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?

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.
- **La détection des connexions inactives (DCD) :** Si vous avez des connexions persistantes qui sont valides mais souvent inactives, de sorte qu'elles se ferment parce qu'elles dépassent les paramètres de délai d'inactivité, vous pouvez activer la détection des connexions inactives pour identifier les connexions inactives mais valides et les maintenir actives (en réinitialisant leurs minuteurs 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 normalisateur 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 9, 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 de TCP pour le routage symétrique (TCP State Bypass), à la page 13, si vous disposez de ce type d'environnement de routage.

Étape 5 Désactiver la gestion aléatoire de la séquence TCP, à la page 16, si l'aléatorisation par défaut brouille les données pour certaines connexions.

Étape 6 Délester les flux volumineux, à la page 18, si vous devez améliorer les performances dans un centre de données exigeant en informatique.

Étape 7 Configurer les paramètres de connexion pour des cartes de classes de trafic spécifiques (tous les services), à la page 23. 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 28, 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

Utilisez la commande **timeout** pour définir les délais d'expiration globaux.

Toutes les valeurs de délai d'expiration sont au format *hh*:*mm*:*ss*, avec une durée maximale de 1193:0:0 dans la plupart des cas. Utilisez la commande **clear configure timeout** pour réinitialiser tous les délais d'expiration à leurs valeurs par défaut. Si vous souhaitez réinitialiser simplement untemporisateur à la valeur par défaut, entrez la commande **timeout** pour ce paramètre avec la valeur par défaut.

Utilisez **0** pour la valeur afin de désactiver un temporisateur.

Vous pouvez configurer les délais d'expiration globaux suivants.

- **timeout conn** *hh*:*mm*:*ss* : le délai d'inactivité après lequel une connexion se ferme, entre 0:5:0 et 1193:0:0. La valeur par défaut est 1 heure (1:0:0).
- **timeout half-closed** *hh*:*mm*:*ss* : 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.**conn** La durée minimale est de 30 secondes. La valeur par défaut est 10 minutes.
- **timeout udp** *hh*:*mm*:*ss* : 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.
- **timeout icmp** *hh*:*mm*:*ss* : le délai d'inactivité pour ICMP, entre 0:0:2 et 1193:0:0. La valeur par défaut est de 2 secondes (0:0:2).
- **timeout icmp-error** *hh*:*mm*:*ss* : le délai d'inactivité avant que l'ASA ne supprime une connexion ICMP après avoir reçu un paquet de réponse d'écho ICMP, entre 0:0:0 et 0:1:0 ou la valeur **timeout 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.
- **timeout sunrpc** *hh*:*mm*:*ss* : 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.
- **timeout H323** *hh*:*mm*:*ss* : le temps d'inactivité après lequel les connexions multimédias H.245 (TCP) et H.323 (UDP) sont fermées, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0). 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).
- **timeout h225** *hh*:*mm*:*ss* : le temps d'inactivité avant la fermeture d'une connexion de signalisation H.225. Le délai d'expiration par défaut pour H.225 est de 1 heure (1:0:0). Pour fermer une connexion immédiatement après la libération de tous les appels, un délai d'expiration de 1 seconde (0:0:1) est recommandé.
- **timeout mgcp** *hh*:*mm*:*ss* : le temps d'inactivité après lequel une connexion de support MGCP est supprimée, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0).
- **timeout mgcp-pat** *hh*:*mm*:*ss* : intervalle absolu après lequel une traduction MGCP PAT est supprimée, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0). La durée minimale est de 30 secondes.
- **timeout sctp** *hh*:*mm*:*ss* : durée 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)
- **timeout sip** *hh*:*mm*:*ss* : durée d'inactivité jusqu'à la fermeture d'une connexion de port de signalisation SIP, entre 0:5:0 et 1193:0:0. La valeur par défaut est de 30 minutes (0:30:0).

- **timeout sip_media** *hh*:*mm*:*ss* : le temps d'inactivité avant la fermeture d'une connexion de port média SIP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes. Le temporisateur de médias SIP est utilisée pour les paquets de médias SIP RTP/RTCP avec SIP UDP, plutôt que le délai d'inactivité d'UDP.
- **timeout sip-provisional-media** *hh*:*mm*:*ss* : la valeur du délai d'expiration pour les connexions média provisoires SIP, entre 0:1:0 et 0:30:0. La valeur par défaut est 2 minutes.
- **timeout sip-invite** *hh*:*mm*:*ss* : le temps d'inactivité après lequel les passages pour les réponses PROVISOIRES et les traductions de médias seront fermés, entre 0:1:0 et 00:30:0. La valeur par défaut est de 3 minutes. (0:3:0).
- **timeout sip-disconnect** *hh*:*mm*:*ss* : le temps d'inactivité après lequel une session SIP est supprimée si le 200 OK n'est pas reçu pour un message CANCEL ou BYE, entre 0:0:1 et 00:10:0. La valeur par défaut est 2 minutes. (0:2:0)
- **timeout uath** *hh*:*mm*:*ss* {**absolute** | **inactivity**} — La durée avant l'expiration du cache d'authentification et d'autorisation et l'utilisateur doit réauthentifier la connexion suivante, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0). Le temporisateur par défaut est **absolute**; vous pouvez définir le délai d'expiration après une période d'inactivité en saisissant le mot-clé **inactivity**. La durée uauth doit être plus courte que la durée xlate. Réglez à 0 pour désactiver la mise en cache. N'utilisez pas 0 si le protocole FTP passif est utilisé pour la connexion ou si la commande virtual http est utilisée pour l'authentification Web.
- **timeout xlate** *hh*:*mm*:*ss* : le temps d'inactivité jusqu'à ce qu'un emplacement de traduction soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est de 3 heures.
- **timeout pat-xlate** *hh*:*mm*:*ss* : 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.
- **timeout tcp-proxy-reassembly** *hh*:*mm*:*ss* : 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).
- **timeout floating-conn** *hh*:*mm*:*ss* : lorsqu'il existe plusieurs routes 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 permettre d'utiliser de meilleures routes, définissez le délai d'expiration à une valeur comprise entre 0:0:30 et 1193:0:0.
- **timeout conn-holddown** *hh*:*mm*:*ss* : 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 du temporisateur 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.
- **timeout igp stale-route** *hh*:*mm*:*ss* : durée pendant laquelle une route périmée est conservée 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.

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'empêcher 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 proxy pour le serveur et génère une réponse SYN-ACK à la requête SYN du client à l'aide de la méthode de témoin 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 Créez une carte de trafic L3/L4 pour identifier les serveurs que vous protégez. Utilisez une correspondance de liste d'accès.

```
class-map name
match parameter
```

Exemple :

```
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```

Étape 2 Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

Exemple :

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

Étape 3 Définissez les limites de connexion embryonnaires.

- **set connection embryonic-conn-max** *n* : le nombre maximal de connexions TCP embryonnaires simultanées autorisées, de 0 à 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions.
- **set connection per-client-embryonic-max** *n* : le nombre maximal de connexions TCP embryonnaires simultanées autorisées par client, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions.
- **set connection syn-cookie-mss** *n* : 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'est significatif que si vous configurez **set connection embryonic-conn-max** ou **per-client-embryonic-max**.

Exemple :

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

Étape 4 Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Étape 5 Configurez les statistiques de détection des menaces pour les attaques interceptées par TCP Intercept.

threat-detection statistics tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

Lieu :

- **rate-interval** *minutes* définit la taille de la fenêtre de surveillance de l'historique, entre 1 et 1 440 minutes. La valeur par défaut est de 30 minutes. Pendant cet intervalle, le système échantillonne le nombre d'attaques 30 fois.
- **burst-rate** *attaques_par_sec* définit le seuil pour la génération de messages syslog, entre 25 et 2147483647. La valeur par défaut est de 400 par seconde. Lorsque le débit en rafale est dépassé, le périphérique génère le message syslog 733104.
- **average-rate** *attacks_per_sec* définit le seuil de débit moyen pour la génération de messages syslog, entre 25 et 2 147 483 647. La valeur par défaut est de 200 par seconde. Lorsque le débit moyen est dépassé, le message syslog 733105 est généré.

Exemple :

```
hostname(config)# threat-detection statistics tcp-intercept
```

Étape 6 Surveillez les résultats à l'aide des commandes suivantes :

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] : affichez les 10 principaux serveurs protégés par l'attaque. Le mot-clé **all** affiche les données historiques 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.
- **clear threat-detection statistics tcp-intercept** : efface les statistiques d'interception TCP.

Exemple :

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

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.

La configuration par défaut comprend les paramètres suivants :

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 18 clear
tcp-options range 20 255 clear
tcp-options md5 allow
tcp-options mss allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

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 Créez une liste TCP pour préciser les critères de normalisation TCP que vous souhaitez rechercher : **tcp-map** *tcp-map-name*

Étape 2 Configurez les critères de liste TCP en saisissant une ou plusieurs des commandes suivantes. Les valeurs par défaut sont utilisées pour toutes les commandes que vous n'entrez pas. Utilisez la forme **no** de la commande pour désactiver le paramètre.

- **check-retransmission** : empêche la retransmission TCP incohérente. Cette commande est désactivée par défaut.
- **checksum-verification** : vérifie la somme de contrôle TCP, en abandonnant les paquets qui échouent la vérification. Cette commande est désactivée par défaut.
- **exceed-mss** {**allow** | **drop**} : autorisez ou abandonnez les paquets dont la longueur des données dépasse la taille maximale de segment TCP. La valeur par défaut est d'autoriser les paquets.
- **invalid-ack** {**allow** | **abandon**} : autorisez ou abandonnez les paquets avec un ACK non valide. La valeur par défaut est d'abandonner le paquet, à l'exception des connexions WAAS, où ils sont autorisés. Vous pourriez voir des 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 le même que le 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.

- **queue-limit** *pkt_num* [**timeout** *seconds*] : définit le nombre maximal de paquets hors ordre qui peuvent être mis en mémoire tampon et mis en ordre pour une connexion TCP, entre 1 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 (la commande **inspect**), et TCP check-retransmission (commande TCP map **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 commande **queue-limit** à 1 ou plus, le nombre de paquets hors ordre 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**. 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.

  L'argument **timeout** *seconds* définit 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 l'argument *pkt_num* est défini à 0 ; vous devez définir la limite à 1 ou au-dessus pour que le mot-clé **timeout** prenne effet.

- **reserved-bits** {**allow** | **clear** | **drop**} : set the action for reserved bits in the TCP header. Vous pouvez **autoriser** le paquet (sans modifier les bits), **effacer** les bits et autoriser le paquet, ou **abandonner** le paquet.
- **seq-past-window** {**allow** | **abandon**} : définir l'action pour les paquets qui ont des numéros de séquence de fenêtre dépassée, 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. Vous pouvez **autoriser** les paquets uniquement si la commande **queue-limit** est définie à 0 (désactivée). La valeur par défaut est d'abandonner les paquets.
- **synack-data** {**allow** | **abandon**} : autorisez ou abandonnez les paquets TCP SYNACK qui contiennent des données. La valeur par défaut est d'abandonner le paquet.
- **syn-data** {**allow** | **abandon**} : autorisez ou abandonnez les paquets SYN avec des données. La valeur par défaut est d'autoriser le paquet.
- **tcp-options** {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action* : définissez l'action pour les paquets avec options TCP. Ces options sont nommées : **md5**, **mss**, **selective-ack** (mécanisme de réception sélectif), **timestamp**, et **window-scale** (mécanisme d'évolutivité des fenêtres). Pour d'autres options, vous les spécifiez par numéro sur le mot-clé **range**, où les limites de plage sont 6-7, 9-18 et 20-255. Pour cibler une seule option par numéro, saisissez le même nombre pour la plage inférieure et supérieure. Vous pouvez saisir la commande plusieurs fois dans une liste pour définir votre politique complète. 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. Voici les actions possibles :

- **allow** [**multiple**] : autorisez les paquets qui contiennent une seule option de ce type. Il s'agit du réglage par défaut pour toutes les options nommées. Si vous souhaitez autoriser les paquets même s'ils contiennent plusieurs instances de l'option, ajoutez le mot-clé **multiple**. (Le mot-clé **multiple** n'est pas disponible avec **range**.)
- **maximum** *limit* : pour **mss** uniquement. Définissez la taille de segment maximale à la limite indiquée, de 68 à 65 535. Le MSS TCP par défaut est défini dans la commande **sysopt connection tcpmss**.
- **clear** : supprimez les options de ce type de l'en-tête et autorisez le paquet. Il s'agit du réglage par défaut pour toutes les options numérotées. Notez que l'effacement de l'option d'horodatage désactive PAWS et RTT.
- **drop** : abandon des paquets qui contiennent cette option. Cette action est disponible pour **md5** et **range** uniquement.

- **ttl-evasion-protection** : 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. La protection contre le contournement TTL est activée par défaut, de sorte que vous n'aurez qu'à saisir la forme **no** de cette commande.

  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.

- **urgent-flag** {**allow** | **clear**} : définit l'action pour les paquets portant l'indicateur URG. Vous pouvez **autoriser** le paquet ou **effacer** l'indicateur et autoriser le paquet. La valeur par défaut est d'effacer l'indicateur.

  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.

- **window-variation** {**allow** | **drop**} : autorise ou abandonne une connexion dont la taille de fenêtre a été modifiée de manière inattendue. La valeur par défaut est d'autoriser la connexion.

  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. Lorsque cette condition est détectée, la connexion peut être abandonnée.

Étape 3 Appliquez la liste TCP à une classe de trafic à l'aide d'une politique de service.

a) Définissez la classe de trafic avec une carte de classe L3/L4 et ajoutez la carte à une carte de politiques.

```
class-map name
match parameter
policy-map name
class name
```

Exemple :

```
hostname(config)# class-map normalization
hostname(config-cmap)# match any
hostname(config)# policy-map global_policy
hostname(config-pmap)# class normalization
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour en savoir plus sur la mise en correspondance des instructions pour les cartes de trafic, consultez Créer une carte de trafic de couche 3/4 pour le trafic de transit.

b) Appliquez la liste TCP : **set connection advanced-options** *tcp-map-name*

Exemple :

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

c) Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Exemples

Par exemple, pour autoriser les paquets d'indicateurs et de décalages urgents pour tout le trafic envoyé à la plage de ports TCP entre le port de données FTP bien connu et le port Telnet, entrez les commandes suivantes :

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

Contourner les vérifications de l'état de TCP pour le routage symétrique (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.

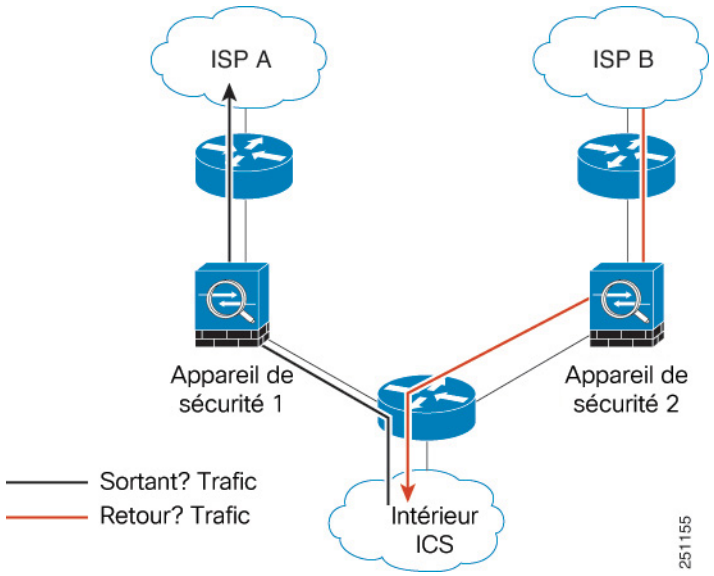
Le problème du routage asymétrique

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 la 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.
- Basculement avec état

Lignes directrices de NAT de contournement d'état TCP

Comme la session de traduction est établie séparément pour chaque ASA, 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 utilisant la commande **set connection timeout idle** pour la carte de trafic de contournement de l'état TCP. Les connexions TCP normales expirent par défaut après 60 minutes.

Procédure

Étape 1 Créez une carte de trafic L3/L4 pour identifier les hôtes qui nécessitent un contournement de l'état TCP. Utilisez une correspondance de liste d'accès pour identifier les hôtes source et de destination.

```
class-map name
match parameter
```

Exemple :

```
hostname(config)# access-list bypass extended permit tcp host 10.1.1.1 host 10.2.2.2
hostname(config)# class-map bypass-class
hostname(config-cmap)# match access-list bypass
```

Étape 2 Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

Exemple :

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class bypass-class
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

Étape 3 Activer le contournement de l'état TCP sur la carte : **set connection advanced-options tcp-state-bypass**

Étape 4 Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Exemple

Voici un exemple de configuration pour le contournement de l'état TCP :

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

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 Créez une carte de trafic L3/L4 pour identifier le trafic dont les numéros de séquence TCP ne doivent pas être rendus aléatoires. 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.

```
class-map name
match parameter
```

Exemple :

```
hostname(config)# access-list preserve-sq-no extended permit tcp any host 10.2.2.2
hostname(config)# class-map no-tcp-random
hostname(config-cmap)# match access-list preserve-sq-no
```

Étape 2 Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

Exemple :

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class no-tcp-random
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

Étape 3 Désactivez la randomisation du numéro de séquence TCP sur la classe :

set connection random-sequence-number disable

Si vous décidez de le réactiver ultérieurement, remplacez « disable » par **enable**.

Étape 4 Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

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
- 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 à ASA 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.

flow-offload enable

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.

En mode contexte multiple, l'activation ou la désactivation du déchargement de flux l'active ou le désactive pour tous les contextes. Vous ne pouvez pas avoir différents paramètres par contexte.

Exemple :

```
ciscoasa(config)# flow-offload enable
```

```
WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.

ciscoasa(config)# write memory
ciscoasa(config)# reload
```

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

a) Créez une carte de trafic L3/L4 pour identifier le trafic admissible au déchargement de flux. La mise en correspondance par liste d'accès ou par port constitue généralement les options les plus courantes.

```
class-map name
match parameter
```

Exemple :

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
```

b) Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

Exemple :

```
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

c) Activer le déchargement de flux sur la carte : **set connection advanced-options flow-offload**

d) Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy offload_policy interface outside
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Exemple

L'exemple suivant carte tout le trafic TCP du sous-réseau 10.1.1.0 255.255.255.224 comme admissible au déchargement et associe la politique à l'interface externe.

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
hostname(config-pmap-c)# set connection advanced-options flow-offload
hostname(config)# service-policy offload_policy interface outside
```

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 désactivée.
- 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 Activez le déchargement de flux IPsec.

flow-offload-ipsec

Étape 2 Activez l'optimisation de sortie pour optimiser le chemin d'accès aux données afin d'améliorer les performances pour les flux de tunnel unique.

flow-offload-ipsec egress-optimization

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. L'optimisation de sortie n'est pas activée par défaut.

Configurer les paramètres de connexion pour des cartes de 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'aléatorisation 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.

La commande **set connection** (pour les limites de connexion et l'aléatorisation de séquence) et les commandes **set connection timeout** sont décrites ici séparément pour chaque paramètre. Cependant, vous pouvez saisir les commandes sur une seule ligne et si vous les saisissez séparément, elles s'affichent dans la configuration comme une seule commande.

Procédure

Étape 1 Créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez personnaliser les paramètres de connexion.

```
class-map name
match parameter
```

Exemple :

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

Pour en savoir plus sur la mise en correspondance des instructions, consultez Créer une carte de trafic de couche 3/4 pour le trafic de transit.

Étape 2 Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

Exemple :

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class CONNS
```

Dans la configuration par défaut, la liste des politiques global_policy est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste global_policy, saisissez global_policy comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

Étape 3 Définir les limites de connexion et la répartition aléatoire du numéro de séquence TCP. (Interception TCP.)

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.

- **set connection conn-max** *n*—(TCP, UDP, SCTP.) Le nombre maximal de connexions simultanées autorisées, entre 0 et 2 000 000, pour l'ensemble de la classe. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Pour les connexions TCP, cela s'applique uniquement aux connexions établies.
  - Si deux serveurs sont configurés pour autoriser les connexions simultanées, la limite de connexion est appliquée à chaque serveur configuré séparément.
  - Étant donné que la limite est appliquée à une classe, un hôte attaquant peut utiliser toutes les connexions et n'en laisser aucune pour les autres hôtes qui correspondent à la classe.
- **set connection per-client-max** *n*—(TCP, UDP, SCTP.) Le nombre maximal de connexions simultanées autorisées par client, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Cette option restreint le nombre maximal de connexions simultanées autorisées pour chaque hôte correspondant à la classe. Pour les connexions TCP, cela inclut les connexions établies, à moitié ouvertes et à moitié fermées.
- **set connection embryonic-conn-max** *n*—Le nombre maximal de connexions TCP embryonnaires simultanées autorisées, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. 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.
- **set connection per-client-embryonic-max** *n*—Le nombre maximal de connexions TCP embryonnaires simultanées autorisées par client, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions.
- **set connection syn-cookie-mss** *n* : 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'est significatif que si vous configurez **set connection embryonic-conn-max** ou **per-client-embryonic-max**.

- **set connection random-sequence-number** {**enable** | **disable**} : activer ou désactiver la randomisation des numéros de séquence TCP. La répartition aléatoire est activée par défaut.

Exemple :

```
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
```

Étape 4 Définissez les délais d'expiration de connexion et la détection de connexion inactive (DCD).

Les valeurs par défaut décrites ci-dessous supposent que vous n'ayez pas modifié les valeurs globales par défaut pour ces comportements à l'aide de la commande **timeout** ; les valeurs globales par défaut remplacent celles décrites ici. Saisissez **0** pour désactiver le temporisateur, afin qu'une connexion n'expire jamais.

- **set connection timeout embryonic** *hh*:*mm*:*ss* : la période de délai d'expiration jusqu'à ce qu'une connexion TCP embryonnaire (semi-ouverte) soit fermée, entre 0:0:5 et 1 193:00:00. La valeur par défaut est 0:0:30.
- **set connection timeout idle** *hh*:*mm*:*ss*[**reset**] : la période de délai d'inactivité après laquelle une connexion établie de n'importe quel protocole se ferme, entre 0:0:1 et 1 193:0:0. La valeur par défaut est 1:0:0. Pour le trafic TCP, le mot-clé **reset** envoie une réinitialisation aux terminaux TCP lorsque la connexion expire.

  Le délai d'inactivité **udp** par défaut est de 2 minutes. Le délai d'inactivité **icmp** par défaut est de 2 secondes. Le délai d'inactivité **esp** et **ha** par défaut est de 30 secondes. Pour tous les autres protocoles, le délai d'inactivité par défaut est de 2 minutes.
- **set connection timeout half-closed** *hh*:*mm*:*ss*—Le délai d'inactivité jusqu'à la fermeture d'une connexion à moitié fermée, entre 0:5:0 (pour la version 9.1(1) et les versions antérieures) ou 0:0:30 (pour la version 9.1(2) et versions ultérieures) et 1193:0:0. 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.
- **set connection timeout dcd** [*retry-interval* [*max_retries*]]—Activez la détection des connexions inactives (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. 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.

  L'intervalle de réessai définit la durée au format *hh*:*mm*:*ss* à attendre après chaque sonde DCD non réactive avant d'envoyer une autre sonde, entre 0:0:1 et 24:0:0. La valeur par défaut est 0:0:15. max-retries définit le nombre de tentatives consécutives échouées pour DCD avant de déclarer la connexion comme inactive. La valeur minimale est 1 et la valeur maximale est 255. La valeur par défaut est égale à 5.

  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.

Exemple :

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
```

Étape 5 Décrémentez le temps de vie (TTL) sur les paquets qui correspondent à la classe : **set connection decrement-ttl**

Cette commande, ainsi que la commande **icmp unreachable**, est nécessaire pour permettre un traceroute via l'ASA qui affiche l'ASA comme l'un des sauts.

Exemple :

```
hostname(config)# class-map global-policy
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map global_policy
hostname(config-pmap)# class global-policy
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

Étape 6 Définir des options avancées.

Les options avancées sont des configurations à usage spécial qui ne sont pas nécessaires dans des circonstances normales. Vous les configurez avec la commande **set connection advanced-options**

- **set connection advanced-options** *tcp_map_name* : personnaliser le comportement du normalisateur TCP en appliquant une liste TCP. Pour de plus amples renseignements, voir Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP), à la page 9.
- **set connection advanced-options tcp-state-bypass** : mettre en œuvre le contournement de l'état TCP. Pour de plus amples renseignements, voir Contourner les vérifications de l'état de TCP pour le routage symétrique (TCP State Bypass), à la page 13.
- **set connection advanced-options sctp-state-bypass** : mettre en œuvre le contournement de l'état SCTP pour désactiver l'inspection dynamique SCTP. Pour en savoir plus, consultez Inspection dynamique SCTP.
- **set connection advanced-options flow-offload** : (ASA sur le Châssis Firepower 4100/9300 , FXOS 1.1.3 ou version ultérieure, uniquement.) Implémentation du 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 entrer la commande **flow-offload enable**, qui ne fait pas partie de la politique de service.

Exemple :

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

Étape 7 Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée global_policy), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une

interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

Exemple

L'exemple suivant définit les limites de connexion et les délais d'expiration pour tout le trafic :

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

Vous pouvez entrer des commandes **set connection** avec plusieurs paramètres ou saisir chaque paramètre en tant que commande distincte. L'ASA combine les commandes en une seule ligne dans la configuration en cours d'exécution. Par exemple, si vous avez saisi les deux commandes suivantes en mode de configuration de classe :

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

La sortie de la commande **show running-config policy-map** afficherait le résultat des deux commandes en une seule commande combinée :

```
set connection conn-max 600 embryonic-conn-max 50
```

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 (CLI). Configurez le comportement de réinitialisation TCP.

service { **resetinbound** [**interface** [*interface_name*] | **resetoutbound** [**interface** [*interface_name*] | **resetoutside** }] […]]

- **resetinbound**. Envoie des réinitialisations TCP pour toutes les sessions TCP entrantes qui tentent de transiter par l'ASA et qui 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 touché. Lorsque cette option n'est

pas activée, l'ASA rejette silencieusement les paquets refusés. Si vous ne spécifiez pas d'interface, ce paramètre s'applique à toutes les interfaces.

- **resetoutbound**. Envoie des réinitialisations TCP pour toutes les sessions TCP sortantes qui tentent de transiter par l'ASA et qui 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 touché. Lorsque cette option n'est pas activée, l'ASA rejette silencieusement les paquets refusés. Par défaut, cette option est activée. Vous pourriez souhaiter désactiver les réinitialisations sortantes pour réduire la charge du processeur pendant les tempêtes de trafic, par exemple.
- **resetoutside**. Active les réinitialisations pour les paquets TCP qui se terminent au niveau de 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 refusés.

  Nous vous recommandons d'utiliser cette option avec la PAT de l'interface. Cette option 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.

Étape 2 Définissez TCP MSS pour vous assurer que la taille maximale de segment TCP pour le trafic de transit ne dépasse pas la valeur que vous avez définie et que la taille maximale n'est pas inférieure à une taille spécifiée.

sysopt connection tcpmss [**minimum**] *bytes*

Sans **minimum** mot-clé. Définissez la taille maximale du segment TCP 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.

minimum. Remplace la taille maximale du segment pour qu'elle ne soit pas inférieure aux octets spécifiés, entre 48 et 65 535 octets. Cette fonctionnalité est désactivée par défaut (définie sur 0).

Étape 3 Définir le délai d'attente de connexion TCP.

sysopt connection timewait

Utilisez cette commande pour forcer 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 pourriez vouloir utiliser cette fonctionnalité si la séquence de terminaison TCP par défaut d'une application hôte terminal est une fermeture simultanée.

Étape 4 Définissez le nombre maximal de segments TCP non traités.

sysopt connection tcp-max-unprocessed-seg *segments*

Définissez 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.

Supervision des connexions

Vous pouvez utiliser les commandes suivantes pour surveiller les connexions :

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

  Affiches des renseignements sur la connexion Des 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**.

Nom de la caractéristique	Versions de plateforme	Description
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. La commande suivante a été modifiée : **set connection timeout**
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 la commande suivante : **timeout floating-conn**.
Délai d'expiration configurable pour PAT xlate	8.4(3)	Lorsqu'une xlate PAT 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 introduit la commande suivante : **timeout pat-xlate**. *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 les commandes suivantes : **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, **set connection per-client-max**.
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 commandes suivantes : **set connection timeout half-closed**, **timeout half-closed**.
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 ajouté la commande suivante : **timeout conn-holddown**.

Nom de la caractéristique	Versions de plateforme	Description
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 ajouté ou modifié les commandes suivantes : **timeout sctp**, **set connection advanced-options sctp-state-bypass**.
Décharge de flux pour l'ASA sur le Firepower 9300Firepower 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 commandes suivantes : **clear flow-offload**, **flow-offload enable**, **set-connection advanced-options flow-offload**, **show conn detail**, **show flow-offload**.
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 la commande suivante : **timeout igp stale-route**.
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 ajouté la commande suivante : **timeout igp stale-route**.
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 ajouté la commande suivante : **timeout icmp-error**
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.
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. Commandes nouvelles ou modifiées : **show conn** (sortie uniquement).

Nom de la caractéristique	Versions de plateforme	Description
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. Commandes nouvelles ou modifiées : **set connection syn-cookie-mss**.
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. Nous avons ajouté les commandes suivantes : **clear flow-offload-ipsec**, **flow-offload-ipsec**, **show flow-offload-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.

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.

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.

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.

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.