Politiques de préfiltrage et de préfiltre

À propos du préfiltrage

Le préfiltre est la première phase du contrôle d'accès, avant que le système n'effectue des évaluations plus exigeantes en ressources. Le préfiltrage est simple, rapide et précoce. Le préfiltre utilise des critères d'en-tête externe limités pour gérer rapidement le trafic. Comparez cela à l'évaluation ultérieure, qui utilise des en-têtes internes et possède des capacités d'inspection plus robustes.

Configurez le préfiltre afin d' :

- Améliorer les performances : plus vous excluez tôt le trafic qui ne nécessite pas d'inspection, mieux c'est. Vous pouvez utiliser un fastpath ou bloquer certains types de tunnels relais en texte brut en fonction de leurs en-têtes d'encapsulation externes, sans inspecter leurs connexions encapsulées. Améliorer les performances : vous pouvez accélérer ou bloquer toutes les autres connexions qui bénéficient d'un traitement anticipé.
- Adapter l'inspection approfondie au trafic encapsulé : vous pouvez modifier le zonage de certains types de tunnels afin de pouvoir gérer ultérieurement leurs connexions encapsulées en utilisant les mêmes critères d'inspection. Un changement de zonage est nécessaire, car après le préfiltre, le contrôle d'accès utilise les en-têtes internes.

À propos des règles du préfiltre

Le préfiltre est une fonctionnalité basée sur des politiques. Pour l'affecter à un périphérique, vous l'affectez à la politique de contrôle d'accès qui est affectée au périphérique.

Composants de la politique : règles et action par défaut

Dans une politique de préfiltre, les *règles de tunnel*, les *règles de préfiltre* et une *action par défaut* gèrent le trafic réseau :

- Règles de tunnel et de préfiltre : tout d'abord, les règles d'une politique de préfiltre gèrent le trafic dans l'ordre que vous spécifiez. Les règles de tunnel correspondent uniquement à des tunnels spécifiques et prennent en charge le changement de zonage. Les règles de préfiltre ont un éventail de contraintes plus large et ne prennent pas en charge le changement de zonage. Pour en savoir plus, consultez Règles de tunnel par rapport aux règles de préfiltre, à la page 2.
- Action par défaut (tunnels uniquement) : si un tunnel ne correspond à aucune règle, l'action par défaut le gère. L'action par défaut peut bloquer ces tunnels ou continuer le contrôle d'accès sur leurs connexions encapsulées individuelles. Vous ne pouvez pas modifier le zonage des tunnels avec l'action par défaut.

  Il n'y a pas d'action par défaut pour le trafic non encapsulé. Si une connexion non encapsulée ne correspond à aucune règle de préfiltre, le système poursuit le contrôle d'accès.

Journalisation des connexions

Vous pouvez consigner les connexions accélérées et bloquées par la politique de préfiltre.

Les événements de connexion contiennent des informations indiquant si et comment les connexions enregistrées, y compris des tunnels entiers, ont été préfiltrées. Vous pouvez afficher ces informations dans des vues d'événements (flux de travail), des tableaux de bord et des rapports, et les utiliser comme critères de corrélation. Gardez à l'esprit que, comme les connexions bloquées et les connexions accélérées ne sont pas soumises à une inspection approfondie, les événements de connexion associés contiennent des informations limitées.

Politique de préfiltre par défaut

Chaque politique de contrôle d'accès est associée à une politique de préfiltre.

Le système utilise une politique par défaut si vous ne configurez pas de préfiltre personnalisé. Au départ, cette politique fournie par le système transmet tout le trafic à la phase suivante de contrôle d'accès. Vous pouvez modifier l'action par défaut de la politique et configurer ses options de journalisation, mais vous ne pouvez pas y ajouter de règles ni la supprimer.

Héritage des politiques de préfiltre et multidétention

Le contrôle d'accès utilise une implémentation hiérarchique qui complète l'architecture multi-détenteur. Entre autres paramètres avancés, vous pouvez verrouiller une association de politiques de préfiltre, appliquant cette association dans toutes les politiques de contrôle d'accès descendantes. Pour en savoir plus, consultez Héritage de la politique de contrôle d'accès.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. La politique de préfiltre par défaut appartient au domaine global.

Règles de tunnel par rapport aux règles de préfiltre

La configuration d'une règle de tunnel ou de préfiltre dépend du type de trafic que vous souhaitez mettre en correspondance et des actions ou de l'analyse plus approfondie que vous souhaitez effectuer.

Caractéristiques	Règles de tunnel	Règles du préfiltre
Fonction principale	Fastpath, blocage ou changement de zonage en texte brut, tunnels d'intercommunication.	Vous pouvez rapidement accélérer le trafic ou bloquer toute autre connexion bénéficiant d'un traitement anticipé.
Critères d'encapsulation et de port/protocole	Les conditions d'encapsulation correspondent uniquement aux tunnels de texte en clair sur les protocoles sélectionnés, répertoriés dans Conditions des règles d'encapsulation, à la page 15.	Les conditions de port peuvent utiliser un éventail plus large de contraintes de port et de protocole que les règles de tunnel; voir Conditions de règle de port, de protocole et de code ICMP.
Critères de réseau	Les conditions de point terminal du tunnel contraignent les points terminaux des tunnels que vous souhaitez gérer; voir Conditions des règles de réseau.	Les conditions du réseau limitent les hôtes source et de destination dans chaque connexion. voir Conditions des règles de réseau.
Direction	Bidirectionnel ou unidirectionnel (configurable). Les règles de tunnel sont bidirectionnelles par défaut, de sorte qu'elles peuvent gérer tout le trafic entre les points de terminaison du tunnel.	Unidirectionnel seulement (non configurable). Les règles de préfiltre correspondent uniquement au trafic de la source à la destination.
Sessions de modification de zone pour une analyse plus approfondie	Pris en charge, utilisation de zones de tunnel; voir Zones de tunnel et préfiltrage, à la page 15.	Non pris en charge.

Préfiltrage ou contrôle d'accès

Les politiques de préfiltre et de contrôle d'accès vous permettent tous deux de bloquer et de faire confiance au trafic, bien que la fonctionnalité de « confiance » de préfiltre soit appelée « fastpathing » car elle saute davantage d'inspections. Le tableau suivant explique cela et d'autres différences entre le préfiltre et le contrôle d'accès, pour vous aider à décider s'il faut configurer le préfiltrage personnalisé.

Si vous ne configurez pas le préfiltre personnalisé, vous ne pouvez qu'approcher la fonctionnalité de préfiltre, et non la reproduire, grâce aux règles de blocage et de confiance placées tôt dans la politique de contrôle d'accès.

Caractéristiques	Préfiltrage	Contrôle d'accès	Pour plus de renseignements, consultez...
Fonction principale	Fastpath ou blocage rapide de certains types de textes en clair, tunnels d'intercommunication (voir Conditions des règles d'encapsulation, à la page 15), ou adapter l'inspection ultérieure à leur trafic encapsulé. Accélérez ou bloquez toutes les autres connexions qui bénéficient d'un traitement anticipé.	Inspectez et contrôlez l'ensemble du trafic réseau à l'aide de critères simples ou complexes, notamment des informations contextuelles et les résultats d'une inspection approfondie.	À propos du préfiltrage, à la page 1
Mise en œuvre	Politique de préfiltre. La politique de préfiltre est appelée par la politique de contrôle d'accès.	Politique de contrôle d'accès. La politique de contrôle d'accès est une configuration principale. En plus d'appeler des sous-politiques, les politiques de contrôle d'accès ont leurs propres règles.	À propos des règles du préfiltre, à la page 1 Association d'autres politiques au contrôle d'accès
Séquence dans le contrôle d'accès	Tout d'abord. Le système fait correspondre le trafic aux critères du préfiltre avant toutes les autres configurations de contrôle d'accès.	—	—
Actions découlant d'une règle	Moins souvent. Vous pouvez interrompre la poursuite de l'inspection (Fastpath et Blocking) ou autoriser une analyse plus approfondie avec le reste du contrôle d'accès (Analyze).	Autre. Les règles de contrôle d'accès ont une plus grande variété d'actions, y compris la surveillance, l'inspection approfondie, le blocage avec réinitialisation et le blocage interactif.	Composants de la règle de tunnel et de préfiltre, à la page 10 Actions de règles de contrôle d'accès

Caractéristiques	Préfiltrage	Contrôle d'accès	Pour plus de renseignements, consultez...
Capacité de contournement	Action de la règle Fastpath Le trafic d'acheminement rapide à l'étape de préfiltre contourne toute inspection et tout traitement ultérieurs, notamment : • Renseignements de sécurité • les exigences d'authentification imposées par une politique d'identité • Déchiffrement SSL • Règles de contrôle d'accès • inspection approfondie des charges utiles de paquets • Découverte • limitation de débit	Action de la règle Trust (confiance). Le trafic approuvé par les règles de contrôle d'accès est uniquement exempté de l'inspection et de la découverte approfondies.	Introduction aux règles de contrôle d'accès
Critères de règle	Limités. Les règles de la politique de préfiltre utilisent des critères de réseau simples : adresse IP, balise VLAN, port et protocole. Pour les tunnels, les conditions de point terminal du tunnel précisent l'adresse IP des interfaces routées des périphériques réseau de chaque côté du tunnel.	Robuste. Les règles de contrôle d'accès utilisent des critères de réseau, mais aussi sur l'utilisateur, l'application, l'URL demandée et d'autres informations contextuelles disponibles dans les charges utiles de paquets. Les conditions du réseau précisent l'adresse IP des hôtes source et de destination.	Règles de tunnel par rapport aux règles de préfiltre, à la page 2 Conditions des règles de préfiltre, à la page 12 Conditions des règles de tunnel, à la page 15
En-têtes IP utilisés (gestion du tunnel)	Le plus à l'extérieur. L'utilisation d'en-têtes externes vous permet de gérer l'ensemble des tunnels d'intercommunication en texte brut. Pour le trafic non encapsulé, le préfiltre utilise toujours des en-têtes « externes », qui dans ce cas sont les seuls en-têtes.	Le plus possible à l'intérieur. Pour un tunnel non chiffré, le contrôle d'accès agit sur ses connexions encapsulées individuelles, et non sur le tunnel dans son ensemble.	Tunnels intermédiaires (Passthrough) et contrôle d'accès, à la page 6

Caractéristiques	Préfiltrage	Contrôle d'accès	Pour plus de renseignements, consultez...
Rezonage des connexions encapsulées en vue d'une analyse plus approfondie	Rezonage du trafic tunnelisé. Les zones de tunnel vous permettent d'adapter l'inspection ultérieure au trafic préfiltré et encapsulé.	Utilise des zones de tunnel. Le contrôle d'accès utilise les zones de tunnel que vous affectez lors du préfiltre.	Zones de tunnel et préfiltrage, à la page 15
Journalisation des connexions	Uniquement pour le trafic en accès rapide et le trafic bloqué. Les connexions autorisées peuvent toujours être enregistrées par d'autres configurations.	Toute connexion.	
Périphériques pris en charge	Cisco Secure Firewall Threat Defense uniquement.	Tous	—

Tunnels intermédiaires (Passthrough) et contrôle d'accès

Les tunnels en texte brut (non chiffrés) peuvent encapsuler plusieurs connexions, circulant souvent entre des réseaux discontinus. Ces tunnels sont particulièrement utiles pour acheminer les protocoles personnalisés sur les réseaux IP, le trafic IPv6 sur les réseaux IPv4, etc.

Un *en-tête d'encapsulation* externe spécifie les adresses IP de source et de destination des *points terminaux du tunnel*, c'est-à-dire les interfaces routées des périphériques réseau de chaque côté du tunnel. Les *en-têtes de charge utile internes* précisent les adresses IP de source et de destination des points terminaux réels des connexions encapsulées.

Souvent, les périphériques de sécurité réseau gèrent les tunnels de texte en clair comme trafic *d'intercommunication*. C'est-à-dire que le périphérique ne fait pas partie des points terminaux du tunnel. Au lieu de cela, il est déployé entre les points terminaux du tunnel et surveille le trafic circulant entre eux.

Certains périphériques de sécurité réseau mettent en œuvre des politiques de sécurité à l'aide d'en-têtes IP externes. Même pour les tunnels de texte en clair, ces périphériques n'ont aucun contrôle sur les connexions encapsulées individuelles et leurs charges utiles.

En revanche, le système utilise le contrôle d'accès comme suit :

- Évaluation de l'en-tête externe : tout d'abord, le préfiltre utilise des en-têtes externes pour gérer le trafic. Vous pouvez bloquer ou parcourir les tunnels en texte brut entier ou d'intercommunication en texte brut à ce stade.
- Évaluation des en-têtes internes : ensuite, le reste du contrôle d'accès (et d'autres fonctionnalités telles que QoS) utilise le niveau détectable le plus à l'intérieur des en-têtes pour assurer le niveau d'inspection et de traitement le plus fin possible.

  Si un tunnel d'intercommunication n'est pas chiffré, le système agit sur ses connexions encapsulées individuelles à ce stade. Vous devez *modifier le zonage* d'un tunnel (voir Zones de tunnel et préfiltrage, à la page 15) pour agir sur toutes ses connexions encapsulées.

Le contrôle d'accès n'a aucun aperçu des tunnels d'intercommunication chiffrés. Par exemple, les règles de contrôle d'accès considèrent un tunnel VPN d'intercommunication comme une seule connexion. Le système gère l'ensemble du tunnel en utilisant uniquement les informations de son en-tête d'encapsulation externe.

Bonnes pratiques de préfiltrage Fastpath

Lorsque vous utilisez l'action fastpath dans une règle de préfiltre, le trafic correspondant contourne l'inspection et est simplement transmis par le périphérique. Utilisez cette action pour le trafic en qui vous pouvez avoir confiance et qui ne bénéficierait d'aucune des fonctionnalités de sécurité disponibles.

Les types de trafic suivants sont idéaux pour le cheminement rapide fastpath. Par exemple, vous pouvez configurer les règles pour activer le routage rapide de tout trafic en provenance ou à destination des adresses IP des points terminaux ou des serveurs. Vous pouvez limiter davantage la règle en fonction des ports utilisés.

- Le trafic VPN qui passe par le périphérique. C'est-à-dire que le périphérique n'est pas un point terminal dans la topologie VPN.
- Trafic de l'analyseur. Les sondes de l'analyseur peuvent créer un grand nombre de faux positifs à partir des politiques de prévention des intrusions.
- Voix/vidéo.
- Sauvegardes.
- Trafic de gestion (sftunnel) qui traverse les périphériques défense contre les menaces . L'inspection approfondie du trafic de gestion (à l'aide de politiques de contrôle d'accès) peut entraîner des problèmes. Vous pouvez préfiltrer en fonction du port TCP/8305 entre le centre de gestion et les périphériques gérés.

Bonnes pratiques de gestion du trafic encapsulé

Cette rubrique traite des directives pour les types de trafic encapsulé suivants :

- Generic Routing Encapsulation (GRE) (Encapsulation de routage générique)
- Protocole point à point (PPP)
- IPinIP
- IPv6inIP
- Teredo

Limites du tunnel GRE

Le traitement du tunnel GRE est limité aux flux IPv4 et IPv6. Les autres protocoles, tels que PPTP etWCCP, ne sont pas pris en charge dans le tunnel GRE.

Comprendre la prise en charge des versions du Snort pour vos périphériques gérés

Le moteur d'inspection utilisé par les périphériques gérés s'appelle Snort. Snort 3 prend en charge plus de fonctionnalités que Snort 2. Pour comprendre leur incidence sur les périphériques gérés de votre réseau, vous devez connaître :

- les versions de Snort prises en charge par votre appareil.

  La prise en charge des versions de Snort est indiquée dans la section sur les composants groupés dans le *Guide de compatibilité Cisco Firepower*.

- Comment les logiciels centre de gestion et défense contre les menaces prennent en charge Snort 2 et Snort 3

  Les limites de Snort 2 et de Snort 3 peuvent être trouvées dans les *limites des fonctionnalités de Snort 3 pour les versions gérées Centre de gestionDéfense contre les menaces* dans Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

GRE v1 et PPTP contournent le traitement du flux externe

Le trafic GRE v1 (parfois appelé *GRE dynamique*) et PPTP contournent le traitement du flux externe.

Le traitement des flux de Passagers est pris en charge pour IPv6inIP et Teredo, mais les limites suivantes s'appliquent :

- Les sessions ont lieu dans un tunnel unique qui n'est pas équilibré
- Il n'y a pas de duplication de la haute disponibilité ou en grappe
- Les relations de flux principal et secondaire ne sont pas conservées
- Les listes blanche et noire des politiques de préfiltre ne sont pas prises en charge

Le champ du numéro de séquence de GRE v0 doit être facultatif.

Tous les points terminaux envoyant du trafic sur le réseau doivent envoyer le trafic GRV0 avec le champ de numéro de séquence facultatif; sinon, le champ du numéro de séquence est supprimé. La RFC 1701 et la RFC 2784 précisent toutes deux le champ de séquence comme facultatif.

Les tunnels fonctionnent avec des interfaces

Les règles de politiques de préfiltre et de contrôle d'accès sont appliquées à tous les types de tunnels sur les interfaces routée, transparente, en ligne-ensemble, en ligne-tap et passive.

Références

Pour en savoir plus sur les protocoles GRE et PPTP, consultez les pages suivantes :

- RFC 1701, RFC 2784 et RFC 2890 (protocole GRE v0)
- RFC 2637 (protocole PPTP et GRE v1)

Exigences et conditions préalables pour les politiques de préfiltre

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

Configurer le préfiltrage

Pour effectuer un préfiltrage personnalisé, configurez les politiques de préfiltre et affectez les politiques aux politiques de contrôle d'accès. C'est par l'intermédiaire de la politique de contrôle d'accès que les politiques de préfiltre sont affectées aux périphériques gérés.

Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées. Pour votre commodité, le système affiche des informations sur la personne qui (le cas échéant) modifie actuellement chaque politique. Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control** > **Prefilter (préfiltrer)**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique) pour créer une politique de préfiltre personnalisée.

Une nouvelle politique de préfiltre n'a aucune règle et une action par défaut Analyze all tunnel traffic (Analyse de tout le trafic de tunnel). Il n'effectue aucune journalisation ni modification de zonage de tunnel. Vous pouvez également **Copier** ( ) ou **Edit** ( ) une politique existante.

Étape 3 Configurez l'action par défaut de la politique de préfiltre et ses options de journalisation.

- Default action (action par défaut) : choisissez une action par défaut pour les tunnels de texte en clair ou d'intercommunication pris en charge : **analyser tout le trafic des tunnels** (avec contrôle d'accès) ou **Bloquer tout le trafic des tunnels**.
- Journalisation des actions par défaut : cliquez sur **Se connecter** ( ) à côté de l'action par défaut. Vous pouvez configurer la journalisation des actions par défaut pour les tunnels bloqués uniquement.

Étape 4 Configurez les règles de tunnel et de préfiltre.

Dans une politique de préfiltre personnalisée, vous pouvez utiliser les deux types de règles, dans n'importe quel ordre. Créer des règles en fonction du type spécifique de trafic que vous souhaitez mettre en correspondance et des actions ou de l'analyse plus approfondie que vous souhaitez effectuer; voir Règles de tunnel par rapport aux règles de préfiltre, à la page 2.

Mise en garde Faites preuve de prudence lorsque vous utilisez des règles de tunnel pour affecter des zones de tunnel. Les connexions dans les tunnels dézonés pourraient ne pas correspondre aux contraintes des zones de sécurité lors d'une évaluation ultérieure. Pour en savoir plus, consultez Zones de tunnel et préfiltrage, à la page 15.

Pour en savoir plus sur la configuration des composants de règle, consultez Composants de la règle de tunnel et de préfiltre, à la page 10.

Étape 5 Évaluer l'ordre des règles. Pour déplacer une règle, cliquez et faites glisser ou utilisez le menu contextuel pour couper et coller.

Créer et ordonner correctement des règles est une tâche complexe, mais essentielle à la mise en place d'un déploiement efficace. Si vous n'effectuez pas une planification rigoureuse, les règles peuvent prévaloir sur d'autres règles ou contenir des configurations non valides. Pour en savoir plus, consultez Bonnes pratiques pour les règles de contrôle d'accès.

Étape 6 Enregistrer la politique de préfiltre.

Étape 7 Pour les configurations qui prennent en charge les contraintes de zone de tunnel, gérez correctement les tunnels dézonés.

Faire correspondre les connexions dans les tunnels dézonés en utilisant les zones de tunnel comme contraintes de zone source.

Étape 8 Associer la politique de préfiltre à la politique de contrôle d'accès déployée sur vos périphériques gérés.

Consultez Association d'autres politiques au contrôle d'accès.

Étape 9 Déployer les changements de configuration.

Remarque Lorsque vous déployez une politique de préfiltre, ses règles ne sont pas appliquées aux sessions de tunnel existantes. Par conséquent, le trafic sur une connexion existante n'est pas lié par la nouvelle politique déployée. En outre, le nombre de résultats de politique est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une politique. Ainsi, le trafic sur une connexion existante qui pourrait correspondre à une politique est omis du nombre de résultats. Pour que les règles de la politique soient appliquées efficacement, effacez les sessions de tunnel existantes, puis déployez la politique.

Prochaine étape

Si vous déployez des règles basées sur le temps, spécifiez le fuseau horaire du périphérique auquel la politique est attribuée. Consultez Fuseau horaire.

Composants de la règle de tunnel et de préfiltre

State Enabled/Disabled (État Activé/Désactivé)

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle à laquelle le trafic correspond est la règle qui traite ce trafic, quel que soit le type de règle (tunnel ou préfiltre).

Action

L'action découlant d'une règle détermine comment le système traite et enregistre le trafic correspondant.

- Fastpath : exempte le trafic correspondant de toute inspection et de tout contrôle supplémentaires, y compris le contrôle d'accès, les exigences d'identité et la limitation de débit. Le Fastpathing d'un tunnel met en route toutes les connexions encapsulées.
- Block (Bloquer) : bloque le trafic correspondant sans autre inspection d'aucune sorte. Le blocage d'un tunnel bloque toutes les connexions encapsulées.
- Analyze (analyser) : permet au trafic de continuer à être analysé par le reste du contrôle d'accès, à l'aide d'en-têtes internes. S'il passe par le contrôle d'accès et toute inspection approfondie connexe, ce trafic peut également être limité en débit. Pour les règles de tunnel, active le changement de zonage avec l'option Affecter une zone de tunnel.

Direction (règles de tunnel seulement)

La direction d'une règle de tunnel détermine la façon dont les critères de source et de destination du système :

- Apparient les tunnels uniquement à partir de la source (unidirectionnel) : font correspondre le trafic de source à destination uniquement. Le trafic correspondant doit provenir de l'une des interfaces source ou de l'un des points terminaux du tunnel spécifiés et quitter par l'une des interfaces de destination ou des points terminaux du tunnel.
- Mettre en correspondance les tunnels de la source et de la destination (bidirectionnel) : mettre en correspondance le trafic de la source à destination et le trafic de la destination à la source. L'effet est identique à l'écriture de deux règles unidirectionnelles, l'une miroir de l'autre.

Les règles de préfiltre sont toujours unidirectionnelles.

Attribuer une zone de tunnel (règles de tunnel uniquement)

Dans une règle de tunnel, l'affectation d'une zone de tunnel (qu'elle soit existante ou créée à la volée) *change le zonage* des tunnels correspondants. Le changement de zonage nécessite l'action Analyze (Analyse).

Le rezonage d'un tunnel permet à d'autres configurations, telles que les règles de contrôle d'accès, de reconnaître toutes les connexions encapsulées du tunnel comme faisant partie d'un même ensemble. En utilisant la zone de tunnel attribuée à un tunnel comme contraintes d'interface, vous pouvez adapter l'inspection à ses connexions encapsulées. Pour en savoir plus, consultez Zones de tunnel et préfiltrage, à la page 15.

Mise en garde Faites preuve de prudence lorsque vous affectez des zones de tunnel. Les connexions dans les tunnels dézonés pourraient ne pas correspondre aux contraintes des zones de sécurité lors d'une évaluation ultérieure. Consultez Utilisation des zones de tunnel, à la page 16 pour obtenir une brève procédure pas à pas d'une implémentation de zone de tunnel et une discussion sur les conséquences du changement de zonage sans gérer explicitement le trafic dézoné.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Le trafic doit correspondre à toutes les conditions d'une règle pour correspondre à la règle. Chaque type de condition a son propre onglet dans l'éditeur de règles.

Vous pouvez préfiltrer le trafic en utilisant les contraintes *d'en-tête externe* suivantes. Vous devez contraindre les règles de tunnel par protocole d'encapsulation.

- Interface : Conditions des règles d'interface
- Réseau (règle de préfiltre)/Points de terminaison du tunnel (règle de tunnel) : Conditions des règles de réseau
- VLAN Conditions de règle des balises VLAN
- Ports (règle de préfiltre)/encapsulation et ports (règle de tunnel) : Conditions de règle de port pour les règles de préfiltre, à la page 14 ou Conditions des règles d'encapsulation, à la page 15
- plage temporelle : Conditions des règles de date et d'heure

Logging (journalisation)

Les paramètres de journalisation d'une règle régissent les enregistrements que le système conserve du trafic qu'il gère.

Dans les règles de tunnel et de préfiltre, vous pouvez consigner le trafic accéléré et bloqué (les actions Fastpath et Block). Pour le trafic soumis à une analyse plus approfondie (l'action Analyze), la journalisation dans la politique de préfiltre est désactivée, bien que les connexions correspondantes puissent toujours être journalisées par d'autres configurations. La journalisation est effectuée sur les flux internes, et non sur le flux d'encapsulation.

Commentaires

Chaque fois que vous enregistrez des modifications à une règle, vous pouvez ajouter des commentaires. Par exemple, vous pouvez résumer la configuration globale à l'intention des autres utilisateurs, ou indiquer quand vous modifiez une règle et la raison de cette modification.

Vous ne pouvez pas modifier ou supprimer ces commentaires après avoir enregistré la règle.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès

Conditions des règles de préfiltre

Les conditions de règles vous permettent d'affiner votre politique de préfiltre pour cibler les réseaux que vous souhaitez contrôler. Voir l'une des sections suivantes pour plus d'informations.

Conditions des règles d'interface

Les conditions de règles d'interface contrôlent le trafic en fonction de ses interfaces de source et de destination.

Selon le type de règle et les périphériques de votre déploiement, vous pouvez utiliser des *objets d'interface* prédéfinis appelés *zones de sécurité* ou des *groupes d'interface* pour créer des conditions d'interface. Les objets d'interface segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques: consultez Interface.

Astuces Restreindre les règles par interface est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle exclut toutes les interfaces d'un périphérique, cette règle n'affecte pas les performances de ce périphérique.

Tout comme toutes les interfaces d'un objet d'interface doivent être du même type (en ligne, passive, commutée, routée ou ASA FirePOWER), tous les objets d'interface utilisés dans une condition d'interface doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas de trafic, dans les déploiements passifs, vous ne pouvez pas restreindre les règles par interface de destination.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :

- Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
- Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions de règle de port pour les règles de préfiltre

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent à d'autres protocoles dans les règles de préfiltre, vous devez plutôt utiliser des règles de tunnel pour la mise en correspondance de GRE, IP dans IP, IPv6 dans IP et du port Toredo 3544.

Conditions des règles de date et d'heure

Vous pouvez spécifier une plage temporelle continue ou une période récurrente.

Par exemple, une règle ne peut s'appliquer que pendant les heures de travail en semaine, chaque fin de semaine ou pendant une période d'arrêt pendant un jour férié.

Les règles basées sur le temps sont appliquées en fonction de l'heure locale du périphérique qui traite le trafic.

Les règles basées sur le temps sont prises en charge uniquement sur les périphériques FTD. Si vous affectez une politique avec une règle basée sur le temps à un autre type de périphérique, la restriction de temps associée à la règle est ignorée sur ce périphérique. Vous verrez des avertissements dans ce cas.

Conditions des règles de tunnel

Les conditions de règles vous permettent d'affiner votre politique de tunnel pour cibler les réseaux que vous souhaitez contrôler. Pour les règles de tunnel, vous pouvez utiliser les conditions suivantes :

- **Interface Objects** (Objets d'interface) : les zones de sécurité ou groupes d'interfaces qui définissent les interfaces de périphériques par lesquelles passent les connexions. Consultez Conditions des règles d'interface.
- **Tunnel Endpoints** (points terminaux de tunnel) : les objets réseau qui définissent les adresses IP de source et de destination du tunnel.
- **VLAN Tags** (Balises VLAN) : la balise VLAN la plus à l'extérieur du tunnel. Consultez Conditions de règle des balises VLAN.
- **Encapsulation and Ports**(Encapsulation et ports) : protocole d'encapsulation du tunnel. Consultez Conditions des règles d'encapsulation, à la page 15.
- **Time range** (plage temporelle) : jours et heures pendant lesquels la règle est active. Si vous ne spécifiez pas de plage temporelle, la règle est toujours active. Consultez Conditions des règles de date et d'heure.

Conditions des règles d'encapsulation

Les conditions d'encapsulation sont spécifiques aux règles de tunnellisation.

Ces conditions contrôlent certains types de tunnels directs en texte brut par leur protocole d'encapsulation. Vous devez choisir au moins un protocole à mettre en correspondance avant de pouvoir enregistrer la règle. À vous de choisir :

- GRE (47)
- IP-en-IP (4)
- IPv6-dans-IP (41)
- Teredo (UDP (17)/3455)

Zones de tunnel et préfiltrage

Les zones de tunnel vous permettent d'utiliser le préfiltrage pour adapter le traitement ultérieur du trafic aux connexions encapsulées.

Un mécanisme spécial est nécessaire car, en général, le système traite le trafic en utilisant le niveau d'en-tête détectable le plus interne. Cela garantit le niveau d'inspection le plus fin possible. Mais cela signifie également que si un tunnel relais passthrough n'est pas chiffré, le système agit sur ses connexions encapsulées individuelles; voir Tunnels intermédiaires (Passthrough) et contrôle d'accès, à la page 6.

Les zones de tunnel résolvent ce problème. Pendant la première phase de contrôle d'accès (préfiltre), vous pouvez utiliser des en-têtes externes pour identifier certains types de tunnels passthrough en texte brut. Ensuite, vous pouvez modifier le *zonage* de ces tunnels en attribuant une *zone de tunnel* personnalisée.

Le rezonage d'un tunnel permet à d'autres configurations, telles que les règles de contrôle d'accès, de reconnaître toutes les connexions encapsulées du tunnel comme faisant partie d'un même ensemble. En utilisant la zone de tunnel attribuée à un tunnel comme contraintes d'interface, vous pouvez adapter l'inspection à ses connexions encapsulées.

Malgré son nom, une zone de tunnel n'est pas une zone de sécurité. Une zone de tunnel ne représente pas un ensemble d'interfaces. Il est plus juste de considérer une zone de tunnel comme une balise qui, dans certains cas, remplace la zone de sécurité associée à une connexion encapsulée.

Mise en garde Pour les configurations qui prennent en charge les contraintes de zone de tunnel, les connexions dans les tunnels dézonés ne correspondent **pas** aux contraintes de zone de sécurité. Par exemple, après le changement de zonage d'un tunnel, les règles de contrôle d'accès peuvent faire correspondre ses connexions encapsulées à la zone *de tunnel* nouvellement attribuée, mais pas à une zone de *sécurité* d'origine.

Consultez Utilisation des zones de tunnel, à la page 16 pour obtenir une brève procédure pas à pas d'une implémentation de zone de tunnel et une discussion sur les conséquences du changement de zonage sans gérer explicitement le trafic dézoné.

Configurations prenant en charge les contraintes de zone de tunnel

Seules les règles de contrôle d'accès prennent en charge les contraintes de zone de tunnel.

Aucune autre configuration ne prend en charge les contraintes de zone de tunnel. Par exemple, vous ne pouvez pas utiliser la QoS pour limiter le débit d'un tunnel de texte brut dans son ensemble; vous ne pouvez limiter le débit que de ses sessions encapsulées individuelles.

Utilisation des zones de tunnel

Cet exemple de procédure résume comment vous pourriez modifier le zonage de tunnels GRE pour une analyse plus approfondie, à l'aide des zones de tunnel. Vous pouvez adapter les concepts décrits dans cet exemple à d'autres scénarios dans lesquels vous devez adapter l'inspection du trafic aux connexions encapsulées dans des tunnels d'intercommunication (passthrough) en texte brut.

Imaginez une situation dans laquelle le trafic interne de votre organisation traverse la zone de sécurité de confiance. La zone de sécurité de confiance représente un ensemble d'interfaces sur plusieurs périphériques gérés déployés à divers emplacements. La politique de sécurité de votre organisation exige que vous autorisiez le trafic interne après une inspection approfondie des exploits et des programmes malveillants.

Le trafic interne comprend parfois des tunnels de texte en clair, de transmission directe et GRE entre des points terminaux particuliers. Comme le profil de trafic de ce trafic encapsulé est différent de votre activité interservices « normale » (il peut être connu et inoffensif), vous pouvez limiter l'inspection de certaines connexions encapsulées tout en respectant votre politique de sécurité.

Dans cet exemple, après avoir déployé les modifications de configuration :

- Les connexions d'intercommunication encapsulées individuelles pour les tunnels encapsulés GRE en texte brut détectés dans la zone de confiance sont évaluées par un seul ensemble de politiques de prévention des intrusions et de fichiers.
- Tout autre trafic dans la zone de confiance est évalué avec un ensemble différent de politiques de fichiers et de prévention des intrusions.

Vous effectuez cette tâche en modifiant le *zonage* des tunnels GRE. Le changement de zonage garantit que le contrôle d'accès associe les connexions encapsulées GRE à une zone de *tunnel* personnalisée, plutôt qu'à leur zone de *sécurité* de confiance d'origine. Un changement de zonage est nécessaire en raison de la façon dont le contrôle d'accès gère le trafic encapsulé; voir Tunnels intermédiaires (Passthrough) et contrôle d'accès, à la page 6 et Zones de tunnel et préfiltrage, à la page 15.

Procédure

Étape 1 Configurez des politiques de prévention des intrusions et de fichiers personnalisées qui adaptent l'inspection approfondie au trafic encapsulé, et un autre ensemble de politiques de prévention des intrusions et de fichiers adapté au trafic non encapsulé.

Étape 2 Configurez le préfiltrage personnalisé pour modifier le zonage des tunnels GRE traversant la zone de sécurité de confiance.

Créez une politique de préfiltre personnalisée et associez-la au contrôle d'accès. Dans cette politique de préfiltre personnalisée, créez une règle de tunnel (dans cet exemple, **`GRE_tunnel_rezone`**) et une zone de tunnel correspondante (**`GRE_tunnel`**). Pour en savoir plus, consultez Configurer le préfiltrage, à la page 9.

Tableau 1 : Règle de tunnel GRE_tunnel_rezone

Composant de règle	Description
Condition de l'objet d'interface	Faites correspondre les tunnels internes uniquement en utilisant la zone de sécurité de confiance comme contraintes d'objet d'interface source et d'objet d'interface de destination.
Condition du point terminal de tunnel	Précisez les points terminaux source et de destination des tunnels GRE utilisés dans votre organisation. Les règles de tunnel sont bidirectionnelles par défaut. Si vous ne modifiez pas l'option **Faire correspondre les tunnels de...**, les points terminaux que vous indiquez comme source et ceux que vous indiquez comme destination n'ont pas d'importance.
Conditions d'encapsulation	Mettre en correspondance le trafic GRE.
Affecter une zone de tunnel	Créez la zone de tunnel **`GRE_tunnel`** et affectez-la aux tunnels qui correspondent à la règle.
Action	Analyse (avec le reste du contrôle d'accès).

Étape 3 Configurez le contrôle d'accès pour gérer les connexions dans les tunnels dézonés.

Dans la politique de contrôle d'accès déployée sur vos périphériques gérés, configurez une règle (dans cet exemple, **`GRE_inspection`**) qui gère le trafic dont vous avez modifié la zone. Pour en savoir plus, consultez Créer et modifier les règles de contrôle d'accès.

Tableau 2 : Règle de contrôle d'accès GRE_inspection

Composant de règle	Description
Condition de la zone de sécurité	Faites correspondre les tunnels dézonés en utilisant la zone de sécurité GRE_tunnel comme contraintes de zone source.
Action	Autoriser, avec inspection approfondie activée. Choisissez les politiques de fichiers et de prévention des intrusions adaptées pour inspecter le trafic interne encapsulé.

Mise en garde Si vous ignorez cette étape, les connexions dézonées peuvent correspondre à **toute** règle de contrôle d'accès non limitée par la zone de sécurité. Si les connexions dézonées ne correspondent à aucune règle de contrôle d'accès, elles sont gérées par l'action par défaut de la politique de contrôle d'accès. Assurez-vous qu'il s'agit bien de votre intention.

Étape 4 Configurez le contrôle d'accès pour gérer les connexions non encapsulées passant dans la zone de sécurité de confiance.

Dans la même politique de contrôle d'accès, configurez une règle (dans cet exemple, **`internal_default_inspection`**) qui gère le trafic non dézoné dans la zone de sécurité de confiance.

Tableau 3 : Règle de contrôle d'accès internal_default_inspection

Composant de règle	Description
Condition de la zone de sécurité	Faites correspondre le trafic interne uniquement hors rezonage en utilisant la zone de sécurité de confiance comme contraintes de zone source et de zone de destination.
Action	Autoriser, avec inspection approfondie activée. Choisissez les politiques de fichiers et de prévention des intrusions adaptées pour inspecter le trafic interne non encapsulé.

Étape 5 Évaluez la position des nouvelles règles de contrôle d'accès par rapport aux règles préexistantes. Modifiez l'ordre des règles si nécessaire.

Si vous placez les deux nouvelles règles de contrôle d'accès l'une à côté de l'autre, peu importe celle que vous mettez en premier. Puisque vous avez redéfini le zonage des tunnels GRE, les deux règles ne peuvent pas se remplacer l'une l'autre.

Étape 6 Enregistrez toutes les configurations modifiées.

Prochaine étape

- Déployer les changements de configuration.

Création de zones de tunnel

La procédure suivante explique comment créer une zone de tunnel dans le gestionnaire d'objets. Vous pouvez également créer des zones lors de la modification d'une règle de tunnel.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Tunnel Zone** (Zone de tunnel) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Tunnel Zone** (Ajouter une zone de tunnel).

Étape 4 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- affecter des zones de tunnel aux tunnels passthrough (d'intercommunication) en texte brut dans le cadre du préfiltrage personnalisé; voir Configurer le préfiltrage, à la page 9.

Déplacement des règles de préfiltre vers une politique de contrôle d'accès

Vous pouvez déplacer des règles de préfiltre d'une politique de préfiltre vers la politique de contrôle d'accès associée.

Avant de commencer

Prenez note des conditions suivantes avant de continuer :

- Seules les règles de préfiltre peuvent être déplacées vers une politique de contrôle d'accès. Les règles de tunnel ne peuvent pas être déplacées.
- Les règles de préfiltre peuvent être déplacées uniquement vers la politique de contrôle d'accès associée.
- Les règles de préfiltre avec les groupes d'interface configurés ne peuvent pas être déplacées.
- Le paramètre **Action** de la règle de préfiltre est remplacé par une action appropriée dans la règle de contrôle d'accès lors du déplacement. Pour savoir à quoi correspond chaque action de la règle de préfiltre, consultez le tableau suivant :

Action de la règle de préfiltre	Action de la règle de contrôle d'accès
Analyser	Autoriser
Bloquer	Bloquer
Chemin d'accès rapide	Confiance

- De même, en fonction de l'action configurée dans la règle de préfiltre, la configuration de la journalisation est définie sur un paramètre approprié après le déplacement de la règle, comme l'indique le tableau suivant.

Action de la règle de préfiltre	Configurations de journalisation activées dans la règle de contrôle d'accès
Analyser	Aucun des paramètres de journalisation n'est activé.
Bloquer	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Chemin d'accès rapide	• Journaliser au début de la connexion • Journaliser à la fin de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP

- Les commentaires dans la configuration de la règle de préfiltre sont perdus après le déplacement de la règle. Cependant, un nouveau commentaire est ajouté dans la règle déplacée mentionnant la politique de préfiltre source.
- Lors du déplacement de règles de la politique source, si un autre utilisateur modifie ces règles, la console FMC affiche un message. Vous pouvez continuer le processus après avoir actualisé la page.

Procédure

Étape 1 Dans l'éditeur de politique de préfiltre, sélectionnez les règles que vous souhaitez déplacer en cliquant avec le bouton gauche de votre souris.

Astuces Pour sélectionner plusieurs règles, utilisez la touche Ctrl (Contrôle) de votre clavier.

Étape 2 Cliquez avec le bouton droit sur les règles sélectionnées et choisissez **Move to another policy** (Déplacer vers une autre politique).

Étape 3 Sélectionnez la politique de contrôle d'accès de destination dans la liste déroulante **Access Policy** (politique d'accès).

Étape 4 Dans la liste déroulante **Place Rules** (Placer les règles), choisissez l'emplacement des règles déplacées :

- Pour les positionner comme dernier ensemble de règles dans la section **par défaut**, choisissez **Au bas (dans la section par défaut)**.
- Pour les positionner comme premier ensemble de règles dans la section **Obligatoire**, choisissez **En haut (dans la section Obligatoire)**.

Étape 5 Cliquez sur **Move** (Déplacer).

Prochaine étape

- Déployer les changements de configuration.

Nombre d'accès de la politique de préfiltrage

Le nombre de résultats indique le nombre de fois qu'une règle de politique s'est déclenchée pour une connexion correspondante.

Pour des informations complètes sur l'affichage du nombre de résultats en matière de politique de préfiltre, consultez Affichage du nombre de résultats de règles.

Délestages de flux importants

Sur Secure Firewall 3100, Châssis Firepower 4100/9300 ,certains trafics que vous configurez pour être accélérés par une politique de préfiltrage sont gérés par le matériel (en particulier, dans la carte d'interface réseau), et non par votre logiciel défense contre les menaces. Le déchargement de ces flux de connexion permet d'augmenter le débit et de réduire la latence, en particulier pour les applications exigeantes en données telles que les transferts de fichiers volumineux. Cette fonctionnalité est particulièrement utile pour les centres de données. C'est ce qu'on appelle *le déchargement de flux statique*.

En outre, par défaut, les périphériques défense contre les menaces déchargent les flux en fonction d'autres critères, notamment la confiance. C'est ce qu'on appelle *le déchargement de flux dynamique*.

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

Voici des exemples d'applications qui peuvent bénéficier du déchargement de flux volumineux :

- les sites de recherche en informatique à haute performance (HPC), où le périphérique défense contre les menaces est déployé entre les stations de stockage et les stations d'informatique à haute performance. Lorsqu'un site de recherche effectue la sauvegarde à l'aide du transfert de fichiers FTP ou de la synchronisation de fichiers sur NFS, l'importance du trafic de données affecte toutes les connexions. 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, où le périphérique défense contre les menaces est déployé entre les postes de travail et Exchange, principalement à des fins de conformité. La sécurité n'est généralement pas un problème, mais la latence est une préoccupation majeure.

Les flux suivants peuvent être déchargés :

- (Décharge de flux statique uniquement.) Les connexions dont le chemin rapide est défini par la politique de préfiltre.
- Trames standard ou Ethernet balisées 802.1Q uniquement.
- (Décharge du flux dynamique uniquement) :

- Flux inspectés dont le moteur d'inspection décide qu'ils n'ont plus besoin d'être inspectés. Ces flux comprennent notamment :
  - Les flux gérés par des règles de contrôle d'accès qui appliquent l'action Trust (confiance) et qui sont basés sur la zone de sécurité, la source et le réseau de destination et la correspondance des ports uniquement.
  - Flux TLS/SSL qui ne sont pas sélectionnés pour le déchiffrement à l'aide de u de déchiffrement.
  - Flux approuvés par la politique de contournement d'application intelligent (IAB), explicitement ou en raison d'un dépassement de seuils de contournement de flux.
  - Flux qui correspondent aux politiques de fichiers ou de prévention des intrusions qui permettent de faire confiance au flux.
  - Tout flux autorisé qui n'a plus besoin d'être inspecté.
- Le préprocesseur IPS suivant a inspecté les flux :
  - SSH et SMTP.
  - Connexions secondaires du préprocesseur FTP
  - Connexions secondaires du préprocesseur SIP (Session Initiation Protocol).
- Les règles de prévention des intrusions qui utilisent des mots-clés (également appelées *options*)

- Le déchargement de flux dynamique n'est *pas* pris en charge sur Secure Firewall 3100.

Important Pour en savoir plus sur les exceptions et les limites aux éléments ci-dessus, consultez Limites de déchargement de flux, à la page 23.

Utiliser le déchargement de flux statique

Pour téléverser le trafic admissible vers le matériel, créez une règle de politique de préfiltre qui applique l'action **Fastpath** (Chemin rapide). Utilisez des règles de préfiltre pour TCP/UDP et des règles de tunnel pour GRE.

(Non recommandé). Pour désactiver le déchargement de flux statique et, comme sous-produit, le déchargement de flux dynamique, utilisez FlexConfig pour exécuter la commande **no flow-offload enable**. Pour en savoir plus à propos de cette commande, consultez le *Guide des commandes de référence de la gamme Cisco ASA*, disponible dans https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html.

Utiliser le déchargement de flux dynamique

Le déchargement de flux dynamique est activé par défaut, sauf sur les périphériques comme Secure Firewall 3100 qui ne le prennent pas en charge.

Pour désactiver le déchargement dynamique :

```
> configure flow-offload dynamic whitelist disable
```

Pour réactiver le déchargement dynamique :

```
> configure flow-offload dynamic whitelist enable
```

Notez que le déchargement dynamique ne se produit que si le déchargement de flux statique est activé, peu importe si le préfiltre est configuré.

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 :

- Firepower 4100/9300 exécutant FXOS 1.1.3 ou version ultérieure.
- Secure Firewall 3100

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 sur les interfaces configurées en mode passif, en ligne ou Tap en ligne. Les interfaces routées et commutées sont les seuls types pris en charge.
- (Secure Firewall 3100.) Déchargement en fonction de l'en-tête interne pour les flux acheminés en tunnel
- (Secure Firewall 3100.) Déchargement multi-instance
- Flux qui nécessitent une inspection par Snort ou d'autres moteurs d'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 qui doivent être chiffrés ou déchiffrés. Par exemple, les connexions déchiffrées en raison de u de déchiffrement.
- Flux de multidiffusion en mode routé. Ils sont pris en charge en mode transparent s'il n'y a que deux interfaces membres dans un groupe de ponts.
- 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 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.
- Les flux qui comprennent des options IP ne peuvent pas être déchargés de manière dynamique.

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.
- Le déchargement de flux dynamique désactive toutes les vérifications du normalisateur TCP.
- 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.

Déchargent de flux dynamique non pris en charge sur certains périphériques

Le déchargement de flux dynamique n'est pas pris en charge sur Secure Firewall 3100.

Conditions d'inversion du déchargement

Après le déchargement d'un flux, les paquets qu'il contient sont renvoyés à défense contre les menaces 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.

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.