaque nouvelle connexion.

Saisissez 0 pour désactiver le délai d'expiration.

- **Connexion**—Le temps d'inactivité jusqu'à ce qu'un emplacement de connexion soit libéré. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 1 heure.
- **Half-Closed**—Le temps d'inactivité jusqu'à la fermeture d'une connexion TCP semi-fermée. Une connexion est considérée comme à moitié fermée si FIN et FIN-ACK ont été vus. Si seul le FIN a été vu, le délai d'expiration de connexion normal s'applique. La durée minimale est de 30 secondes. La valeur par défaut est 10 minutes.
- **UDP**—le temps d'inactivité avant la fermeture d'une connexion UDP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes.
- **ICMP**—le temps d'inactivité après lequel les états ICMP généraux sont fermés. La valeur par défaut et minimale est de 2 secondes.
- **Erreur ICMP** : délai d'inactivité avant que l'ASA supprime une connexion ICMP après avoir reçu un paquet de réponse ECHO ICMP, entre 0:0:0 et 0:1:0 ou la valeur du délai d'expiration ICMP, selon la valeur la plus basse. La valeur par défaut est 0 (désactivé). Lorsque ce délai d'expiration est désactivé et que vous activez l'inspection ICMP, l'ASA supprime la connexion ICMP dès qu'une réponse d'écho est reçue; ainsi, toutes les erreurs ICMP générées pour la connexion (maintenant fermée) sont abandonnées. Ce délai d'expiration retarde la suppression des connexions ICMP afin que vous puissiez recevoir des erreurs ICMP importantes.
- **H.323**—le temps d'inactivité après lequel les connexions multimédias H.245 (TCP) et H.323 (UDP) sont fermées. La valeur par défaut est et minimale est de 5 minutes. Comme le même indicateur de connexion est défini sur les connexions multimédias H.245 et H.323, la connexion H.245 (TCP) partage le délai d'inactivité avec la connexion multimédia H.323 (RTP et RTCP).
- **H.225**—le temps d'inactivité avant la fermeture d'une connexion de signalisation H.225. La valeur par défaut est de 1 heure. Pour fermer une connexion immédiatement après l'élimination de tous les appels, un délai d'expiration de 1 seconde (0:0:1) est recommandé.
- **MGCP**—le temps d'inactivité après lequel une connexion de support MGCP est supprimée. La valeur par défaut est de 5 minutes, mais vous pouvez la fixer à 1 seconde.
- **MGCP PAT**—le temps d'inactivité après lequel une traduction de PAT MGCP est supprimée. La valeur par défaut est 5 minutes. La durée minimale est de 30 secondes.
- **TCP Proxy Reassembly**—le délai d'inactivité après lequel les paquets en mémoire tampon en attente de réassemblage sont abandonnés, entre 0:0:10 et 1193:0:0. La valeur par défaut est de 1 minute (0:1:0).
- **Floating Connection**—Lorsqu'il existe plusieurs routes vers un réseau avec différentes métriques, le système utilise celle ayant la meilleure métrique au moment de la création de la connexion. Si un meilleur routage devient disponible, ce délai d'expiration permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser le meilleur routage. La valeur par défaut est 0 (la connexion n'expire jamais). Pour permettre d'utiliser de meilleures routes, définissez le délai d'expiration à une valeur comprise entre 0:0:30 et 1193:0:0. Cette minuterie ne s'applique pas aux connexions par le biais

d'interfaces de tunnel virtuel (VTI). Si une connexion par l'intermédiaire d'un VTI est bloquée, vous devez l'effacer manuellement.

- **SCTP** : délai d'inactivité jusqu'à la fermeture d'une connexion SCTP (Stream Control Transmission Protocol), entre 0:1:0 et 1193:0:0. La valeur par défaut est 2 minutes. (0:2:0)
- **Stale Routes** (Routes périmées) — Durée de conservation d'une route périmée avant de la retirer de la base d'informations du routeur. Ces routes sont destinées aux protocoles de passerelle interne tels que OSPF. La valeur par défaut est de 70 secondes (00:01:10), la plage est comprise entre 00:00:10 et 00:01:40.
- **SUNRPC**—le temps d'inactivité jusqu'à ce qu'un emplacement SunRPC soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 10 minutes.
- **SIP**—le temps d'inactivité avant la fermeture d'une connexion de port de signalisation SIP. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 30 minutes.
- **SIP Media**—le temps d'inactivité avant la fermeture d'une connexion de port de support SIP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes. La minuterie de médias SIP est utilisée pour les paquets de médias SIP RTP/RTCP avec SIP UDP, plutôt que le délai d'inactivité d'UDP.
- **SIP Provisional Media**—la valeur du délai d'expiration pour les connexions multimédias provisoires SIP, entre 1 et 30 minutes. La valeur par défaut est 2 minutes.
- **SIP Invite**—le temps d'inactivité après lequel les passages pour les réponses PROVISOIRES et les xlates de médias seront fermés, entre 0:1:0 et 00:30:0. La valeur par défaut est de 3 minutes. (0:3:0).
- **SIP Disconnect**—le temps d'inactivité après lequel la session SIP est supprimée si 200 OK n'est pas reçu pour un message CANCEL ou BYE, entre 0:0:1 et 0:10:0. La valeur par défaut est 2 minutes. (0:2:0)
- **Authentication absolute**—la durée jusqu'à ce que la mémoire cache d'authentification expire et que les utilisateurs doivent s'authentifier à nouveau pour une nouvelle connexion. Cette minuterie est utilisée uniquement dans le mandataire direct, ce qui est une règle AAA. Cette durée doit être inférieure au délai d'expiration de l'intervalle de traduction. Le système attend que l'utilisateur établisse une nouvelle connexion pour demander à nouveau. Avant de désactiver la mise en cache pour forcer l'authentification à chaque nouvelle connexion, tenez compte des limites suivantes.
  - Ne définissez pas cette valeur à 0 si le FTP passif est utilisé sur les connexions.
  - Lorsque la valeur absolue de l'authentification est 0, l'authentification HTTPS peut ne pas fonctionner. Si un navigateur lance plusieurs connexions TCP pour téléverser une page Web après l'authentification HTTPS, la première connexion est autorisée, mais les connexions suivantes déclenchent l'authentification. Par conséquent, une page d'authentification s'affiche en permanence, même après une authentification réussie. Pour contourner ce problème, définissez le délai d'expiration absolu de l'authentification à 1 seconde. Cette solution de contournement ouvre une fenêtre d'occasion d'une seconde qui pourrait permettre aux utilisateurs non authentifiés de traverser le pare-feu s'ils proviennent de la même adresse IP source.
- **Authentication inactivity**—le temps d'inactivité jusqu'à ce que le cache d'authentification expire et que les utilisateurs doivent s'authentifier à nouveau pour une nouvelle connexion. Cette durée doit être inférieure à la valeur de l'intervalle de traduction. Ce délai est désactivé par défaut. Ce délai est désactivé par défaut. Cette minuterie est utilisée uniquement dans le mandataire direct, ce qui est une règle AAA.
- **Translation Slot**—le temps d'inactivité jusqu'à ce qu'un intervalle de traduction NAT soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est de 3 heures.

- **PAT Translation Slot** (8.4(3) et versions ultérieures, sans inclure 8.5(1) et 8.6(1))—Le temps d'inactivité jusqu'à ce qu'un intervalle de traduction PAT soit libéré, entre 0:0:30 et 0:5:0. La valeur par défaut est de 30 secondes. Vous pourriez souhaiter augmenter le délai d'expiration si les routeurs en amont rejettent les nouvelles connexions utilisant un port PAT libéré, car la connexion précédente pourrait toujours être ouverte sur le périphérique en amont.
- **Connection Holddown** (Maintien de connexion) — Durée pendant laquelle le système doit maintenir une connexion lorsque la route utilisée par la connexion n'existe plus ou est inactive. Si le routage ne devient pas actif au cours de cette période d'attente, la connexion est libérée. Le but de la minuterie de maintien de connexion est de réduire l'effet du basculement des routes, où les routes peuvent apparaître et disparaître rapidement. Vous pouvez réduire le délai de maintien pour accélérer la convergence des routes. La valeur par défaut est de 15 secondes, et la plage est comprise entre 00:00:00 et 00:00:15.

Étape 3 Cliquez sur **Apply** (Appliquer).

Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP)

Une attaque par déni de service par inondation SYN se produit lorsqu'un attaquant envoie une série de paquets SYN à un hôte. Ces paquets proviennent généralement d'adresses IP usurpées. Le flux constant de paquets SYN maintient la file d'attente SYN du serveur pleine, ce qui l'empêche de répondre aux demandes de connexion des utilisateurs légitimes.

Vous pouvez limiter le nombre de connexions amorces pour aider à prévenir les attaques par inondation SYN. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination.

Lorsque le seuil de connexion embryonnaire d'une connexion est franchi, l'ASA agit comme un proxy pour le serveur et génère une réponse SYN-ACK à la requête SYN du client à l'aide de la méthode des cookies SYN, de sorte que la connexion ne soit pas ajoutée à la file d'attente SYN de l'hôte ciblé. Le témoin SYN est le numéro de séquence initial renvoyé dans le SYN-ACK qui est construit à partir du MSS, de l'horodatage et d'un hachage mathématique d'autres éléments pour créer principalement un code secret. Si l'ASA reçoit un ACK en retour du client avec le numéro de séquence correct et dans la fenêtre temporelle valide, il peut alors authentifier que le client est réel et autoriser la connexion au serveur. Le composant qui effectue le rôle de mandataire s'appelle TCP Intercept.

Le processus de bout en bout pour protéger un serveur contre une attaque par inondation SYN implique la définition des limites de connexion, l'activation des statistiques d'interception TCP, puis la surveillance des résultats.

Avant de commencer

- Veillez à ce que la limite de connexions amorces soit inférieure à la file d'attente TCP SYN sur le serveur que vous souhaitez protéger. Sinon, les clients valides ne peuvent plus accéder au serveur pendant une attaque SYN. Pour déterminer des valeurs raisonnables pour les limites amorces, analysez soigneusement la capacité du serveur, le réseau et l'utilisation du serveur.
- Selon le nombre de cœurs de CPU sur votre modèle d'ASA, le nombre maximal de connexions simultanées et de connexions embryonnaires peut dépasser les nombres configurés en raison de la façon dont chaque cœur gère les connexions. Dans le pire des cas, l'ASA autorise jusqu'à *n*-1 connexions supplémentaires et connexions embryonnaires, où *n* est le nombre de cœurs. Par exemple, si votre modèle comporte 4

cœurs, si vous configurez 6 connexions simultanées et 4 connexions amorces, vous pourriez en avoir 3 de chaque type. Pour déterminer le nombre de cœurs correspondant à votre modèle, saisissez la commande **show cpu core**.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)**.

Étape 2 Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour les serveurs que vous souhaitez protéger, modifiez-la.

Étape 3 Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).

Étape 4 Pour Traffic Classification (Classification du trafic), sélectionnez **Source and Destination IP Addresses (uses ACL)** (Adresses IP source et de destination [utilise l'ACL]) et cliquez sur **Next** (Suivant).

Étape 5 Pour la règle d'ACL, saisissez les adresses IP des serveurs dans **Destination**, et précisez le protocole pour les serveurs. En règle générale, vous utilisez **any** pour la **Source**. Cliquez sur **Next** (Suivant) lorsque vous avez terminé.

Par exemple, si vous souhaitez protéger les serveurs Web 10.1.1.5 et 10.1.1.6, saisissez :

- Source = any
- Destination = 10.1.1.5, 10.1.1.6
- Destination Protocol (Protocole de destination) = tcp/http

Étape 6 Sur la page Rule Actions (Actions de règles), cliquez sur l'onglet **Paramètres de connexion** et complétez les options suivantes :

- **Embryonic Connections** (Connexions embryonnaires) : le nombre maximal de connexions TCP embryonnaires par hôte jusqu'à 2 000 000. La valeur par défaut est **0**, ce qui signifie que le nombre maximal de connexions embryonnaires est autorisé. Par exemple, vous pouvez la définir à 1 000.
- **Per Client Embryonic Connections** (Connexions embryonnaires par client) : le nombre maximal de connexions TCP embryonnaires simultanées pour chaque client jusqu'à 2 000 000. Lorsqu'une nouvelle connexion TCP est demandée par un client qui a déjà le nombre maximal de connexions embryonnaires par client ouvertes par l'intermédiaire de l'ASA, l'ASA empêche la connexion. Par exemple, vous pouvez la définir à 50.
- **TCP Syn Cookie MSS** (MSS des témoins SYN TCP) : la taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions embryonnaires lors de l'atteinte de la limite de connexions embryonnaires, de 48 à 65 535. La valeur par défaut est 1380. Ce paramètre n'a de sens que si vous configurez **Embryonic Connections** (Connexions embryonnaires) ou **Per Client Embryonic Connections** (Connexions embryonnaires par client).

Étape 7 Cliquez sur **Finish** (Terminer) pour enregistrer la règle et sur **Apply** (Appliquer) pour mettre à jour le périphérique.

Étape 8 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**, et activez au moins les statistiques **TCP Intercept** (Interception TCP) dans le groupe Threat Detection Statistics (Statistiques de détection des menaces).

Vous pouvez simplement activer toutes les statistiques ou simplement activer l'interception TCP. Vous pouvez également ajuster la fenêtre et les débits de surveillance.

Étape 9 Choisissez **Home (Accueil)** > **Firewall Dashboard (Tableau de bord du pare-feu)**, et consultez le tableau de bord **Top Ten Protected Servers under SYN Attack** (Dix principaux serveurs protégés faisant l'objet d'une attaque SYN) pour surveiller les résultats.

Cliquez sur le bouton **Detail** (Détails) pour afficher les données d'échantillonnage de l'historique. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

Vous pouvez effacer les statistiques en saisissant la commande **clear threat-detection statistics tcp-intercept** à l'aide de **Tools (Outils) > Command Line Interface (Interface de ligne de commande).**

Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP)

Le normaliseur TCP identifie les paquets anormaux sur lesquels l'ASA peut agir lorsqu'ils sont détectés; par exemple, l'ASA peut autoriser, abandonner ou effacer les paquets. La normalisation TCP contribue à protéger l'ASA contre les attaques. La normalisation TCP est toujours activée, mais vous pouvez personnaliser le comportement de certaines fonctionnalités.

Pour personnaliser le normaliseur TCP, définissez d'abord les paramètres à l'aide d'une liste TCP. Vous pouvez ensuite appliquer la liste aux classes de trafic sélectionnées à l'aide des politiques de service.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **TCP Maps (Listes TCP)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle liste TCP. Attribuez un nom à la liste.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Dans le champ **Queue Limit** (Limite de file d'attente), saisissez le nombre maximal de paquets hors ordre qui peuvent être mis en mémoire tampon et mis en ordre pour une connexion TCP, entre 0 et 250 paquets.

La valeur par défaut est 0, ce qui signifie que ce paramètre est désactivé et que la limite de file d'attente du système par défaut est utilisée en fonction du type de trafic :

- Les connexions pour l'inspection d'application et TCP check-retransmission ont une limite de file d'attente de 3 paquets. Si l'ASA reçoit un paquet TCP avec une taille de fenêtre différente, la limite de la file d'attente est modifiée dynamiquement pour correspondre au paramètre annoncé.
- Pour les autres connexions TCP, les paquets hors ordre sont transmis sans être modifiés.

Si vous définissez la limite de file d'attente à 1 ou au-dessus, le nombre de paquets désordonnés autorisés pour tout le trafic TCP correspond à ce paramètre. Par exemple, pour l'inspection d'application et le trafic TCP check-retransmission, tous les paramètres annoncés des paquets TCP sont ignorés au profit du paramètre

Queue Limit (Limite de file d'attente). Pour les autres trafics TCP, les paquets hors ordre sont maintenant mis en mémoire tampon et mis en ordre au lieu d'être transmis sans modification.

Étape 4 Dans le champ **Timeout** (Délai d'expiration), définissez la durée maximale pendant laquelle les paquets hors ordre peuvent rester dans la mémoire tampon, entre 1 et 20 secondes.

S'ils ne sont pas mis en ordre et transmis dans le délai d'expiration, ils sont abandonnés. La valeur par défaut est de 4 secondes. Vous ne pouvez pas modifier le délai d'expiration d'un trafic si la limite de file d'attente est définie à 0; vous devez définir la limite à 1 ou plus pour que le délai d'expiration prenne effet.

Étape 5 Pour **Reserved Bits** (Bits réservés), sélectionnez comment gérer les paquets qui ont des bits réservés dans l'en-tête TCP : **Clear and allow** (Effacer et autoriser) (supprimer les bits avant d'autoriser le paquet), **Allow only (Autoriser uniquement**) (ne pas modifier les bits, la valeur par défaut) ou **Drop the packet** (Abandonner le paquet).

Étape 6 Sélectionnez l'une des options suivantes :

- **Clear urgent flag** (Effacer l'indicateur urgent) : efface l'indicateur URG dans un paquet avant de l'autoriser. L'indicateur URG est utilisé pour indiquer que le paquet contient des informations de priorité plus élevée que les autres données du flux. Le RFC de TCP est vague sur l'interprétation exacte de l'indicateur URG, donc les systèmes finaux gèrent les décalages urgents de différentes manières, ce qui peut rendre le système final vulnérable aux attaques.
- **Drop connection on window variation** (Abandonner la connexion en cas de variation de fenêtre) : abandonne une connexion dont la taille de fenêtre a été modifiée de manière inattendue. Le mécanisme de taille de fenêtre permet à TCP d'annoncer une grande fenêtre et d'annoncer ultérieurement une fenêtre beaucoup plus petite sans avoir accepté trop de données. À partir de la spécification TCP, la « réduction de la fenêtre » est fortement déconseillée.
- **Drop packets that exceed maximum segment size** (Abandonner les paquets qui dépassent la taille maximale de segment) : abandonne les paquets qui dépassent le MSS défini par l'homologue.
- **Check if transmitted data is the same as original** (Vérifier si les données transmises sont identiques aux données d'origine) : active les vérifications des données de retransmission, qui empêchent les retransmissions TCP incohérentes.
- **Drop packets which have past-window sequence** (Abandonner les paquets dont la séquence est au-delà de la fenêtre) : abandonne les paquets qui ont des numéros de séquence au-delà de la fenêtre, c'est-à-dire que le numéro de séquence d'un paquet TCP reçu est supérieur au bord droit de la fenêtre de réception TCP. Pour autoriser ces paquets, désélectionnez cette option et définissez **Queue Limit** (Limite de file d'attente) à 0 (désactivation de la limite de file d'attente).
- **Drop SYN Packets with data** (Abandonner les paquets SYN avec données) : abandonne les paquets SYN qui contiennent des données.
- **Enable TTL Evasion Protection** (Activer la protection contre l'évitement TTL) : la TTL maximale pour une connexion est déterminée par la TTL dans le paquet initial La TTL des paquets suivants peut diminuer, mais elle ne peut pas augmenter. Le système réinitialisera la TTL au plus bas TTL vu précédemment pour cette connexion. Cela empêche les attaques d'évitement TTL.

  Par exemple, un agresseur peut envoyer un paquet qui passe la politique avec un TTL très court. Lorsque le TTL passe à zéro, un routeur entre l'ASA et le terminal abandonne le paquet. C'est à ce stade que l'agresseur peut envoyer un paquet malveillant avec un TTL long qui apparaît à l'ASA comme une retransmission et qui est transmis. Pour l'hôte du terminal, cependant, il s'agit du premier paquet reçu par l'agresseur. Dans ce cas, un agresseur peut réussir sans que la sécurité empêche l'attaque.

- **Verify TCP Checksum** (Vérifier la somme de contrôle TCP) : vérifie la somme de contrôle TCP, en abandonnant les paquets qui échouent à la vérification.
- **Drop SYNACK Packets with data** (Abandonner les paquets SYNACK avec données) : abandonne les paquets TCP SYNACK qui contiennent des données.
- **Drop packets with invalid ACK** (Abandonner les paquets avec un ACK non valide) : abandonne les paquets avec un ACK non valide. Vous pourriez voir des adresses ACK non valides dans les instances suivantes :
  - Dans l'état de la réception SYN-ACK de la connexion TCP, si le numéro ACK d'un paquet TCP reçu n'est pas exactement identique au numéro de séquence du paquet TCP suivant, il s'agit d'un ACK non valide.
  - Chaque fois que le numéro d'accusé de réception d'un paquet TCP reçu est supérieur au numéro de séquence du prochain paquet TCP envoyé, il s'agit d'un ACK non valide.

Remarque
Les paquets TCP avec un ACK non valide sont automatiquement autorisés pour les connexions WAAS.

Étape 7 (Facultatif) Cliquez sur l'onglet **TCP Options** (Options TCP) et définissez l'action pour les paquets qui contiennent des options TCP.

Vous pouvez effacer les options avant d'autoriser les paquets, autoriser les paquets s'ils contiennent une seule option d'un type donné ou autoriser les paquets même s'ils ont plusieurs options d'un type donné. La valeur par défaut est d'autoriser les cinq options nommées tant qu'une option donnée ne s'affiche pas plus d'une fois par paquet (sinon le paquet est abandonné), tout en effaçant toutes les autres options. Vous pouvez également abandonner les paquets contenant l'option MD5 ou l'une des options numérotées. Notez que si une connexion TCP est inspectée, toutes les options sont effacées, à l'exception des options MSS et d'accusé de réception sélectif (SACK), quelle que soit votre configuration.

a) Sélectionnez l'action pour les options **d'accusé de réception sélectif**, **d'horodatage TCP** et **d'échelle de fenêtre**.

L'effacement de l'option d'horodatage désactive PAWS et RTT.

b) Sélectionnez l'action pour l'option **MSS** (Taille maximale du segment).

En plus des actions normales Allow (Autoriser), Allow multiple (Autoriser plusieurs) et Clear (Effacer), vous pouvez sélectionner **Specify Maximum** (Préciser la valeur maximale) et saisir la taille maximale de segment, de 68 à 65 535. Le MSS TCP par défaut est défini sur la page **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **TCP Options (Options TCP)** .

c) Choisissez si vous souhaitez définir l'option **Allow packets with the MD5 option** (Autoriser les paquets avec l'option MD5).

Si vous décochez la case, les paquets qui contiennent l'option MD5 sont abandonnés. Si vous sélectionnez l'option, vous pouvez appliquer les actions normales d'autoriser, autoriser plusieurs ou effacer.

d) Sélectionnez l'action pour les options par plage de numéros.

Les options numérotées 6 à 7, 9 à 18 et 20 à 255 sont effacées par défaut. Vous pouvez plutôt autoriser les options ou abandonner les paquets qui contiennent l'option. Vous pouvez spécifier différentes actions pour différentes plages d'options : saisissez simplement le nombre inférieur et supérieur pour la plage, sélectionnez l'action et cliquez sur **Add** (Ajouter). Pour configurer une action pour une seule option, saisissez le même nombre pour les plages inférieure et supérieure.

Pour supprimer une plage configurée, sélectionnez-la et cliquez sur **Delete** (Supprimer).

Étape 8 Cliquez sur **OK** puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser la liste TCP dans une politique de service. La liste affecte le trafic uniquement lorsqu'elle est appliquée par le biais d'une politique de service.

Étape 9 Appliquez la liste TCP à une classe de trafic à l'aide d'une politique de service.

a) Choisissez **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)**.
b) Ajoutez ou modifiez une règle. Vous pouvez appliquer la règle globalement ou à une interface. Par exemple, pour personnaliser le traitement aberrant de paquets pour tout le trafic, créez une règle globale qui correspond à tout trafic. Passez à la page Rule Actions (Actions de règle).
c) Cliquez sur l'onglet **Connection Settings** (Paramètres de connexion).
d) Choisissez **Use TCP Map** (Utiliser la liste TCP) et sélectionnez la liste que vous avez créée.
e) Cliquez sur **Finish** (Terminer) ou **OK** (OK), puis sur **Apply** (Appliquer).

Contourner les vérifications de l'état TCP pour le routage asymétrique (TCP State Bypass)

Si vous disposez d'un environnement de routage asymétrique dans votre réseau, où le flux sortant et le flux entrant pour une connexion donnée peuvent passer par deux périphériques ASA différents, vous devez mettre en œuvre le contournement de l'état TCP sur le trafic concerné.

Cependant, le contournement de l'état TCP diminue la sécurité de votre réseau, vous devez donc appliquer le contournement sur les classes de trafic très spécifiques et limitées.

Les rubriques suivantes expliquent la problématique et sa solution plus en détail.

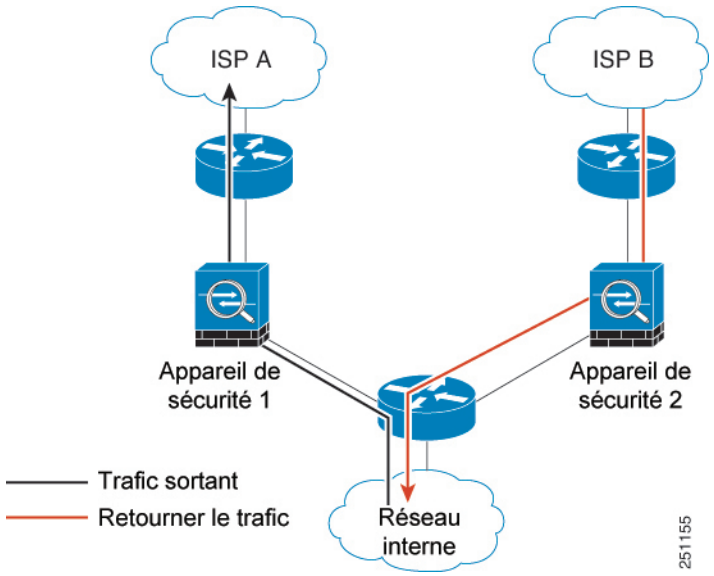
Le problème du routage asymétrique

Par défaut, tout le trafic qui passe par ASA est inspecté à l'aide de l'algorithme de sécurité adaptatif et est soit autorisé, soit abandonné en fonction de la politique de sécurité. ASA optimise la performance du pare-feu en vérifiant l'état de chaque paquet (nouvelle connexion ou connexion établie) et l'affecte au chemin de gestion de session (un nouveau paquet SYN de connexion), au chemin rapide (une connexion établie) ou au chemin de contrôle trajectoire du plan (inspection avancée).

Les paquets TCP qui correspondent à des connexions existantes sur le chemin rapide peuvent passer par l'ASA sans vérifier de nouveau tous les aspects de la politique de sécurité. Cette fonctionnalité maximise les performances. Cependant, la méthode d'établissement de la session dans le chemin rapide à l'aide du paquet SYN et les vérifications qui se produisent dans le chemin rapide (comme le numéro de séquence TCP) peuvent faire obstacle aux solutions de routage dissymétrique : les flux sortant et entrant d'une connexion doit passer par le même périphérique ASA.

Par exemple, une nouvelle connexion est dirigée vers le périphérique de sécurité 1. Le paquet SYN passe par le chemin de gestion de session et une entrée pour la connexion est ajoutée au tableau du chemin rapide. Si les paquets suivants de cette connexion passent par le périphérique de sécurité 1, les paquets correspondent à l'entrée du chemin rapide et sont transmis. Mais si les paquets suivants sont acheminés au périphérique de sécurité 2, où aucun paquet SYN n'a été soumis par le chemin de gestion de session, il n'y a pas d'entrée dans le chemin rapide pour la connexion et les paquets sont abandonnés. La figure suivante montre un exemple de routage symétrique dans lequel le trafic sortant passe par un ASA différent du trafic entrant :

Illustration 1 : Routage asymétrique



Si le routage asymétrique est configuré sur les routeurs en amont et que le trafic alterne entre deux périphériques ASA, vous pouvez configurer le contournement de l'état TCP pour un trafic spécifique. Le contournement de l'état TCP modifie la façon dont les sessions sont établies dans le chemin rapide et désactive les vérifications du chemin rapide. Cette fonctionnalité traite le trafic TCP de la même manière qu'elle traite une connexion UDP : lorsqu'un paquet non SYN correspondant aux réseaux spécifiés entre dans le périphérique ASA, et qu'il n'y a pas d'entrée de chemin rapide, le paquet passe par le chemin de gestion de session pour établir le connexion sur le chemin rapide. Une fois dans le chemin rapide, le trafic contourne les vérifications du chemin rapide.

Lignes directrices et limites du contournement d'état TCP

Fonctionnalités non prises en charge du contournement de l'état TCP

Les fonctionnalités suivantes ne sont pas prises en charge lorsque vous utilisez le contournement de l'état TCP :

- Inspection d'application : l'inspection nécessite que le trafic entrant et sortant passe par le même ASA, donc l'inspection n'est pas appliquée au trafic de contournement d'état TCP.
- Sessions authentifiées par AAA : lorsqu'un utilisateur s'authentifie auprès d'un ASA, le trafic revenant par l'autre ASA sera refusé, car l'utilisateur ne s'est pas authentifié auprès de cet ASA.
- Interception TCP, limite maximale de connexions explorées, répartition aléatoire des numéros de séquence TCP : l'ASA ne fait pas le suivi de l'état de la connexion, donc ces fonctionnalités ne sont pas appliquées.
- Normalisation TCP : le normalisateur TCP est désactivé.

Lignes directrices relatives à la NAT pour le contournement d'état TCP

Comme la session de traduction est établie séparément pour chaque périphérique, veillez à configurer la NAT statique sur les deux périphériques pour le trafic de contournement d'état TCP. Si vous utilisez la NAT

dynamique, l'adresse choisie pour la session sur le périphérique 1 sera différente de celle choisie pour la session sur le périphérique 2.

Configurer le contournement d'état TCP

Pour contourner la vérification de l'état TCP dans des environnements de routage symétrique, définissez avec soin une classe de trafic qui s'applique aux hôtes ou aux réseaux concernés uniquement, puis activez le contournement de l'état TCP sur la classe de trafic à l'aide d'une politique de service. Étant donné que le contournement réduit la sécurité du réseau, limitez son application autant que possible.

Avant de commencer

S'il n'y a aucun trafic sur une connexion donnée pendant 2 minutes, la connexion expire. Vous pouvez remplacer cette valeur par défaut en modifiant le **délai d'inactivité** pour la classe de trafic de contournement de l'état TCP. Les connexions TCP normales expirent par défaut après 60 minutes.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)**.

Étape 2 Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour les hôtes, modifiez-la.

Étape 3 Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).

Étape 4 Pour Traffic Classification (Classification du trafic), sélectionnez **Source and Destination IP Addresses (uses ACL)** (Adresses IP source et de destination [utilise l'ACL]) et cliquez sur **Next** (Suivant).

Étape 5 Pour la règle d'ACL, saisissez les adresses IP des hôtes à chaque extrémité de la route dans **Source** et **Destination**, et spécifiez le protocole TCP. Cliquez sur **Next** (Suivant) lorsque vous avez terminé.

Par exemple, si vous souhaitez contourner la vérification de l'état TCP entre 10.1.1.1 et 10.2.2.2, saisissez :

- Source = 10.1.1.1
- Destination = 10.2.2.2
- Protocole de destination = tcp

Étape 6 Dans la page Rule Actions (Actions de règle), cliquez sur l'onglet **Connection Settings** (Paramètres de connexion) et sélectionnez **TCP State Bypass** (Contournement de l'état TCP).

Étape 7 Cliquez sur **Finish** (Terminer) pour enregistrer la règle et **Apply** (Appliquer) pour mettre à jour le périphérique.

Désactiver la gestion aléatoire de la séquence TCP

Chaque connexion TCP a deux numéros de séquence initiaux (ISN) : un généré par le client et un généré par le serveur. L'ASA effectue la randomisation de l'ISN du SYN TCP dans les sens entrant et sortant.

La distribution aléatoire de l'ISN de l'hôte protégé empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session. Cependant, la répartition aléatoire

des séquences TCP rompt en pratique les SACK TCP (accusé de réception sélectif), car les numéros de séquence que voit le client sont différents de ce que le serveur voit.

Vous pouvez désactiver la répartition aléatoire des numéros de séquence initial TCP si nécessaire, par exemple, parce que les données sont brouillées. Par exemple :

- Si un autre pare-feu en ligne effectue également la répartition aléatoire des numéros de séquence initiaux, il n'est pas nécessaire que les deux pare-feu effectuent cette action, même si cette action n'affecte pas le trafic.
- Si vous utilisez le protocole eBGP multi-sauts via l'ASA et que les homologues eBGP utilisent le protocole MD5. La randomisation rompt la somme de contrôle MD5.
- Si vous utilisez un périphérique WAAS qui exige que l'ASA ne randomise pas les numéros de séquence des connexions.
- Si vous activez le contournement matériel pour l'ISA 3000, les connexions TCP sont abandonnées lorsque l'ISA 3000 ne fait plus partie du chemin de données.



Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)** .

Étape 2 Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour le trafic ciblé, modifiez-la.

Étape 3 Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).

Étape 4 Pour la classification du trafic, identifiez le type de correspondance de trafic. La correspondance de classe doit concerner le trafic TCP; vous pouvez identifier des hôtes spécifiques (avec une liste de contrôle d'accès), faire une correspondance de port TCP ou simplement faire correspondre n'importe quel trafic. Cliquez sur **Next** (Suivant) et configurez les hôtes dans la liste de contrôle d'accès ou définissez les ports, puis cliquez à nouveau sur **Next** (Suivant).

Par exemple, si vous souhaitez désactiver l'aléatoireisation du numéro de séquence TCP pour tout le trafic TCP dirigé vers l'adresse 10.2.2.2, saisissez :

- Source = any
- Destination = 10.2.2.2
- Protocole de destination = tcp

Étape 5 Sur la page Rule Actions (Actions de règles), cliquez sur l'onglet **Connection Settings (paramètres de connexion)** et décochez **la case de hasarder le numéro de séquence**.

Étape 6 Cliquez sur **Finish** (Terminer) pour enregistrer la règle et **Apply** (Appliquer) pour mettre à jour le périphérique.

Délester les flux volumineux

Si vous déployez l'ASA sur les périphériques pris en charge dans un centre de données, vous pouvez identifier le trafic sélectionné à décharger vers un chemin ultra-rapide, où le trafic est commuté dans la carte réseau elle-même. Le déchargement peut vous aider à améliorer les performances des applications exigeantes en données, telles que les transferts de fichiers volumineux.

- Les sites de recherche en informatique à haute performance (HPC), où l'ASA est déployé entre les stations de stockage et les stations d'informatique à haute performance. Lorsqu'un site de recherche effectue une sauvegarde à l'aide du transfert de fichiers FTP ou de la synchronisation de fichiers sur NFS, l'importance du trafic de données affecte tous les contextes sur l'ASA. Le déchargement du transfert de fichiers FTP et de la synchronisation des fichiers sur NFS réduit l'impact sur le reste du trafic.
- La négociation à haute fréquence (HFT), où l'ASA est déployé entre les postes de travail et l'Exchange, principalement à des fins de conformité. La sécurité n'est généralement pas un problème, mais la latence est une préoccupation majeure.

Avant d'être déchargé, l'ASA applique d'abord un traitement de sécurité normal, tel que les règles d'accès et l'inspection, lors de l'établissement de la connexion. L'ASA effectue également le démontage de la session. Mais une fois une connexion établie, si elle peut être déchargée, le traitement ultérieur se produit dans la carte réseau plutôt que dans l'ASA.

Les flux déchargés continuent de recevoir une inspection dynamique limitée, comme la vérification des indicateurs TCP de base et des options, et la vérification des sommes de contrôle si vous la configurez. Le système peut sélectivement transmettre les paquets au système de pare-feu pour un traitement plus approfondi si nécessaire.

Pour identifier les flux qui peuvent être déchargés, vous créez une règle de politique de service qui applique le service de déchargement de flux. Un flux correspondant est ensuite déchargé s'il répond aux conditions suivantes :

- Adresses IPv4 uniquement.
- TCP, UDP, GRE uniquement.
- Trames standard ou Ethernet balisées 802.1Q uniquement.
- (Mode transparent uniquement.) Le déchargement de multidiffusion est disponible pour les groupes de ponts qui contiennent deux et seulement deux interfaces.

Les flux inverses pour les flux déchargés sont également déchargés.

Limites de déchargement de flux

Tous les flux ne peuvent pas être déchargés. Même après le déchargement, il est possible de désactiver le déchargement d'un flux dans certaines conditions. Voici quelques-unes des limites :

Limites du périphérique

La fonctionnalité est prise en charge sur les périphériques suivants :

- Secure Firewall 3100 (statique uniquement)

- Firepower 4100/9300

Flux qui ne peuvent pas être déchargés

Les types de flux suivants ne peuvent pas être déchargés.

- Flux qui n'utilise pas l'adressage IPv4, comme l'adressage IPv6.
- Flux pour tout protocole autre que TCP, UDP et GRE.



Remarque Les connexions PPTP GRE ne peuvent pas être déchargées.

- Flux qui nécessitent une inspection. Dans certains cas, comme FTP, le canal de données secondaire peut être déchargé bien que le canal de contrôle ne puisse pas être déchargé.
- Connexions VPN IPsec et TLS/DTLS qui se terminent sur le périphérique.
- Flux de multidiffusion en mode routé.
- Flux de multidiffusion en mode transparent pour les groupes de ponts qui comportent trois interfaces ou plus.
- Flux d'interception TCP.
- Flux de contournement d'état TCP Vous ne pouvez pas configurer le déchargement de flux et le contournement de l'état TCP sur le même trafic.
- Flux mandataires AAA de type cut-through.
- Vpath, flux liés à VXLAN.
- Flux balisés avec les groupes de sécurité.
- Flux inverses qui sont transférés à partir d'un nœud de grappe différent, en cas de flux dissymétriques dans une grappe.
- Flux centralisés en grappe, si le propriétaire du flux n'est pas l'unité de contrôle.

Restrictions supplémentaires

- Le déchargement de flux et la détection de connexion inactive (DCD) ne sont pas compatibles. Ne configurez pas la DCD sur les connexions qui peuvent être déchargées.
- si plusieurs flux correspondant aux conditions de déchargement de flux sont mis en file d'attente pour être déchargés en même temps au même emplacement sur le matériel, seul le premier flux est déchargé. Les autres flux sont traités normalement. C'est ce qu'on appelle une *collision*. Utilisez la commande **show flow-offload flow** dans l'interface de ligne de commande pour afficher les statistiques de cette situation.
- Bien que les flux déchargés passent par les interfaces FXOS, les statistiques pour ces flux ne s'affichent pas sur l'interface de périphérique logique. Par conséquent, les compteurs d'interface de périphérique logique et les débits de paquets ne reflètent pas les flux déchargés.

Conditions d'inversion du déchargement

Après le déchargement d'un flux, les paquets qu'il contient sont renvoyés au système d'exploitation du pare-feu pour traitement ultérieur s'ils remplissent les conditions suivantes :

- Ils comprennent les options TCP autres que l'horodatage.
- Ils sont fragmentés.
- Ils sont soumis au routage à chemins multiples à coûts égaux (ECMP), et les paquets entrants sont déplacés d'une interface à une autre.
- Une modification de la table de routage s'applique au flux. Un paquet est renvoyé au périphérique pour déterminer la nouvelle route.

Configurer le déchargement de flux

Pour configurer le déchargement de flux, vous devez activer le service, puis créer des politiques de service pour identifier le trafic admissible au déchargement. Pour le Firepower 4100/9300 : lorsque vous activez le service pour la première fois, vous devez redémarrer. .

Procédure

Étape 1 Activez le service de déchargement de flux.

Pour le Firepower 4100/9300 : lorsque vous activez le service pour la première fois, vous devez redémarrer.

Si un redémarrage est requis, des considérations particulières s'appliquent aux grappes ou aux paires de basculement si vous souhaitez effectuer un changement sans interruption :

- Mise en grappe : saisissez d'abord la commande sur le nœud de contrôle, mais ne redémarrez pas le nœud de contrôle immédiatement. Au lieu de cela, redémarrez d'abord chaque nœud de la grappe, puis revenez au nœud de contrôle et redémarrez-le. Vous pouvez ensuite configurer la politique de service de déchargement sur le nœud de contrôle.
- Basculement : saisissez d'abord la commande sur l'unité active, sans la redémarrer immédiatement. Au lieu de cela, redémarrez l'unité en veille, puis redémarrez l'unité active. Vous pouvez ensuite configurer la politique de service de déchargement sur l'unité active.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Offload Engine (Moteur de déchargement)**.
b) Cochez **Enable Offload Engine** (Activer le moteur de déchargement).
c) Cliquez sur **Apply**.
d) Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications dans la configuration de démarrage.
e) (Firepower 4100/9300) Sélectionnez **Tools (Outils)** > **System Reload** (Redémarrage du système) pour redémarrer le périphérique.

Étape 2 Créez la règle de politique de service qui identifie le trafic admissible au déchargement.

a) Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)**.
b) Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour les hôtes, modifiez-la.

c) Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).
d) Pour Traffic Classification (Classification du trafic), la mise en correspondance par liste d'accès (**Source and Destination IP Addresses (uses ACL) (Adresses IP source et de destination (utilise une ACL**))) ou par port (**TCP or UDP or SCTP Destination Port**) constitue généralement les options les plus courantes. Sélectionnez une option et cliquez sur **Next** (Suivant).
e) Saisissez les critères d'ACL ou de port. Cliquez sur **Next** (Suivant) lorsque vous avez terminé.

   Par exemple, si vous souhaitez rendre tout le trafic TCP sur le sous-réseau 10.1.1.0/255.255.255.224 admissible au déchargement, saisissez :

   - Source = 10.1.1.0/255.255.255.224 (ou 10.1.1.0/27)
   - Destination = any
   - Protocole de destination = tcp

f) Sur la page Rule Actions (actions de règles), cliquez sur l'onglet **Connection Settings (paramètres de connexion)** et sélectionnez **Flow Offload (déchargement de flux)**.
g) Cliquez sur **Finish** (Terminer) pour enregistrer la règle et sur **Apply** (Appliquer) pour mettre à jour le périphérique.

Décharge de flux IPsec

Vous pouvez configurer des modèles de périphérique de prise en charge pour utiliser le déchargement de flux IPsec. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique.

Les opérations déchargées sont spécifiquement liées au traitement de pré déchiffrement et de déchiffrement à l'entrée, et au traitement de pré chiffrement et de chiffrement à la sortie. Le logiciel système gère le flux interne pour appliquer vos politiques de sécurité.

Le déchargement de flux IPsec est activé par défaut et s'applique aux types de périphériques suivants :

- Secure Firewall 3100

Limites du déchargement de flux IPsec

Les flux IPsec suivants ne sont pas déchargés :

- Tunnels IKEv1. Seuls les tunnels IKEv2 seront déchargés. IKEv2 prend en charge les chiffrements plus forts.
- Flux pour lesquels une régénération basée sur le volume est configurée.
- Flux pour lesquels la compression est configurée.
- Flux des modes de transport. Seuls les flux en mode tunnel seront déchargés.
- Format AH. Seul le format ESP/NAT-T sera pris en charge.
- Les flux dont la post-fragmentation est configurée.

- Flux qui ont une taille de fenêtre d'anti-relecture autre que 64 bits et l'anti-relecture n'est pas désactivé.
- Les flux pour lesquels le filtre de pare-feu est activé.
- Mode à contextes multiples.

Configurer le déchargement de flux IPsec

Le déchargement de flux IPSec est activé par défaut sur les plateformes matérielles qui prennent en charge la fonctionnalité. Cependant, l'optimisation de sortie n'est pas activée par défaut, vous devez donc la configurer si vous souhaitez cette fonctionnalité.

Avant de commencer

Le déchargement de flux IPsec est configuré globalement. Vous ne pouvez pas le configurer pour les flux de trafic sélectionnés.

Utilisez la forme **no** de ces commandes pour désactiver les fonctionnalités.

Pour voir l'état actuel de la configuration, utilisez la commande **show flow-offload ipsec info**.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **IPsec Offload (Déchargement IPsec)**.

Étape 2 Sélectionnez **IPsec Offload** (Déchargement IPsec) pour activer le déchargement de flux IPsec.

Étape 3 Sélectionnez **Egress Optimization For IPSec Offload** (Optimisation de sortie pour le déchargement IPsec) pour optimiser le chemin d'accès aux données afin d'améliorer les performances pour les flux de tunnel unique.

La configuration pour l'optimisation de sortie est distincte du déchargement de flux. Cependant, même si elle est activée, elle n'a d'incidence que si vous activez également le déchargement de flux IPsec.

Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services)

Vous pouvez configurer différents paramètres de connexion pour des classes de trafic spécifiques à l'aide des politiques de service. Utilisez les politiques de service pour :

- Personnalisez les limites de connexion et les délais d'expiration utilisés pour la protection contre les attaques DoS et SYN-flooding.
- Implémentez la détection de connexion inactive pour que les connexions valides, mais inactives, restent actives.
- Désactivez l'aléatoirisation du numéro de séquence TCP dans les cas où vous n'en avez pas besoin.
- Personnalisez la manière dont le normalisateur TCP protège contre les paquets TCP anormaux.

- Implémentez le contournement de l'état TCP pour le trafic soumis à un routage asymétrique. Le trafic de contournement n'est pas soumis à l'inspection.
- Implémentez le contournement de l'état SCTP (Stream Control Transmission Protocol) pour désactiver l'inspection dynamique SCTP.
- Mettez en œuvre le déchargement de flux pour améliorer les performances sur les plateformes matérielles prises en charge.
- Décrémentez la durée de vie (TTL) des paquets afin que l'ASA s'affiche dans la sortie traceroute.

Remarque Si vous décrémentez la durée de vie, les paquets avec une TTL de 1 seront abandonnés, mais une connexion sera ouverte pour la session en supposant que la connexion pourrait contenir des paquets avec une TTL plus élevée. Notez que certains paquets, comme les paquets hello d'OSPF, sont envoyés avec TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues pour les appareils ASA en mode transparent. Les paramètres de décrément de la durée de vie n'ont pas d'incidence sur le processus OSPF lorsque l'ASA fonctionne en mode routé.

Vous pouvez configurer n'importe quelle combinaison de ces paramètres pour une classe de trafic donnée, à l'exception du contournement de l'état TCP et de la personnalisation du normaliseur TCP, qui s'excluent mutuellement.

Astuces Cette procédure montre une politique de service pour le trafic qui passe par l'ASA. Vous pouvez également configurer la connexion maximale et la connexion embryonnaire maximale pour le trafic de gestion (vers le périphérique).

Avant de commencer

Si vous souhaitez personnaliser le normalisateur TCP, créez la liste TCP requise avant de continuer.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter) > Add Service Policy Rule (Ajouter une règle de politique de service)**. Passez par l'assistant jusqu'à la page Règles.
- Si vous avez une règle pour laquelle vous modifiez les paramètres de connexion, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 2 Sur la page ou l'onglet Rule Actions (Actions de règles) de l'assistant, sélectionnez l'onglet **Connection Settings** (Paramètres de connexion).

Étape 3 Pour définir le nombre maximal de connexions, configurez les valeurs suivantes dans la zone Maximum Connections (Nombre maximal de connexions) :

Par défaut, il n'y a aucune limite à la connexion. Si vous mettez en œuvre des limites, le système doit commencer à les suivre, ce qui peut augmenter l'utilisation du processeur et de la mémoire et entraîner des problèmes opérationnels pour les systèmes soumis à une charge élevée, en particulier dans une grappe.

- **Maximum TCP, UDP and SCTP Connections**—(TCP, UDP, SCTP.) Le nombre maximal de connexions simultanées pour tous les clients dans la classe de trafic, jusqu'à 2 000 000. La valeur par défaut est 0, ce qui signifie que le nombre maximal de connexions possibles est autorisé. Pour les connexions TCP, ce nombre s'applique aux connexions établies uniquement.
- **Embryonic Connections** (Connexions embryonnaires) : spécifie le nombre maximal de connexions TCP embryonnaires par hôte jusqu'à 2 000 000. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination. La valeur par défaut est **0**, ce qui signifie que le nombre maximal de connexions embryonnaires est autorisé. En définissant une limite non nulle, vous activez l'interception de TCP, qui protège les systèmes internes contre les attaques DoS perpétrées en inondant une interface de paquets SYN du protocole TCP. Définissez également les options par client pour vous protéger contre l'inondation SYN.
- **Per Client Connections (Connexions par client)** — (TCP, UDP, SCTP.) Spécifie le nombre maximal de connexions simultanées pour chaque client jusqu'à 2 000 000. Lorsqu'une nouvelle connexion est tentée par un client qui a déjà ouvert le nombre maximal de connexions par client, l'ASA rejette la connexion et abandonne le paquet. Pour les connexions TCP, cela inclut les connexions établies, à moitié ouvertes et à moitié fermées.
- **Per Client Embryonic Connections** (Connexions embryonnaires par client) — Spécifie le nombre maximal de connexions TCP embryonnaires simultanées pour chaque client jusqu'à 2 000 000. Lorsqu'une nouvelle connexion TCP est demandée par un client qui a déjà le nombre maximal de connexions embryonnaires par client ouvertes par l'intermédiaire de l'ASA, l'ASA empêche la connexion.
- **TCP Syn Cookie MSS** (MSS des témoins SYN TCP) — La taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions embryonnaires lors de l'atteinte de la limite de connexions embryonnaires, de 48 à 65 535. La valeur par défaut est 1380. Ce paramètre n'a de sens que si vous configurez **Embryonic Connections** ou **Per Client Embryonic Connections**.

Étape 4 Pour configurer les délais d'expiration de connexion, configurez les valeurs suivantes dans la zone TCP Timeout (Délai d'expiration TCP) :

- **Embryonic Connection Timeout** (Délai d'expiration de la connexion embryonnaire) — Le temps d'inactivité jusqu'à ce qu'un logement de connexion TCP embryonnaire (à moitié ouvert) soit libéré. Saisissez 0:0:0 pour désactiver le délai d'expiration pour la connexion. La valeur par défaut est de 30 secondes.
- **Half Closed Connection Timeout** (Délai d'expiration de la connexion à moitié fermée) —Le délai d'inactivité jusqu'à la fermeture d'une connexion à moitié fermée, entre 0:5:0 (pour 9.1(1) et antérieur) ou 0:0:30 (pour 9.1(2) et ultérieur) et 1 193:0:0. La valeur par défaut est 0:10:0. Les connexions à moitié fermées ne sont pas affectées par la détection des connexions inactives (DCD). De plus, l'ASA n'envoie pas de réinitialisation lorsqu'il interrompt les connexions à moitié fermées.
- **Idle Connection Timeout (Délai d'inactivité de la connexion)** — Le délai d'inactivité jusqu'à ce qu'un logement de connexion (de *n'importe quel* protocole, pas seulement TCP) soit libéré. Saisissez 0:0:0 pour désactiver le délai d'expiration pour la connexion. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 1 heure.

- **Send reset to TCP endpoints before timeout** (Envoyer une réinitialisation aux terminaux TCP avant l'expiration) — Indique si l'ASA doit envoyer un message de réinitialisation TCP aux terminaux de la connexion avant de libérer le logement de connexion.
- **Dead Connection Detection (DCD)** (Détection des connexions inactives [DCD]) — Indique s'il faut activer Dead Connection Detection (DCD). Avant de faire expirer une connexion inactive, l'ASA sonde les hôtes finaux pour déterminer si la connexion est valide. Si les deux hôtes répondent, la connexion est conservée, sinon la connexion est libérée. Définissez le nombre maximal de tentatives (par défaut est 5, la plage est comprise entre 1 et 255) et l'intervalle de nouvelle tentative, qui est la période d'attente après chaque sonde DCD sans réponse avant d'envoyer une autre sonde (0:0:1 à 24:0:0, la valeur par défaut est 0:0:15). Lorsque vous utilisez le mode transparent du pare-feu, vous devez configurer des routes statiques pour les points terminaux. Vous ne pouvez pas configurer le DCD sur les connexions qui sont également déchargées, alors assurez-vous que le DCD et les classes de trafic de déchargement de flux ne se chevauchent pas.Utilisez la commande **show conn detail** pour suivre le nombre de sondes DCD envoyées par l'initiateur et le répondeur.

  Pour les systèmes qui fonctionnent dans une configuration de grappe ou haute disponibilité, nous vous recommandons de ne pas définir l'intervalle à moins d'une minute (0:1:0). Si la connexion doit être déplacée entre les systèmes, les modifications requises prennent plus de 30 secondes et la connexion peut être supprimée avant que la modification ne soit effectuée.

Étape 5 Pour désactiver les numéros de séquence aléatoires, décochez **Randomize Sequence Number** (Rendre le numéro de séquence aléatoire).

La distribution aléatoire de l'ISN de l'hôte protégé empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session.

Étape 6 Pour personnaliser le comportement du normaliseur TCP, cochez **Use TCP Map** (Utiliser une liste TCP) et choisissez une liste TCP existante dans la liste déroulante (le cas échéant), ou ajoutez-en une nouvelle en cliquant sur **New** (Nouveau).

Étape 7 Pour décrémenter le délai de vie (TTL) des paquets qui correspondent à la classe, cochez **Decrement time to live for a connection** (Décrémenter le temps de vie d'une connexion).

Le décrément de TTL est nécessaire pour que l'ASA s'affiche dans les routes de trace en tant que l'un des sauts. Vous devez également augmenter la limite de débit pour les messages ICMP Unreachable sur **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès à la gestion) > ICMP**.

Étape 8 Pour activer le contournement de l'état TCP, cochez **TCP State Bypass** (Contournement de l'état TCP).

Étape 9 Pour activer le contournement de l'état SCTP, cochez **SCTP State Bypass** (Contournement de l'état SCTP).

Implémentez le contournement de l'état SCTP pour désactiver l'inspection dynamique SCTP. Pour en savoir plus, consultez Inspection dynamique SCTP.

Étape 10 (ASA sur le Châssis Firepower 4100/9300 , FXOS 1.1.3 ou version ultérieure, uniquement.) Pour activer le déchargement de flux, cochez **Flow Offload** (Déchargement de flux).

Le trafic éligible est déchargé vers un chemin ultra-rapide, où les flux sont commutés dans la carte réseau elle-même. Vous devez également activer le service de déchargement. Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Offload Engine (Moteur de déchargement)**.

Étape 11 Cliquez sur **OK** ou **Finish** (Terminer).

Configurer les options TCP

Vous pouvez configurer des options pour contrôler certains aspects du comportement TCP. Les paramètres par défaut pour ces réglages sont appropriés pour la plupart des réseaux.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced** > **TCP Options** > **(Options TCP avancées)**.

Étape 2 Configurez le comportement de réinitialisation TCP par interface.

a) Sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

b) Sélectionnez les options souhaitées :

- **Send reset reply for denied inbound TCP packets** (Envoyer une réponse de réinitialisation pour les paquets TCP entrants refusés). Envoyez des réinitialisations TCP pour toutes les sessions TCP entrantes qui tentent de transiter par l'ASA et sont refusées par l'ASA en fonction des listes d'accès ou des paramètres AAA. L'ASA envoie également des réinitialisations pour les paquets qui sont autorisés par une liste d'accès ou AAA, mais qui n'appartiennent pas à une connexion existante et sont refusés par le pare-feu dynamique. Le trafic entre les interfaces de même niveau de sécurité est également affecté. Lorsque cette option n'est pas activée, l'ASA rejette silencieusement les paquets refusés.

c) Cliquez sur **OK**.

Étape 3 Configurez les autres options TCP :

- **Send reset reply for denied outside TCP packets** (Envoyer une réponse de réinitialisation pour les paquets TCP externes refusés). Envoie des réinitialisations pour les paquets TCP qui se terminent à l'interface la moins sécurisée et qui sont refusés par l'ASA en fonction des listes d'accès ou des paramètres AAA. L'ASA envoie également des réinitialisations pour les paquets qui sont autorisés par une liste d'accès ou AAA, mais qui n'appartiennent pas à une connexion existante et qui sont refusés par le pare-feu dynamique. Lorsque cette option n'est pas activée, l'ASA rejette silencieusement les paquets des connexions refusées.

  Nous vous recommandons d'utiliser cette option avec l'interface PAT. Cela permet à l'ASA de terminer les connexions IDENT provenant d'un serveur SMTP ou FTP externe. La réinitialisation active de ces connexions évite le délai d'expiration de 30 secondes.

- **Force maximum segment size for TCP connection to be X bytes** (Forcer la taille de segment maximale de la connexion TCP à X octets). Définissez la taille de segment TCP maximale en octets, entre 48 et tout nombre maximal : Par défaut, la MTU est de 1380 octets. Vous pouvez désactiver cette fonctionnalité en mettant les octets à 0.

- **Force minimum segment size for TCP connection to be X bytes** (Forcer la taille de segment minimale de la connexion TCP à X octets). Remplace la taille maximale du segment pour qu'elle ne soit pas inférieure au nombre d'octets spécifié, entre 48 et 65 535 octets. Cette fonctionnalité est désactivée par défaut (définie sur 0).

- **Force TCP connection to linger in TIME_WAIT state for at least 15 seconds after TCP close-down** (Forcer la connexion TCP à persister dans l'état TIME_WAIT pendant au moins 15 secondes après la fermeture du TCP). Force chaque connexion TCP à persister dans un état TIME_WAIT raccourci d'au moins 15 secondes après la dernière séquence de fermeture TCP normale. Vous pouvez utiliser cette

fonctionnalité si une séquence de fin TCP par défaut de l'application d'hôte terminal est une fermeture simultanée.

- **TCP Maximum unprocessed segments (Nombre maximal de segments TCP non traités).** Vous pouvez définir le nombre maximal de segments TCP non traités, de 6 à 24. La valeur par défaut est 6. Si vous constatez que les téléphones SIP ne se connectent pas au gestionnaire d'appels, vous pouvez essayer d'augmenter le nombre maximal de segments TCP non traités.

Étape 4 Cliquez sur **Apply** (Appliquer).

Supervision des connexions

Utilisez les pages suivantes pour surveiller les connexions :

- Utilisez **Home (Accueil)** > **Firewall Dashboard** > **(Tableau de bord Pare-feu)**, puis consultez **Top Ten Protected Servers (Dix principaux serveurs protégés) dans le tableau de bord SYN Attack (Attaque SYN)** pour surveiller TCP Intercept. Cliquez sur le bouton **Detail** (Détails) pour afficher les données d'échantillonnage de l'historique. Le système ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.
- Utilisez **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Connections (Connexions)** pour afficher les connexions actuelles.
- Utilisez **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Connection Graphs (Graphiques de connexion)** pour surveiller les performances.

De plus, vous pouvez saisir les commandes suivantes à l'aide de **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

- **show conn** [**detail**]

  Affiches des renseignements sur la connexion. Les informations détaillées utilisent des indicateurs pour indiquer des caractéristiques de connexion spéciales. Par exemple, l'indicateur « b » désigne un trafic soumis au contournement d'état TCP.

  Lorsque vous utilisez le mot-clé **detail**, vous pouvez voir des informations sur la sonde de détection de connexion inactive (DCD), qui indiquent la fréquence à laquelle la connexion a été sondée par l'initiateur et le répondeur. Par exemple, les détails d'une connexion compatible avec DCD ressembleraient à ce qui suit :

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show flow-offload** {**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

Affiche des renseignements sur le déchargement de flux, notamment l'état général, l'utilisation du processeur pour le déchargement, le nombre et les détails des flux déchargés, ainsi que les statistiques des flux déchargés.

- **show service-policy**

  Affiche les statistiques de politique de service, y compris les statistiques de détection de connexion inactive (DCD).

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  Affichez les 10 principaux serveurs protégés et soumis à des attaques. Le mot-clé **all** affiche les données d'historique de tous les serveurs suivis. Le mot-clé **detail** affiche les données d'échantillonnage de l'historique. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.



Remarque Dans la configuration de l'ASA, les connexions embryonnaires (demandes de connexion qui n'ont pas encore terminé le processus de négociation en trois temps) sont fermées rapidement et ne sont pas synchronisées entre les périphériques actif et en veille. Cette conception garantit l'efficacité et la sécurité du système à haute disponibilité. Pour cette raison, une différence dans le nombre de connexions entre les deux ASA est normale.

Historique des paramètres de connexion

Nom de la caractéristique	Versions de plateforme	Description
contournement de l'état du TCP	8.2(1)	Cette fonctionnalité a été introduite. La commande suivante a été introduite : **set connection advanced-options tcp-state-bypass**.
Délai d'expiration de connexion pour tous les protocoles	8.2(2)	Le délai d'inactivité a été modifié pour s'appliquer à tous les protocoles, pas seulement au TCP. L'écran suivant a été modifié : Configuration > Firewall (Pare-feu) > Service Policies (Politiques de service) > Rule Actions (Actions de règle) > Connection Settings (Paramètres de connexion).
Délai d'expiration pour les connexions utilisant une route statique de sauvegarde	8.2(5)/8.4(2)	Lorsqu'il existe plusieurs routes statiques vers un réseau avec différentes métriques, l'ASA utilise celle ayant la meilleure métrique au moment de la création de la connexion. Si un meilleur routage devient disponible, ce délai d'expiration permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser le meilleur routage. La valeur par défaut est 0 (la connexion n'expire jamais). Pour profiter de cette fonctionnalité, modifiez le délai d'expiration pour une nouvelle valeur. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux).

Nom de la caractéristique	Versions de plateforme	Description
Délai d'expiration configurable pour PAT xlate	8.4(3)	Lorsqu'un PAT xlate expire (par défaut après 30 secondes) et que l'ASA réutilise le port pour une nouvelle traduction, certains routeurs en amont peuvent rejeter la nouvelle connexion, car la connexion précédente peut toujours être ouverte sur le périphérique en amont. Le délai d'expiration de PAT xlate est maintenant configurable, à une valeur comprise entre 30 secondes et 5 minutes. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux). *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*
Augmentation des limites de connexion maximales pour les règles de politique de service	9.0(1)	Le nombre maximal de connexions pour les règles de politique de service a été augmenté de 65 535 à 2 000 000. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Connection Settings (Paramètres de connexion).
Réduction de la valeur minimale du délai d'expiration à moitié fermé à 30 secondes	9.1(2)	La valeur minimale du délai d'expiration à moitié fermé pour le délai d'expiration global et le délai d'expiration de connexion a été réduite de 5 minutes à 30 secondes pour fournir une meilleure protection DoS. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Connection Settings (Paramètres de connexion); Configuration (Configuration) > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux).
Délai d'expiration de la connexion pour la convergence des routes.	9.4(3) 9.6(2)	Vous pouvez maintenant configurer la durée pendant laquelle le système doit maintenir une connexion lorsque le routage utilisé par la connexion n'existe plus ou est inactif. Si le routage ne devient pas actif au cours de cette période d'attente, la connexion est libérée. Vous pouvez réduire le délai de maintien pour accélérer la convergence des routes. Cependant, la valeur par défaut de 15 secondes est appropriée pour la plupart des réseaux afin d'éviter l'oscillation des routes. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.
Délai d'inactivité SCTP et contournement de l'état SCTP	9.5(2)	Vous pouvez définir un délai d'inactivité pour les connexions SCTP. Vous pouvez également activer le contournement de l'état SCTP pour désactiver l'inspection avec état SCTP sur une classe de trafic. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)** ; assistant **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, onglet **Connection Settings (Paramètres de connexion)**.

Nom de la caractéristique	Versions de plateforme	Description
Décharge de flux pour l'ASA sur le Firepower 9300	9.5(2.1)	Vous pouvez identifier les flux qui doivent être déchargés de l'ASA et commutés directement dans la carte réseau (sur le Firepower 9300). Cela offre des performances améliorées pour les flux de données volumineux dans les centres de données. Cette fonctionnalité nécessite FXOS 1.1.3. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Offload Engine (Moteur de déchargement)**, l'onglet **Rule Actions (Actions de règles)** > **Connection Settings (Paramètres de connexion)** lors de l'ajout ou de la modification des règles sous **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
Prise en charge du déchargement de flux pour l'ASA sur le Firepower 4100.	9.6(1)	Vous pouvez identifier les flux qui doivent être déchargés de l'ASA et commutés directement dans la carte réseau pour le Firepower 4100. Cette fonctionnalité requiert FXOS 1.1.4. Il n'y a aucune nouvelle commande ni écran ASDM pour cette fonctionnalité.
Prise en charge du déchargement de flux pour les connexions de multidiffusion en mode transparent.	9.6(2)	Vous pouvez désormais décharger les connexions de multidiffusion à basculer directement dans la carte d'interface réseau sur les périphériques Firepower 4100 et 9300 en mode transparent. Le déchargement de multidiffusion est disponible pour les groupes de ponts qui contiennent deux et seulement deux interfaces. Il n'y a aucune nouvelle commande ni écran ASDM pour cette fonctionnalité.

Nom de la caractéristique	Versions de plateforme	Description
Modifications dans la gestion des options TCP.	9.6(2)	Vous pouvez désormais spécifier des actions pour les options TCP MSS et MD5 dans l'en-tête TCP d'un paquet lors de la configuration d'une carte TCP. De plus, la gestion par défaut des options MSS, horodatage, taille de fenêtre et accusé de réception sélectif a été modifiée. Auparavant, ces options étaient autorisées, même s'il y avait plus d'une option d'un type donné dans l'en-tête. Désormais, les paquets sont abandonnés par défaut s'ils contiennent plusieurs options d'un type donné. Par exemple, précédemment, un paquet avec 2 options d'horodatage était autorisé, il sera maintenant abandonné. Vous pouvez configurer une carte TCP pour autoriser plusieurs options du même type pour MD5, MSS, accusé de réception sélectif, horodatage et taille de fenêtre. Pour l'option MD5, la valeur par défaut précédente était d'effacer l'option, tandis que la valeur par défaut est maintenant de l'autoriser. Vous pouvez également abandonner les paquets contenant l'option MD5. Pour l'option MSS, vous pouvez définir la taille de segment maximum dans la carte TCP (par classe de trafic). La valeur par défaut pour toutes les autres options TCP reste la même : elles sont effacées. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **TCP Maps (Cartes TCP)** Add/Edit dialog box (Boîte de dialogue Ajouter/modifier).
Délai d'expiration de route obsolète pour les protocoles de passerelle intérieure	9.7(1)	Vous pouvez maintenant configurer le délai d'expiration pour supprimer des routes obsolètes pour les protocoles de passerelle intérieure tels que OSPF. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.
Délai d'expiration global pour les erreurs ICMP	9.8(1)	Vous pouvez maintenant définir le délai d'inactivité avant que l'ASA ne supprime une connexion ICMP après avoir reçu un paquet de réponse d'écho ICMP. Lorsque ce délai d'expiration est désactivé (par défaut) et que vous activez l'inspection ICMP, l'ASA supprime la connexion ICMP dès qu'une réponse d'écho est reçue; ainsi, toutes les erreurs ICMP générées pour la connexion (maintenant fermée) sont abandonnées. Ce délai d'expiration retarde la suppression des connexions ICMP afin que vous puissiez recevoir des erreurs ICMP importantes. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.
Délai d'inactivité par défaut pour le contournement d'état TCP	9.10(1)	Le délai d'inactivité par défaut pour les connexions de contournement d'état TCP est désormais de 2 minutes au lieu de 1 heure.

Nom de la caractéristique	Versions de plateforme	Description
Informations sur l'initiateur et le répondeur pour la détection des connexions inactives (DCD) et prise en charge du DCD dans une grappe.	9.13(1)	Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande **show conn detail** pour obtenir des informations sur l'initiateur et le répondeur. La détection des connexions inactives vous permet de maintenir une connexion inactive, et la sortie **show conn** vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe. Nouveaux écrans ou modifiés : aucun.
Configurer la taille maximale de segment (MSS) pour les connexions amorces.	9.16(1)	Vous pouvez configurer une politique de service afin de définir la taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions amorces lors de l'atteinte de la limite de connexions amorces. Cela est important pour les politiques de service dans lesquelles vous définissez également des nombres maximums de connexions amorces. Écrans nouveaux ou modifiés : **Paramètres de connexion** de l'assistant d'ajout ou de modification d'une politique de service.
Configurer le délai d'inactivité global de l'initialisation de l'appel SIP	9.16(x)	Vous pouvez configurer le délai d'inactivité après lequel une session SIP dans l'état d'appel Call_Init (après la réception du message d'invitation initial) sera supprimée, c'est-à-dire lorsqu'aucune réponse n'est reçue, entre 0:0:1 et 1193:0:0. La valeur par défaut est de 32 secondes (0:00:32).
Décharge de flux IPsec.	9.18(1)	Sur la Secure Firewall 3100, les flux IPsec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Écrans ajoutés ou modifiés : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **IPsec Offload (Déchargement IPsec)**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.