Politiques de service

Vous pouvez utiliser les politiques de service Firepower Threat Defense pour appliquer des services à des classes de trafic spécifiques. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Une politique de service comprend plusieurs actions ou règles appliquées à une interface ou appliquées globalement.

À propos des politiques de service Firepower Threat Defense

Vous pouvez utiliser les politiques de service Firepower Threat Defense pour appliquer des services à des classes de trafic spécifiques. Grâce aux politiques de service, vous n'êtes pas limité à appliquer les mêmes services à toutes les connexions qui entrent dans le périphérique ou dans une interface donnée.

Une classe de trafic est une combinaison de l'interface et d'une liste de contrôle d'accès étendue (ACL). Les règles « autoriser » de l'ACL déterminent quelles connexions font partie de la classe. Tout trafic « refusé » dans la liste de contrôle d'accès n'est tout simplement pas appliqué : ces connexions ne sont pas réellement abandonnées. Vous pouvez utiliser les adresses IP et les ports TCP/UCP pour identifier les connexions correspondantes aussi précisément que vous le souhaitez.

Il existe deux types de classes de trafic :

- Interface basée sur les règles : si vous spécifiez une zone ou un groupe d'interfaces de sécurité dans une règle de politique de service, la règle s'applique au trafic « autorisé » d'ACL qui passe par une interface qui fait partie des objets d'interface.

  Pour une fonctionnalité donnée, les règles basées sur l'interface appliquées à l'interface d'entrée prévalent toujours sur les règles globales : si une règle basée sur l'interface d'entrée s'applique à une connexion, toute règle globale correspondante est ignorée. Si aucune interface d'entrée ou règle globale ne s'applique, une règle de service d'interface sur l'interface de sortie est appliquée.

- Règles globales : ces règles s'appliquent à toutes les interfaces. Si une règle basée sur l'interface ne s'applique pas à une connexion, les règles globales sont vérifiées et appliquées à toutes les connexions

autorisées par la liste de contrôle d'accès. Si aucun service ne s'applique, les connexions se déroulent sans qu'aucun service ne soit appliqué.

Une connexion donnée ne peut correspondre qu'à une seule classe de trafic, globale ou basée sur l'interface, pour une fonctionnalité donnée. Il devrait y avoir au plus une règle pour une combinaison donnée d'interface et de flux de trafic.

Les règles de politique de service sont appliquées après les règles de contrôle d'accès. Ces services sont configurés uniquement pour les connexions que vous autorisez.

Lien entre les politiques de service et FlexConfig et autres fonctionnalités

Avant la version 6.3(0), vous pouviez configurer les règles de service liées à la connexion à l'aide des objets FlexConfig prédéfinis TCP_Embryronic_Conn_Limit et TCP_Embryronic_Conn_Timeout. Vous devez supprimer ces objets et rétablir vos règles en utilisant la politique de service Firepower Threat Defense. Si vous avez créé des objets FlexConfig personnalisés pour implémenter l'une de ces fonctionnalités liées à la connexion (c'est-à-dire les commandes **set connection**), vous devez également supprimer ces objets et implémenter les fonctionnalités au moyen de la politique de service.

Étant donné que les fonctionnalités de politique de service liées à la connexion sont traitées comme un groupe de fonctionnalités distinct des autres fonctionnalités implémentées par les règles de service, vous ne devriez pas rencontrer de problèmes de chevauchement des classes de trafic. Cependant, soyez prudent lors de la configuration des éléments suivants :

- Les règles de politique QoS sont mises en œuvre à l'aide de l'interface de commande en ligne de politique de service. Ces règles sont appliquées avant les règles de service basées sur la connexion. Cependant, la QoS et les paramètres de connexion peuvent être appliqués aux mêmes classes de trafic ou à des classes de trafic qui se chevauchent.
- Vous pouvez utiliser les politiques FlexConfig pour mettre en œuvre des inspections d'applications et NetFlow personnalisés. Utilisez la commande **show running-config** pour examiner l'interface de ligne de commande qui configure déjà les règles de service, y compris les commandes **policy-map**, **class-map** et **service-policy**. Netflow et l'inspection des applications sont compatibles avec la QoS et les paramètres de connexion, mais vous devez comprendre la configuration existante avant de mettre en œuvre FlexConfig. Les paramètres de connexion sont appliqués avant les inspections d'applications et NetFlow.

Remarque Les classes de trafic créées à partir de la politique de service Firepower Threat Defense sont nommées **class_map_***ACLname*, où *ACLname* est le nom de l'objet ACL étendu utilisé dans la règle de politique de service.

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 défense contre les menaces. 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. Vous configurez les délais d'expiration globaux dans la politique de la plateforme Firepower Threat Defense. Sélectionnez **Devices (périphériques)** > **Platform Settings**(paramètres de la plateforme).

- **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) le défense contre les menaces. 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, défense contre les menaces 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. Vous pouvez configurer la normalisation TCP à l'aide de la politique FlexConfig.
- **Contournement d'état TCP** : vous pouvez contourner la vérification de l'état TCP si vous utilisez le routage dissymétrique dans votre réseau.

Exigences et conditions préalables pour les politiques de service

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d’accès

Administrateur de réseau

Lignes directrices et limites relatives aux politiques de service

- Les politiques de service s’appliquent uniquement aux interfaces routées ou de commutation, en mode routé ou transparent. Elles ne s’appliquent pas aux interfaces définies en ligne ou passives.
- Vous pouvez avoir tout au plus 25 classes de trafic pour une interface donnée ou la politique globale. Plus précisément, cela signifie qu'il ne peut pas y avoir plus de 25 règles de politique de service pour la politique globale pour une zone de sécurité ou un groupe d'interfaces. Cependant, pour les interfaces, puisque la même interface peut apparaître à la fois dans une zone de sécurité et dans un groupe d’interfaces, sachez que la limitation réelle dépend des interfaces, et non de la zone ou du groupe. Ainsi, vous pourriez ne pas pouvoir avoir 25 règles par zone/groupe en fonction des membres de vos zones/groupes.
- Il ne peut y avoir qu'une seule règle pour une combinaison donnée d'objet d'interface et de flux de trafic.
- Lorsque vous apportez des modifications à la configuration de la politique de service, toutes les nouvelles connexions utilisent la nouvelle politique de service. Les connexions existantes continuent d’utiliser la politique qui était configurée au moment de l’établissement de la connexion. Si vous souhaitez que toutes les connexions utilisent immédiatement la nouvelle politique, vous devez déconnecter les connexions actuelles pour qu’elles puissent se reconnecter à l’aide de la nouvelle politique. À partir d'une session SSH ou d'une console CLI, entrez la commande **clear conn** ou **clear local-host**.

Configurer les politiques de service Threat Defense

Vous pouvez utiliser les politiques de service de défense contre les menaces pour appliquer des services à des classes de trafic spécifiques. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d’expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s’applique à toutes les applications TCP. Une politique de service comprend plusieurs actions ou règles appliquées à une interface ou appliquées globalement.

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Access Control**(contrôle d’accès), puis cliquez sur **Edit** (✎) pour la politique de contrôle d’accès dont vous souhaitez modifier la politique de service Threat Defense.

Étape 2 Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 3 Cliquez sur **Edit** (✎) dans le groupe **de politiques du service Threat Defense**.

Une boîte de dialogue s’ouvre et affiche la politique existante. La politique consiste en une liste ordonnée de règles, séparées entre les règles globales (qui s’appliquent à toutes les interfaces) et les règles basées sur l’interface. Le tableau indique l’objet d’interface et le nom de la liste de contrôle d’accès étendu (qui, ensemble, définissent la classe de trafic pour la règle), ainsi que les services appliqués.

Étape 4 Effectuez l'une des actions suivantes :

- Cliquez sur **Add Rule** (Ajouter une règle) pour créer une nouvelle règle. Consultez Configurer une règle de politique de service, à la page 5.
- Cliquez sur **Edit** (✎) pour modifier une règle existante. Consultez Configurer une règle de politique de service, à la page 5.
- Cliquez sur **Supprimer** (🗑) pour supprimer une règle.
- Cliquez sur une règle et faites-la glisser vers un nouvel emplacement pour la déplacer. Vous ne pouvez pas faire glisser des règles entre l'interface et les listes globales, vous devez plutôt modifier la règle pour modifier l'interface/le paramètre global. La première règle de la liste qui correspond à une connexion est appliquée à la connexion.

Étape 5 Cliquez sur **OK** lorsque vous avez terminé de modifier la politique.

Étape 6 Cliquez sur **Save** (Enregistrer) dans la fenêtre **Advanced** (Avancé). Les modifications ne sont pas enregistrées tant que vous ne cliquez pas sur Save (Enregistrer).

Configurer une règle de politique de service

Configurez les règles de politique de service pour appliquer les services à des classes de trafic spécifiques.

Avant de commencer

Accédez à **Objets** > **Gestion des objets** > **Liste d'accès** > **Étendue** et créez une liste d'accès étendue qui définit le trafic auquel la règle s'applique. La règle est appliquée à toutes les connexions correspondant aux règles d'autorisation de la liste d'accès étendue. Définissez les règles d'ACL avec précision, de sorte que votre règle de politique de service s'applique uniquement au trafic nécessitant le service.

Si vous créez une règle basée sur l'interface, vous devez également avoir configuré les interfaces sur les périphériques affectés et les avoir ajoutés aux zones de sécurité ou aux groupes d'interfaces.

Procédure

Étape 1 Si vous n'êtes pas encore dans la boîte de dialogue de politique de service de défense contre les menaces (Threat Defense Service Policy), choisissez **Politiques** > **Contrôle d'accès**, modifiez la politique de contrôle d'accès, sélectionnez **Paramètres avancés** à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis modifiez la **Threat Defense Service Policy** (Politique de service Threat Defense).

Étape 2 Effectuez l'une des actions suivantes :

- Cliquez sur **Add Rule** (Ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

L'assistant de règle de politique de service s'ouvre pour vous guider dans le processus de configuration de la règle.

Étape 3 À l'étape **Interface Object** (objet d'interface), sélectionnez l'option qui définit les interfaces qui utiliseront la politique.

- **Apply Globally**(appliquer globalement) : sélectionnez cette option pour créer une règle globale, qui s'applique à toutes les interfaces.
- **Select Interface Objects** (sélectionner les objets de l'interface) : sélectionnez cette option pour créer une règle basée sur l'interface. Ensuite, sélectionnez les zones de sécurité ou les objets d'interface qui contiennent les interfaces souhaitées et cliquez sur **>** pour les déplacer vers la liste sélectionnée **Suivante**. La règle de politique de service est configurée sur chaque interface contenue dans les objets sélectionnés; elle n'est pas configurée sur la zone ou le groupe lui-même.

Cliquez lorsque les critères d'interface sont complets.

Étape 4 À l'étape **Flux de trafic**, sélectionnez l'objet ACL étendu qui définit les connexions auxquelles la règle s'applique, puis cliquez sur **Next** (Suivant).

Étape 5 À l'étape des **Paramètres de connexion**, configurez les services à appliquer à cette classe de trafic.

- **Enable TCP State Bypass** (connexions TCP uniquement) : Implémentez TCP State Bypass (le contournement d'état TCP). Les connexions soumises au contournement d'état TCP ne sont inspectées par aucun moteur d'inspection et contournent toute vérification d'état TCP et toute normalisation 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 8.

  Remarque Utilisez le contournement d'état TCP à des fins de dépannage ou lorsque le routage dissymétrique ne peut pas être résolu. Cette fonctionnalité désactive plusieurs fonctionnalités de sécurité, ce qui peut entraîner un nombre élevé de connexions si vous ne la mettez pas en œuvre correctement avec une classe de trafic définie de manière étroite.

- **Randomize TCP Sequence Number** (connexions TCP uniquement) : active ou désactive la répartition aléatoire des numéros de séquence TCP. La répartition aléatoire est activée par défaut. Pour en savoir plus, consultez Désactiver la gestion aléatoire de la séquence TCP, à la page 12.
- **Enable Decrement TTL** (connexions TCP uniquement) : décrémente la durée de vie (TTL) des paquets qui correspondent à la classe. 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 une TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues.

  Remarque Si vous souhaitez que le périphérique défense contre les menaces s'affiche sur les traceroutes, vous devez configurer l'option de décrément de la TTL et définir la limite de débit ICMP unreachable dans la politique des paramètres de la plateforme. Consultez Faire en sorte que le périphérique défense contre les menaces s'affiche sur Traceroutes, à la page 17.

- **Connections** : limites du nombre de connexions autorisées pour l'ensemble de la classe. Avant de configurer ces options :
  - **Maximum TCP and UDP** (connexions TCP/UDP uniquement) : le nombre maximal de connexions simultanées autorisées, entre 0 et 2000000, pour l'ensemble de la classe. Pour TCP, ce nombre s'applique aux connexions établies uniquement. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. 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. Définissez la limite par client pour résoudre ce problème.

- **Maximum Embryronic** (connexions TCP uniquement) : le nombre maximal de connexions TCP amorces simultanées (celles qui n'ont pas terminé l'établissement de liaison TCP) autorisée, entre 0 et 2000000. 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. Pour en savoir plus, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 14.

- **Connections Per Client**(connexions par client) : limites du nombre de connexions autorisées pour un client donné (adresse IP source). Avant de configurer ces options :
  - **Maximum TCP et UDP** (connexions TCP/UDP uniquement) : le nombre maximal de connexions simultanées autorisées par client, entre 0 et 2000000. Pour TCP, cela inclut les connexions établies, à moitié ouvertes (amorces) et à moitié fermées. 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.
  - **Maximum Embryronic** (connexions TCP uniquement) : nombre maximal de connexions TCP amorces simultanées autorisée par client, entre 0 et 2000000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Pour en savoir plus, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 14.

- **Connections Syn Cookie MSS** – 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, de 48 à 65 535. La valeur par défaut est 1380. Ce paramètre n'a de sens que si vous configurez le nombre **maximal d'amorces** pour les connexions ou par client, ou les deux.

- **Connections Timeout**(délai d'expiration des connexions) : paramètres de délai d'expiration à appliquer à la classe de trafic. Ces délais d'expiration remplacent les délais d'expiration globaux définis dans la politique des paramètres de plateforme. Vous pouvez configurer les éléments suivants :
  - **Embryronic** (connexions TCP uniquement) : Le délai d'expiration jusqu'à la fermeture d'une connexion TCP amorce (partiellement ouverte), entre 0:0:5 et 1193:00:00. La valeur par défaut est 0:0:30.
  - **Half Closed** (connexions TCP uniquement) : Le délai d'inactivité jusqu'à la fermeture d'une connexion à moitié fermée, entre 0:0:30 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, le système n'envoie pas de réinitialisation lorsqu'il interrompt les connexions à moitié fermées.
  - **Idle** (connexions TCP, UDP, ICMP, IP) : Le délai d'inactivité après lequel une connexion établie de n'importe quel protocole se ferme, entre 0:0:1 et 1193:0:0. La valeur par défaut est 1:0:0, sauf si vous sélectionnez l'option TCP State Bypass (Contournement d'état TCP), où la valeur par défaut est 0:2:0.
  - **Reset Connection Upon Timeout (Réinitialiser la connexion à l'expiration)** (connexions TCP uniquement) : s'il faut envoyer un paquet TCP RST aux deux systèmes d'extrémité après la suppression des connexions inactives.

- **Detect Dead Connections** (connexions TCP uniquement) : s'il faut activer la détection des connexions inactives (DCD). Avant de faire expirer une connexion inactive, le système 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. Par conséquent, ne configurez pas le DCD sur les connexions que vous utilisez pour le chemin rapide dans la politique de préfiltre. Utilisez la commande **show conn detail** dans l'interface de ligne de commande défense contre les menaces pour suivre le nombre de sondes DCD envoyées par l'initiateur et le répondeur.

Configurez les options suivantes :

- **Detection Timeout**(délai d'expiration de détection) : la durée au format hh:mm:ss à attendre après chaque défaillance de chaque sonde DCD avant d'envoyer une autre sonde, entre 0:0:1 et 24:0:0. La valeur par défaut est 0:0:15.

  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.

- **Nouvelles tentatives de détection** – Le nombre de tentatives consécutives ayant échoué de DCD avant de déclarer la connexion inactive, de 1 à 255. La valeur par défaut est égale à 5.

Étape 6 Cliquez sur le bouton « **Finish** » (terminer) pour enregistrer vos modifications.

La règle est ajoutée au bas de la liste appropriée, Interfaces ou Global. Les règles globales sont mises en correspondance dans l'ordre descendant. Les règles de la liste Interfaces sont mises en correspondance dans l'ordre descendant pour chaque objet d'interface. Placez les règles pour les classes de trafic définies de façon précise au-dessus des règles plus générales, pour vous assurer que les bons services sont appliqués. Vous pouvez déplacer les règles au sein de chaque liste par glisser-déposer. Vous ne pouvez pas déplacer des règles entre les listes.

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 défense contre les menaces 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

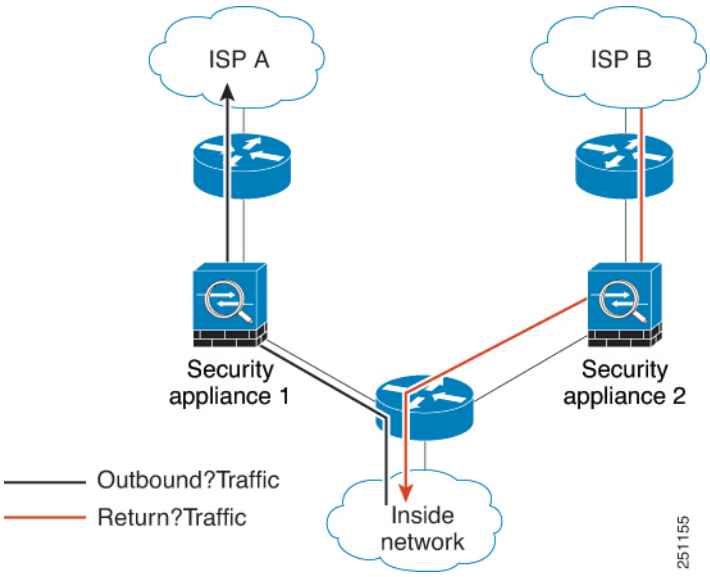
Par défaut, tout le trafic qui passe par défense contre les menaces est inspecté à l'aide de l'algorithme de sécurité adaptatif et est soit autorisé, soit abandonné en fonction de la politique de sécurité. défense contre les menaces optimise la performance du pare-feu en vérifiant l'état de chaque paquet (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 le défense contre les menaces 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 défense contre les menaces.

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 défense contre les menaces 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 défense contre les menaces, 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 défense contre les menaces, et qu'il n'y a pas d'entrée de chemin rapide, le paquet passe par le chemin de gestion de session pour établir le connexion sur le chemin rapide. Une fois dans le chemin rapide, le trafic contourne les vérifications du chemin rapide.

Lignes directrices et limites du contournement d'état TCP

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

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

- Inspection d'application : l'inspection nécessite que le trafic entrant et sortant passe par le même défense contre les menaces, donc l'inspection n'est pas appliquée au trafic de contournement d'état TCP.

- Inspection Snort : l'inspection nécessite que le trafic entrant et sortant passe par le même périphérique. Cependant, l'inspection Snort n'est pas automatiquement contournée pour le trafic de contournement d'état TCP. Vous devez également configurer une règle de chemin rapide de préfiltre pour la classe de trafic pour laquelle vous configurez le contournement de l'état TCP.
- Interception TCP, limite maximale de connexions explorées, répartition aléatoire des numéros de séquence TCP : le défense contre les menaces 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

Directives de NAT de contournement d'état TCP

Comme la session de traduction est établie séparément pour chaque défense contre les menaces, 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. Vous devez également configurer une politique de chemin rapide de préfiltre correspondante pour le même trafic afin de vous assurer que le trafic contourne également l'inspection.

Étant donné que le contournement réduit la sécurité du réseau, limitez son application autant que possible.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic.

Par exemple, pour définir une classe de trafic pour le trafic TCP de 10.1.1.1 à 10.2.2.2, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **Nom** pour l'objet, par exemple contourner.
e) Cliquez sur **Add** pour ajouter une nouvelle règle.
f) Conservez **Allow** (autorisation) pour l'action.
g) Saisissez 10.1.1.1 sous la liste **Source** et cliquez sur **Add** (Ajouter), et 10.2.2.2 sous la liste **Destination**, puis cliquez sur **Add**.
h) Cliquez sur **Port**, sélectionnez **TCP (6)** sous la liste **Selected Source Ports (ports source sélectionnés)**, puis cliquez sur **Add** (Ajouter). N'saisissez pas de numéro de port, ajoutez simplement TCP comme protocole, qui couvrira tous les ports.
i) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.
j) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique du service de contournement d'état TCP.

Par exemple, pour configurer le contournement de l'état TCP pour cette classe de trafic globalement, procédez comme suit :

a) Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** (✎) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally (appliquer globalement)** > **Next (suivant)**.
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next** (Suivant).
f) Sélectionnez **Activer le contournement de l'état TCP**
g) (Facultatif) Réglez le Délai **d'inactivité** pour les connexions contournées. La valeur par défaut est 2 minutes.
h) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
i) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
j) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

Étape 3 Configurez une règle de chemin rapide de préfiltre pour la classe de trafic.

Vous ne pouvez pas utiliser l'objet ACL dans la règle de préfiltre. Vous devez donc recréer la classe de trafic soit directement dans la règle de préfiltre, soit en créant d'abord des objets de réseau qui définissent la classe.

La procédure suivante suppose qu'une politique de préfiltre est déjà associée à la politique de contrôle d'accès. Si vous n'avez pas encore créé de politique de préfiltre, accédez à **Politiques** > **Préfiltre** et créez d'abord la politique. Vous pouvez ensuite suivre cette procédure pour l'associer à la politique de contrôle d'accès et créer la règle.

Pour continuer avec notre exemple, cette procédure crée une règle Fastpath pour le trafic TCP de 10.1.1.1 à 10.2.2.2.

a) Choisissez **Politiques** > **Contrôle d'accès** et modifiez la politique qui comporte la règle de politique de service de contournement TCP.
b) Cliquez sur le lien de la **politique de préfiltre**, qui se trouve à gauche immédiatement sous la description de la politique.
c) Dans la boîte de dialogue Prefilter Policy (politique de préfiltre), sélectionnez la politique à affecter au périphérique si la politique correcte n'est pas déjà sélectionnée. Ne cliquez pas sur OK pour le moment.

   Comme vous ne pouvez pas ajouter de règles à la politique de préfiltre par défaut, vous devez choisir une politique personnalisée.

d) Dans la boîte de dialogue de la politique de préfiltre, cliquez sur **Edit** (✎). Cette action ouvre une nouvelle fenêtre de navigateur dans laquelle vous pouvez modifier la politique.
e) Cliquez sur **Add Prefilter Rule** (ajouter une règle de préfiltre) et configurez une règle avec les propriétés suivantes.

   - **Nom** : n'importe quel nom que vous jugez significatif, tel que TCPBypass.
   - **Action** : sélectionnez **Fastpath**.

- **Interface Objects (objets** de l'interface) – Si vous avez configuré le contournement de l'état TCP comme règle globale, conservez la valeur par défaut, quelconque, pour la source et la destination. Si vous avez créé une règle basée sur l'interface, sélectionnez les mêmes objets d'interface que vous avez utilisés pour la règle dans la liste **Source Interface Objects** (objets de l'interface source) et conservez-les comme destination.
- **Networks**(réseaux) : ajoutez la version 10.1.1 à la liste des **réseaux sources** et la version 10.2.2.2 à la liste des **réseaux de destination**. Vous pouvez soit utiliser des objets réseau, soit ajouter manuellement les adresses.
- **Ports** : sous les ports **source sélectionnés**, sélectionnez TCP(6), **n'indiquez pas de port**, puis cliquez sur **Add** (ajouter). Cela appliquera la règle à tout le trafic TCP (et uniquement), quel que soit le numéro de port TCP.

f) Cliquez sur **Add** pour ajouter la règle à la politique de préfiltre.
g) Cliquez sur **Save** pour enregistrer vos modifications à la politique de préfiltre.

Vous pouvez maintenant fermer la fenêtre de modification du préfiltre et revenir à la fenêtre de modification de la politique de contrôle d'accès.

h) Dans la fenêtre de modification de la politique de contrôle d'accès, la boîte de dialogue Politique de préfiltre doit toujours être ouverte. Cliquez sur **OK** pour enregistrer vos modifications apportées à l'affectation de politique de préfiltre.
i) Cliquez sur **Save** dans la politique de contrôle d'accès pour enregistrer l'affectation de politique de préfiltre modifiée, si vous l'avez modifiée.

Vous devez déployer les modifications sur les périphériques concernés.

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. Le périphérique défense contre les menaces effectue la transmission aléatoire 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. Voici quelques situations dans lesquelles vous pourriez souhaiter désactiver la répartition aléatoire.

- 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 le périphérique 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 le périphérique défense contre les menaces ne randomise pas les numéros de séquence des connexions.

- Si vous activez le contournement matériel pour ISA 3000 et TCP, les connexions sont abandonnées lorsque ISA 3000 ne fait plus partie du chemin de données.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic.

Par exemple, pour définir une classe de trafic pour le trafic TCP à partir de n'importe quel hôte vers la version 10.2.2.2, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **nom** pour l'objet, par exemple, keep-sq-no.preserve
e) Cliquez sur **Add** pour ajouter une nouvelle règle.
f) Conservez **Allow** (autorisation) pour l'action.
g) Laissez la liste **Source** vide, saisissez 10.2.2.2 sous la liste **Destination**, puis cliquez sur **Add** (Ajouter).
h) Cliquez sur **Port**, sélectionnez **TCP (6)** sous la liste **Selected Source Ports (ports source sélectionnés)**, puis cliquez sur **Add** (Ajouter). N'saisissez pas de numéro de port, ajoutez simplement TCP comme protocole, qui couvrira tous les ports.
i) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.
j) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique de service qui désactive la répartition aléatoire des numéros de séquence TCP.

Par exemple, pour désactiver la répartition aléatoire pour cette classe de trafic globalement, procédez comme suit :

a) Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** () pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally (appliquer globalement)** > **Next (suivant)**.
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next** (Suivant).
f) Désélectionnez **Randomize TCP Sequence Number** (Rendre le numéro de séquence TCP aléatoire).
g) (Facultatif) Ajustez les autres options de connexion selon vos besoins.
h) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
i) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
j) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

Vous devez déployer les modifications sur les périphériques concernés.

Exemples de règles de politique de service

Les rubriques suivantes donnent des exemples de règles de politique de service.

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 amorce d'une connexion est franchi, défense contre les menaces agit comme un serveur mandataire pour le serveur et génère une réponse SYN-ACK à la requête SYN du client à l'aide de la méthode du 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 défense contre les menaces 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.

La définition de limites de connexion peut protéger un serveur contre une attaque par inondation SYN. Vous pouvez éventuellement activer les statistiques TCP Intercept et surveiller les résultats de votre politique. La procédure suivante explique le processus de bout en bout.

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 de périphérique Cisco Secure Firewall Threat Defense, le nombre maximal de connexions simultanées et de connexions amorces peut dépasser les nombres configurés en raison de la façon dont chaque cœur gère les connexions. Dans le pire des cas, le périphérique autorise jusqu'à n-1 connexions supplémentaires et connexions amorces, 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** dans l'interface de ligne de commande du périphérique.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic, qui est la liste des serveurs que vous souhaitez protéger.

Par exemple, pour définir une classe de trafic afin de protéger les serveurs Web ayant les adresses IP 10.1.1.5 et 10.1.1.6 :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **Name** (nom) pour l'objet, par exemple, protected-servers.
e) Cliquez sur **Add** pour ajouter une nouvelle règle.
f) Conservez **Allow** (autorisation) pour l'action.
g) Laissez la liste **Source** vide, saisissez 10.1.1.5 sous la liste **Destination**, puis cliquez sur **Add** (Ajouter).
h) Saisissez également 10.1.1.6 sous la liste **Destination** et cliquez sur **Add** (Ajouter).
i) Cliquez sur **Port**, sélectionnez **HTTP** dans la liste des ports disponibles, puis cliquez sur **Add to Destination** (Ajouter à la destination). Si votre serveur prend également en charge les connexions HTTPS, ajoutez également ce port.
j) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.
k) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique de service qui définit les limites de connexion amorces.

Par exemple, pour définir la limite amorce totale simultanée à 1 000 connexions et la limite par client à 50 connexions, procédez comme suit :

a) Choisissez **Policies(Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** (✎) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally (appliquer globalement)** > **Next (suivant)** .
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next (Suivant).**
f) Saisissez 1 000 dans le champ**Connections** > **Maximum Embryronics** (Connexions amorces maximales).
g) Saisissez 50 dans le champ **Connections Per Client** > **Maximum Embryonic** (Connexions amorces maximales par client).
h) (Facultatif) Ajustez les autres options de connexion selon vos besoins.
i) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
j) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
k) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

Étape 3 (Facultatif) Configurez les débits pour les statistiques TCP Intercept.

TCP Intercept utilise les options suivantes pour déterminer le débit de collecte de statistiques. Toutes les options ont des valeurs par défaut, donc si ces fréquences répondent à vos besoins, vous pouvez ignorer cette étape.

- Rate Interval (intervalle de fréquence) : taille de la fenêtre de surveillance de l'historique, entre 1 et 1440 minutes. La valeur par défaut est de 30 minutes. Pendant cet intervalle, le système échantillonne le nombre d'attaques 30 fois.

- Fréquence de rafale (Burst Rate) : le seuil de 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.
- Fréquence moyenne : le seuil de débit moyen pour la génération de messages syslog, entre 25 et 2147483647. La valeur par défaut est de 200 par seconde. Lorsque le débit moyen est dépassé, le périphérique génère le message syslog 733105.

Si vous souhaitez modifier ces options, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **FlexConfig** > **Text Object** (Objet texte).
c) Cliquez sur **Edit** ( ) pour l'objet défini par le système threat_defense_statistics.
d) Bien que vous puissiez modifier directement les valeurs, l'approche recommandée est d'ouvrir la section **Override** (Remplacement) et de cliquer sur **Add** (Ajouter) pour créer un remplacement de périphérique.
e) Sélectionnez les périphériques auxquels vous affecterez la politique de service (grâce à l'affectation de la politique de contrôle d'accès) et cliquez sur **Add** (ajouter) pour les déplacer vers la liste sélectionnée.
f) Cliquez sur **Override** (Remplacer).
g) L'objet doit avoir trois entrées. Cliquez donc sur **Nombre** selon vos besoins jusqu'à ce que vous obteniez 3.
h) Saisissez les valeurs dont vous avez besoin, dans l'ordre de 1 à 3, comme intervalle de fréquence, la fréquence de rafale et la fréquence moyenne. Consultez la description de l'objet pour vérifier que vous saisissez les valeurs dans le bon ordre.
i) Cliquez sur **Add** (ajouter) dans la boîte de dialogue Object Override (Remplacer les objets).
j) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Edit Text Object (modifier l'objet texte).

Étape 4 Activer les statistiques TCP Intercept

Vous devez configurer une politique FlexConfig pour activer les statistiques TCP Intercept.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Si vous possédez déjà une politique affectée aux périphériques, modifiez-la. Sinon, créez une nouvelle politique et affectez-la aux périphériques concernés.
c) Sélectionnez l'objet **Threat_Detection_Configure** dans la liste **Available FlexConfig** (FlexConfig disponible) et cliquez sur **>>**. L'objet est ajouté à la liste **Selected Append FlexConfigs** (Ajouts sélectionnés FlexConfigs).
d) Cliquez sur **Save** (enregistrer).
e) (Facultatif) Vous pouvez vérifier que vous avez défini les bons paramètres en cliquant sur **Preview Config** (Aperçu de la configuration) et en sélectionnant l'un des périphériques.

Le système génère les commandes CLI qui seront écrites sur le périphérique lors du prochain déploiement. Ces commandes comprennent celles nécessaires pour la politique du service ainsi que celles nécessaires pour les statistiques de détection des menaces. Faites défiler l'aperçu vers le bas pour voir l'interface de ligne de commande en annexe. La commande des statistiques TCP Intercept devrait ressembler à ce qui suit, si vous utilisez les valeurs par défaut (saut de ligne ajouté pour plus de clarté) :

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

Étape 5 Vous devez déployer les modifications sur les périphériques concernés.

Étape 6 Surveillez les statistiques TCP Intercept à partir de l'interface de ligne de commande du périphérique à l'aide des commandes suivantes :

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] : Pour afficher 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. Le système 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 Vous pouvez utiliser la commande **shun** pour bloquer les adresses IP hôtes attaquantes. Pour supprimer le blocage, utilisez la commande **no shun**.

- **clear threat-detection statistics tcp-intercept** : pour effacer les statistiques TCP Intercept.

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)
```

Faire en sorte que le périphérique défense contre les menaces s'affiche sur Traceroutes

Par défaut, le périphérique défense contre les menaces n'apparaît pas sur les Traceroutes en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par le périphérique et augmenter la limite de débit pour les messages ICMP unreachable. Pour ce faire, vous devez configurer une règle de politique de service et ajuster la politique des paramètres de plateforme ICMP.

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 une TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues. Gardez ces considérations à l'esprit lorsque vous définissez votre classe de trafic.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic pour laquelle activer les rapports Traceroute.

Par exemple, pour définir une classe de trafic pour toutes les adresses, mais à l'exclusion du trafic OSPF, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **nom** pour l'objet, par exemple, traceroute-enabled.
e) Cliquez sur **Add** (ajouter) pour ajouter une règle et exclure OSPF.
f) Modifiez l'action pour **Block** (blocage), cliquez sur **Port** (port), sélectionnez **OSPFIGP (89)** comme protocole sous la liste **Destination Ports** (Ports de destination), puis cliquez sur **Add** pour ajouter le protocole à la liste sélectionnée.
g) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List entry (entrée de liste d'accès étendu) pour ajouter la règle OSPF à la liste d'accès (ACL).
h) Cliquez sur **Add** (ajouter) pour ajouter une règle afin d'inclure toutes les autres connexions.
i) Conservez **Allow** (autoriser) pour l'action et laissez les listes Source et Destination vides.
j) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.

   Assurez-vous que la règle de refus OSPF est supérieure à la règle Allow Any (autoriser tout). Glissez et déposez pour déplacer les règles si nécessaire.

k) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique de service qui décrémente la valeur de la durée de vie.

Par exemple, pour décrémenter la durée de vie globalement, procédez comme suit :

a) Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** (✎) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally** (appliquer globalement) et cliquez sur **Next** (suivant).
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next** (Suivant).
f) Sélectionnez **Activer le décrément du TTL**.
g) (Facultatif) Ajustez les autres options de connexion selon vos besoins.
h) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
i) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
j) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

   Vous devez déployer les modifications sur les périphériques concernés.

Étape 3 Augmenter la limite de débit pour les messages ICMP inaccessibles.

a) Choisissez **Devices (Périphériques)** > **Platform Settings (Paramètres de la plateforme)**.
b) Si vous possédez déjà une politique affectée aux périphériques, modifiez-la. Sinon, créez une nouvelle politique de paramètres de plateforme Threat Defense et affectez-la aux périphériques concernés.
c) Sélectionnez **ICMP** dans la table des matières.
d) Augmentez la **limite de débit**, par exemple, à 50. Vous pouvez également augmenter la **taille de la rafale**, par exemple à 10, pour vous assurer que suffisamment de réponses sont générées dans la limite de débit.

   Vous pouvez laisser le tableau des règles ICMP vide, il n'est pas lié à cette tâche.

e) Cliquez sur **Save** (enregistrer).

Étape 4 Vous devez déployer les modifications sur les périphériques concernés.

Surveillance des politiques de service

Vous pouvez surveiller les informations relatives à la politique de service à l'aide de l'interface de ligne de commande du périphérique. Voici quelques commandes utiles.

- **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 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. Le système 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.

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.