Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center, version 7.2

Dernière modification : 2025-07-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

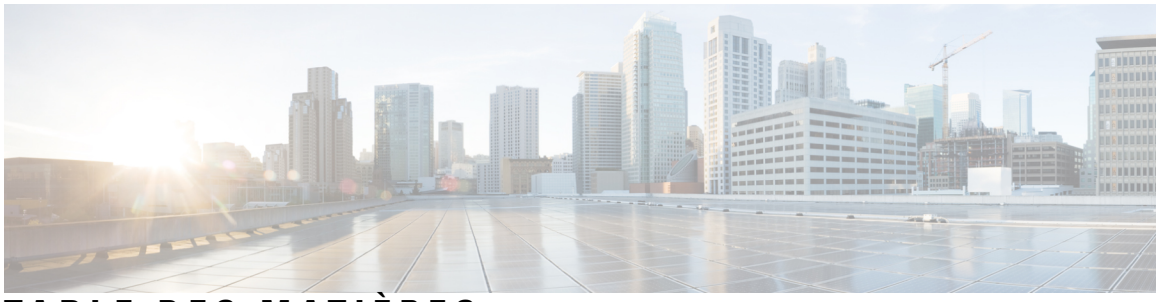
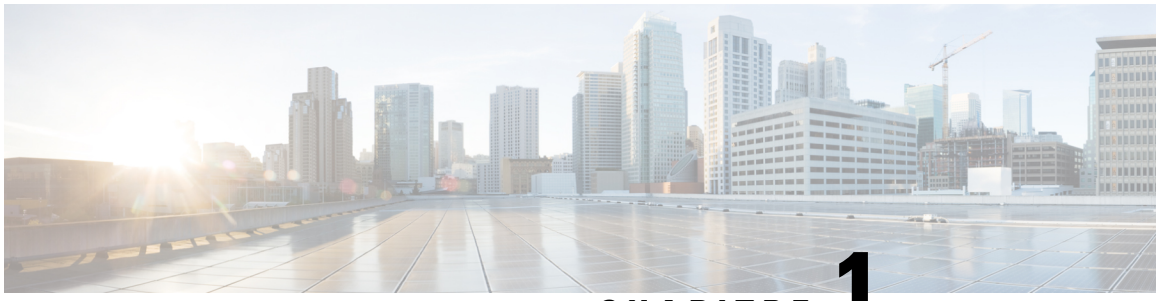


TABLE DES MATIÈRES



CHAPITRE 1

Un aperçu de l'analyse de réseau et de la politique de prévention des intrusions

Le moteur d'inspection Snort fait partie intégrante du périphérique Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense). Ce chapitre fournit une présentation de Snort 3 et de l'analyse de réseau et des politiques de prévention des intrusions. Il fournit également un aperçu des politiques d'analyse de réseau et de prévention des intrusions fournies et personnalisées par le système.

À propos des politiques d'analyse de réseau et de prévention des intrusions

Les politiques d'analyse de réseau et de prévention des intrusions fonctionnent ensemble dans le cadre de la fonction de détection et de prévention des intrusions.

- L'expression *détection des intrusions* fait généralement référence au processus de surveillance et d'analyse passives du trafic réseau à la recherche des intrusions potentielles et de stockage des données d'attaque pour l'analyse de la sécurité. C'est ce que l'on appelle parfois « IDS ».
- Le terme *prévention des intrusions* comprend le concept de détection des intrusions, mais ajoute la possibilité de bloquer ou de modifier le trafic malveillant lorsqu'il traverse votre réseau. C'est ce que l'on appelle parfois « IPS ».

Dans un déploiement de prévention des intrusions, lorsque le système examine les paquets :

- Une **politique d'analyse de réseau** régit la façon dont le trafic est *décodé* et *prétraité* afin qu'il puisse être évalué de manière plus approfondie, en particulier pour détecter un trafic anormal qui pourrait signaler une tentative d'intrusion.

- Une **politique** de prévention des intrusions utilise des règles d'*intrusion et de préprocesseur* (parfois appelées collectivement *règles de prévention des intrusions*) pour examiner les paquets décodés à la recherche d'attaques basées sur des modèles. Les politiques de prévention des intrusions sont associées à *des ensembles de variables*, ce qui vous permet d'utiliser des valeurs nommées pour refléter avec précision votre environnement réseau.

Les politiques d'analyse de réseau et de prévention des intrusions sont toutes deux appelées par une politique de contrôle d'accès parente, mais à des moments différents. Pendant que le système analyse le trafic, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (prétraitement et règles de prévention des intrusions supplémentaires). Ensemble, les politiques d'analyse de réseau et de prévention des intrusions permettent une inspection large et approfondie des paquets. Elles peuvent vous aider à détecter le trafic réseau, à vous alerter et à vous protéger contre le trafic réseau qui pourrait menacer la disponibilité, l'intégrité et la confidentialité des hôtes et de leurs données.

Le système est livré avec plusieurs politiques d'analyse de réseau et de prévention des intrusions du même nom (par exemple, Sécurité et connectivité équilibrées) qui se complètent et fonctionnent ensemble. En utilisant des politiques fournies par le système, vous pouvez profiter de l'expérience de Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos définit les états des règles de prévention des intrusions et des inspecteurs, et fournit les configurations initiales pour les inspecteurs et d'autres paramètres avancés.

Vous pouvez également créer des politiques personnalisées d'analyse de réseau et de prévention des intrusions. Vous pouvez ajuster les paramètres des politiques personnalisées pour inspecter le trafic de la manière qui vous semble la plus importante, afin d'améliorer à la fois les performances de vos périphériques gérés et votre capacité à répondre efficacement aux événements qu'ils génèrent.

Vous créez, modifiez, enregistrez et gérez les politiques d'analyse de réseau et de prévention des intrusions à l'aide d'éditeurs de politiques similaires dans l'interface Web. Lorsque vous modifiez l'un ou l'autre de ces types de politique, un panneau de navigation s'affiche sur le côté gauche de l'interface Web; le côté droit affiche diverses pages de configuration.

Reportez-vous aux vidéos pour obtenir de l'aide et des renseignements supplémentaires :

- Présentation condensée de Snort 3
- Présentation étendue de Snort 3

Plateforme d'inspection Snort

La plateforme d'inspection Snort fait partie intégrante du périphérique Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense). La plateforme d'inspection analyse le trafic en temps réel pour fournir une inspection approfondie des paquets. Les politiques d'analyse de réseau et de prévention des intrusions utilisent les capacités de la plateforme d'inspection Snort pour détecter les intrusions et en protéger le système.

Snort 3

Snort 3 est la dernière version du moteur d'inspection de Snort, qui présente de grandes améliorations par rapport à la version antérieure de ce dernier. L'ancienne version de Snort est Snort 2. Snort 3 est plus efficace, et offre de meilleures performances et une meilleure évolutivité.

L’architecture de Snort 3 a été repensée pour inspecter plus de trafic avec des ressources équivalentes par rapport à Snort 2. Snort 3 permet une insertion simplifiée et flexible des analyseurs de trafic. Snort 3 fournit également une nouvelle syntaxe de règles qui facilite l’écriture de règles et rend visibles les équivalents des règles d’objets partagés.

Les autres changements importants concernant Snort 3 sont les suivants :

- Contrairement à Snort 2, qui utilise plusieurs instances de Snort, Snort 3 associe plusieurs threads à une seule instance de Snort. Cela utilise moins de mémoire, améliore les temps de rechargement Snort, prend en charge un plus grand nombre de règles de prévention des intrusions ainsi qu’une cartographie du réseau plus vaste. Le nombre de threads Snort varie selon la plateforme et est identique au nombre d’instances de Snort 2 pour chaque plateforme. L’utilisation est pratiquement transparente.
- Version Snort par Threat Defense : le moteur d’inspection Snort est spécifique à Threat Defense et non au Cisco Secure Firewall Management Center (anciennement le centre de gestion Cisco Firepower Management Center). Centre de gestion peut gérer plusieurs Threat Defense, chacun avec l’une ou l’autre des versions de Snort (Snort 2 et Snort 3). Bien que les politiques de prévention des intrusions de centre de gestionsoient uniques, le système applique la version Snort 2 ou Snort 3 d’une politique de prévention des intrusions pour la protection contre les intrusions en fonction du moteur d’inspection sélectionné du périphérique.
- Règles de décodeur : les règles de décodeur de paquets se déclenchent uniquement dans la politique de prévention des intrusions par défaut. Le système ignore les règles de décodeur que vous activez dans d’autres politiques.
- Règles d’objet partagé : Snort 3 prend en charge certaines des règles de prévention des intrusions d’objet partagé (SO), mais pas toutes (règles avec un ID de générateur (GID) égal à 3). Les règles d’objet partagé activées qui ne sont pas prises en charge ne se déclenchent pas.
- Inspection multicouche pour les renseignements sur la sécurité – Snort 3 détecte l’adresse IP la plus à l’intérieur, quelle que soit la couche.
- Prise en charge des plateformes : Snort 3 nécessite Threat Defense 7.0 ou une version ultérieure. Elle n’est pas prise en charge par ASA FirePOWER ou NGIPSv.
- Périphériques gérés : un centre de gestionThreat Defenseavec la version 7.0 peut prendre en charge simultanément les versions 6.4, 6.5, 6.6, 6.7 et 7.0 de Snort 2 et la version 7.0 de Snort 3 Threat Defense.
- Interruption de trafic lors du changement de version Snort : le changement de version Snort interrompt l’inspection du trafic et quelques paquets peuvent être abandonnés pendant le déploiement.
- Politiques unifiées : quelle que soit la version du moteur Snort sous-jacent qui est activée dans les Threat Defense gérés, les politiques de contrôle d’accès, les politiques de prévention des intrusions et les politiques d’analyse de réseau configurées dans les centre de gestion fonctionnent de manière transparente lors de l’application des politiques. Toutes les politiques de prévention des intrusions dans les versions 7.0 et ultérieures de centre de gestion comportent deux versions, la version Snort 2 et la version Snort 3. La politique de prévention des intrusions est unifiée, ce qui signifie qu’elle a un nom, une politique de base et un mode d’inspection communs, bien qu’il existe deux versions de la politique (version Snort 2 et version Snort 3). Les versions Snort 2 et Snort 3 de la politique de prévention des intrusions peuvent être différentes en termes de paramètres de règles. Cependant, lorsque la politique de prévention des intrusions est appliquée à un périphérique, le système identifie automatiquement la version Snort activée sur le périphérique et applique les paramètres de règle configurés pour cette version.
- Lightweight Security Package (LSP) (Paquet de sécurité léger) : remplace les mises à jour des règles Snort (SRU) par les mises à jour des règles de prévention des intrusions et de configuration de nouvelle

génération de Snort 3. Le téléchargement de mises à jour télécharge à la fois le LSP Snort 3 et la SRU Snort 2.

Les mises à jour LSP fournissent des règles de prévention des intrusions et des règles d'inspecteurs nouvelles et mises à jour, des états modifiés pour les règles existantes et des paramètres de politique de prévention des intrusions par défaut modifiés pour centre de gestion et Threat Defense version 7.0 ou supérieure. Lorsque vous mettez à niveau un centre de gestion de la version 6.7 ou antérieure à la version 7.0, il prend en charge les LSP et les SRU. Les mises à jour de règles peuvent également supprimer des règles, fournir de nouvelles catégories de règles et variables par défaut, et modifier les valeurs des variables par défaut. Pour en savoir plus sur les mises à jour des LSP, consultez la rubrique *Mettre à jour les règles de prévention des intrusions* dans la dernière version du *Guide de configuration du centre de gestion Cisco Firepower Management Center*.

- Mappage des règles et des présélections Snort 2 et Snort 3 : les règles Snort 2 et Snort 3 sont mappées et le mappage est fourni par le système. Cependant, il ne s'agit pas d'un mappage un à un. Les politiques de base en matière de prévention des intrusions fournies par le système sont préconfigurées pour Snort 2 et Snort 3 et fournissent la même prévention des intrusions, bien qu'avec des ensembles de règles différents. Les politiques de base fournies par le système pour Snort 2 et Snort 3 sont mappées entre elles pour les mêmes paramètres de prévention des intrusions.Pour plus de renseignements, consultez Afficher le mappage de politique de base Snort 2 et Snort 3, à la page 26.
- Annulation des règles de remplacement Snort 2 et Snort 3 : lorsqu'un Threat Defense est mis à niveau vers la version 7.0, vous pouvez mettre à niveau la plateforme d'inspection de Threat Defense vers la version Snort 3. Centre de gestion met en correspondance tous les remplacements dans les règles existantes de la version Snort 2 des politiques de prévention des intrusions avec les règles Snort 3 correspondantes en utilisant le mappage fourni par Talos. Cependant, si des remplacements supplémentaires sont effectués après la mise à niveau ou si vous avez installé un nouveau Threat Defense à la version 7.0, ils doivent être synchronisés manuellement. Pour en savoir plus, consultez Synchroniser les règles de Snort 2 avec celles de Snort 3, à la page 27.
- Règles de prévention des intrusions personnalisées : vous pouvez créer des règles de prévention des intrusions personnalisées dans Snort 3. Vous pouvez également importer les règles de prévention des intrusions personnalisées qui existent pour Snort 2 dans Snort 3. Pour en savoir plus, consultez Règles personnalisées dans Snort 3, à la page 45.
- Commutation entre les moteurs Snort 2 et Snort 3 : les Threat Defense qui prennent en charge Snort 3 peuvent également prendre en charge Snort 2. Le passage de Snort 3 à Snort 2 n'est pas recommandé du point de vue de l'efficacité.

Important Bien que vous puissiez changer de version Snort librement, les modifications de règles de prévention des intrusions dans une version de Snort ne seront pas mises à jour automatiquement dans l'autre version. Si vous modifiez l'action de règle pour une règle d'une version Snort, assurez-vous de reproduire la modification dans l'autre version avant de changer de version Snort. L'option de synchronisation fournie par le système synchronise uniquement les modifications de la version Snort 2 de la politique de prévention des intrusions avec la version Snort 3, et non l'inverse.

Lignes directrices et limites relatives aux politiques d'analyse de réseau et de prévention des intrusions

- Un pourcentage élevé de trafic composé de petits paquets diminue les performances de Snort. Ce comportement est observé même lorsque tous les préprocesseurs sont désactivés.
- Lorsque vous tentez de déployer une modification de configuration sur un périphérique Threat Defense avec une mémoire faible, le déploiement de Snort est également déclenché. Il en résulte une utilisation élevée de la mémoire RSS. L'utilisation de la mémoire Snort est également affectée si vous déployez des configurations importantes sur le périphérique, telles que plusieurs politiques IPS contenant un grand nombre de règles IPS Snort, d'objets de réseau et de listes de contrôle d'accès. Vous pouvez atténuer ces problèmes de mémoire en optimisant la configuration. Pour connaître les bonnes pratiques en matière de configuration des règles de contrôle d'accès afin d'optimiser la configuration, consultez Bonnes pratiques pour les règles de contrôle d'accès.
- Si vous augmentez la mémoire d'une instance Threat Defense Virtual, vous devez redéployer la configuration pour Snort 3 afin d'utiliser la mémoire supplémentaire.

Remarque L'allocation de mémoire Snort 3 n'est pas automatiquement ajustée lorsque vous augmentez la mémoire de l'instance Threat Defense Virtual. Vous devez redéployer la configuration pour régénérer les fichiers de configuration pertinents, tels que `memory_allocation.lua`, qui appliquent les limites de ressources mises à jour à Snort 3.

Limites de la fonctionnalité Snort 3 pour Threat Defense géré par Centre de gestion

Le tableau suivant répertorie les fonctions prises en charge sur Snort 2 mais non sur Snort 3 pour les périphériques Threat Defense gérés par centre de gestion.

Tableau 1 : Limites des fonctionnalités de Snort 3

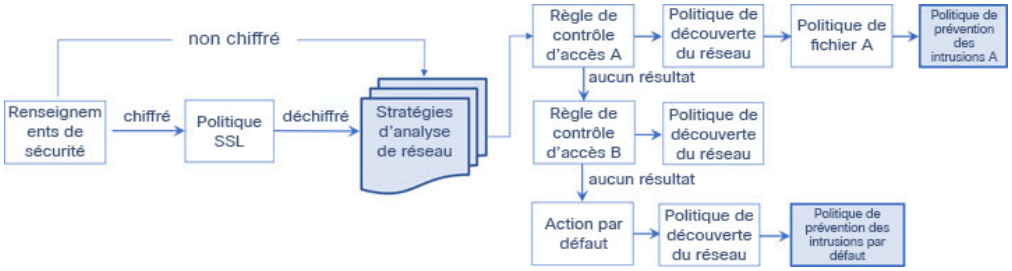
Politique/domaine	Fonctionnalités non prises en charge
Politique de contrôle d'accès	Les paramètres de l'application suivants : • Recherche sécuritaire • YouTube EDU

Politique/domaine	Fonctionnalités non prises en charge
Politique de prévention des intrusions	• Couches de la politique • Seuil de règle globale • Configuration de la journalisation : • SNMP • Mises à jour des règles SRU car Snort 3 prend uniquement en charge les mises à jour des règles LSP
Autres fonctionnalités	Journalisation des événements avec noms de domaines complets

Comment les politiques examinent le trafic à la recherche d'intrusions

Lorsque le système analyse le trafic dans le cadre de votre déploiement de contrôle d'accès, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (règles de prévention des intrusions et paramètres avancés).

Le diagramme suivant montre, de manière simplifiée, l'ordre d'analyse du trafic dans un déploiement en ligne de la prévention des intrusions et d'AMP for Networks. Il montre comment la politique de contrôle d'accès fait appel à d'autres politiques pour examiner le trafic et dans quel ordre ces politiques sont appelées. Les phases d'analyse de réseau et de sélection de la politique de prévention des intrusions sont mises en surbrillance.



Dans un déploiement en ligne (c'est-à-dire lorsque les configurations pertinentes sont déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne), le système peut bloquer le trafic sans autre inspection, à presque toutes les étapes du processus illustré. La solution Security Intelligence, la politique SSL, les politiques d'analyse de réseau, les politiques de fichiers et les politiques de prévention des intrusions peuvent toutes supprimer ou modifier le trafic. Seule la politique de découverte de réseau, qui inspecte passivement les paquets, ne peut pas affecter le flux de trafic.

De même, à chaque étape du processus, un paquet peut entraîner la génération d'un événement par le système. Les intrusions et les événements de préprocesseur (parfois appelés collectivement *incidents d'intrusion*) sont des indications qu'un paquet ou son contenu peuvent présenter un risque pour la sécurité.

Astuces Le diagramme ne reflète pas le fait que les règles de contrôle d'accès traitent le trafic chiffré lorsque votre configuration d'inspection SSL le laisse passer, ou si vous ne configurez pas l'inspection SSL. Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers.

Notez que pour une connexion unique, bien que le système sélectionne une politique d'analyse de réseau avant une règle de contrôle d'accès comme le montre le diagramme, un certain prétraitement (notamment un prétraitement de la couche applicative) a lieu après la sélection de la règle de contrôle d'accès. Cela n'affecte **pas** la façon dont vous configurez le prétraitement dans les politiques d'analyse de réseau personnalisées.

Décodage, normalisation et prétraitement : politiques d'analyse de réseau

Sans décodage et prétraitement, le système ne pourrait pas évaluer correctement le trafic pour détecter les intrusions, car les différences de protocole rendraient impossible la mise en correspondance de modèles. Les politiques d'analyse de réseau régissent ces tâches de gestion du trafic :

- une **fois** le trafic filtré par Security Intelligence
- une **fois** le trafic chiffré déchiffré par une politique SSL facultative
- **avant que** le trafic puisse être inspecté par des politiques de fichiers ou de prévention des intrusions

Une politique d'analyse de réseau régit le traitement des paquets par phases. Tout d'abord, le système décode les paquets qui passent par les trois premières couches TCP/IP, puis poursuit la normalisation, le prétraitement et la détection des anomalies de protocole :

- Le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format qui peut être facilement utilisé par les inspecteurs et, ultérieurement, par les règles de prévention des intrusions. Chaque couche de la pile TCP/IP est décodée tour à tour, en commençant par la couche de liaison de données jusqu'aux couches de réseau et de transport. Le décodeur de paquets détecte également divers comportements anormaux dans les en-têtes de paquets.
- Dans les déploiements en ligne, le préprocesseur de normalisation en ligne formate (normalise) le trafic pour minimiser les risques que les attaquants échappant à la détection. Il prépare les paquets pour l'examen par d'autres inspecteurs et prépare les règles de prévention des intrusions, et veille à ce que les paquets traités par le système soient les mêmes que les paquets reçus par les hôtes de votre réseau.
- Divers inspecteurs des couches de réseau et de transport détectent les attaques qui exploitent la fragmentation IP, effectuent la validation de la somme de contrôle et le prétraitement de la session TCP et UDP.

  Notez que certains paramètres avancés de transport et de réseau de l'inspecteur s'appliquent globalement à tout le trafic géré par les périphériques cibles d'une politique de contrôle d'accès. Vous les configurez dans la politique de contrôle d'accès plutôt que dans une politique d'analyse de réseau.
- Divers décodeurs de protocole de la couche d'application normalisent des types spécifiques de données de paquets dans des formats que le moteur de règles de prévention des intrusions peut analyser. La normalisation des codages de protocoles de la couche d'application permet au système d'appliquer efficacement les mêmes règles de prévention des intrusions liées au contenu aux paquets dont les données sont présentées différemment et d'obtenir des résultats significatifs.

- Les inspecteurs Modbus, DNP3, CIP et SCADA s7commplus détectent les anomalies de trafic et fournissent des données aux règles de prévention des intrusions. Les protocoles de supervision, de contrôle et d'acquisition de données (SCADA) surveillent, contrôlent et acquièrent des données des processus industriels, des processus d'infrastructure et d'installation tels que la fabrication, la production, le traitement de l'eau, la distribution d'énergie électrique, les systèmes aéroportuaires et d'expédition, et ainsi de suite.
- Plusieurs inspecteurs vous permettent de détecter des menaces spécifiques, comme l'ouverture arrière, les analyses de ports, les inondations SYN et d'autres attaques basées sur le débit.

  Notez que vous configurez l'inspecteur de données sensibles, qui détecte les données sensibles telles que les numéros de carte de crédit et les numéros de sécurité sociale en texte ASCII, dans les politiques de prévention des intrusions.

Remarque Lorsque l'identité du serveur TLS est désactivée, Snort 3 n'effectue pas de détection de non-concordance SNI. Il évalue uniquement le SNI dans le paquet Client Hello et contourne la validation du nom commun (CN) du certificat dans le paquet Server Hello.

Dans une politique de contrôle d'accès nouvellement créée, une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic pour *toutes* les politiques de prévention des intrusions appelées par la même politique parente de contrôle d'accès. Au départ, le système utilise la politique d'analyse de réseau Sécurité et connectivité équilibrées par défaut, mais vous pouvez la remplacer par une autre politique d'analyse de réseau fournie par le système ou personnalisée. Dans un déploiement plus complexe, les utilisateurs avancés peuvent adapter les options de prétraitement du trafic à des zones de sécurité, à des réseaux et à des VLAN spécifiques en attribuant différentes politiques d'analyse de réseau personnalisées pour prétraiter le trafic correspondant.

Remarque Pour une stratégie de contrôle d'accès avec une action découlant d'une règle définie sur **Trust** et une règle de préfiltre avec une action définie sur **Fastpath** avec les options de journalisation désactivées, vous remarquerez que les événements de fin de flux sont toujours générés dans le système. Les événements ne sont pas visibles sur les pages des événements du centre de gestion.

Règles de contrôle d'accès : sélection de la politique de prévention des intrusions

Après le prétraitement initial, les règles de contrôle d'accès (le cas échéant) évaluent le trafic. Dans la plupart des cas, la première règle de contrôle d'accès à laquelle un paquet correspond est la règle qui gère ce trafic; vous pouvez surveiller, faire confiance, bloquer ou autoriser le trafic correspondant.

Lorsque vous autorisez le trafic avec une règle de contrôle d'accès, le système peut inspecter le trafic à la recherche de données de découverte, de programmes malveillants, de fichiers interdits et d'intrusions, dans cet ordre. Le trafic ne correspondant à aucune règle de contrôle d'accès est géré par l'action par défaut de la politique de contrôle d'accès, qui peut également inspecter les données de découverte et les intrusions.

Remarque Tous les paquets, **quelle que soit** la politique d'analyse de réseau qui les prétraite, correspondent aux règles de contrôle d'accès configurées et sont donc potentiellement sujets à une inspection par les politiques de prévention des intrusions, dans l'ordre descendant.

Le diagramme en Comment les politiques examinent le trafic à la recherche d'intrusions, à la page 6 montre le flux du trafic dans un périphérique dans un déploiement en ligne de la prévention des intrusions et de AMP for Networks, comme suit :

- La règle de contrôle d'accès A permet au trafic correspondant de se poursuivre. La politique de découverte du réseau inspecte ensuite le trafic pour identifier des données de découverte, afin de détecter les fichiers interdits et les programmes malveillants par la politique A de fichiers, puis les intrusions sont repérées par la politique de prévention des intrusions A.
- La règle de contrôle d'accès B permet également de mettre en correspondance le trafic. Cependant, dans ce scénario, le trafic n'est pas inspecté pour détecter les intrusions (ou les fichiers ou les programmes malveillants), donc aucune politique de prévention des intrusions ou de fichier n'est associée à la règle. Notez que par défaut, le trafic que vous autorisez la poursuite est inspecté par la politique de découverte de réseau; vous n'avez pas besoin de configurer cela.
- Dans ce scénario, l'action par défaut de la politique de contrôle d'accès permet une mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de découverte de réseau, puis par une politique de prévention des intrusions. Vous pouvez (sans y être obligé) utiliser une politique de prévention des intrusions différente lorsque vous associez des politiques de prévention des intrusions aux règles de contrôle d'accès ou à l'action par défaut.

L'exemple du diagramme n'inclut aucune règle de blocage ou d'approbation, car le système n'inspecte pas le trafic bloqué ou de confiance.

Inspection d'intrusion : politiques, règles et ensembles de variables de prévention d'intrusion

De même, vous pouvez utiliser une politique IPS comme dernière ligne de défense du système avant que le trafic ne soit autorisé à se rendre à destination. Les politiques d'intrusion régissent la manière dont le système inspecte le trafic à la recherche de violations de la sécurité et, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. La fonction principale des politiques de prévention des intrusions est de gérer les règles de prévention des intrusions et de préprocesseur activées et la façon dont elles sont configurées.

Règles de prévention des intrusions et de l'inspecteur

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments qui détectent les tentatives d'exploitation des vulnérabilités de votre réseau. le système utilise une règle de prévention des intrusions pour analyser le trafic réseau et vérifier s'il correspond aux critères de la règle. Le système compare les paquets aux conditions spécifiées dans chaque règle et, si les données du paquet correspondent à toutes les conditions spécifiées dans une règle, la règle se déclenche.

Le système comprend les types de règles suivants, créées par Cisco Talos Intelligence Group (Talos) :

- *les règles de prévention des intrusions d'objets partagés*, qui sont compilées et ne peuvent pas être modifiées (à l'exception des informations d'en-tête de règle telles que les ports source et de destination et les adresses IP)

- *les règles de prévention des intrusions en texte standard*, qui peuvent être enregistrées et modifiées en tant que nouvelles instances personnalisées de la règle.
- *les règles de préprocesseur*, qui sont des règles associées aux inspecteurs et aux options de détection des décodeurs de paquets dans la politique d'analyse de réseau. Vous ne pouvez pas copier ou modifier les règles de l'inspecteur. La plupart des règles de l'inspecteur sont désactivées par défaut; vous devez leur permettre d'utiliser les inspecteurs pour générer des événements et, dans un déploiement en ligne, abandonner les paquets fautifs.

Lorsque le système traite les paquets conformément à une politique de prévention des intrusions, un optimiseur de règles classe d'abord toutes les règles activées en sous-ensembles en fonction de critères tels que la couche de transport, le protocole d'application, la direction vers ou à partir du réseau protégé, etc. Ensuite, le moteur de règles de prévention des intrusions sélectionne les sous-ensembles de règles appropriés à appliquer à chaque paquet. Enfin, un moteur de recherche à règles multiples effectue trois types de recherches différents pour déterminer si le trafic correspond à la règle :

- La recherche de champ de protocole recherche les correspondances dans des champs particuliers d'un protocole d'application.
- La recherche de contenu générique recherche les correspondances d'octets ASCII ou binaires dans les données utiles du paquet.
- La recherche d'anomalies de paquet recherche les en-têtes de paquet et les charges utiles qui, plutôt que de contenir un contenu spécifique, enfreignent des protocoles bien établis.

Dans une politique de prévention des intrusions personnalisée, vous pouvez ajuster la détection en activant et en désactivant les règles, ainsi qu'en écrivant et en ajoutant vos propres règles de texte standard. Vous pouvez également utiliser les recommandations de Cisco pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.

Remarque Lorsqu'il y a suffisamment de paquets pour traiter un trafic spécifique selon une règle de blocage, le système continue d'évaluer le trafic restant en fonction d'autres règles. Si du trafic restant correspond à une règle définie pour bloquer, la session est bloquée. Cependant, si le système analyse le trafic restant à transmettre, l'état du trafic indique en attente pour la règle qui est bloquée faute de paquets complets.

Ensembles de variables

Chaque fois que le système utilise une politique de prévention des intrusions pour évaluer le trafic, il utilise un *ensemble de variables* associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles d'intrusion pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles et de règles dynamiques.

Le système fournit un seul ensemble de variables par défaut, qui comprend des variables par défaut prédéfinies. La plupart des règles d'objet partagé et des règles de texte standard fournies par le système utilisent ces variables par défaut prédéfinies pour définir les réseaux et les numéros de port. Par exemple, la majorité des règles utilisent la variable `$HOME_NET` pour préciser le réseau protégé et la variable `$EXTERNAL_NET`pour préciser le réseau non protégé (ou externe). En outre, les règles spécialisées utilisent souvent d'autres variables prédéfinies. Par exemple, les règles qui détectent les exploits contre les serveurs Web utilisent les variables `$HTTP_SERVERS` et `$HTTP_PORTS`.

Astuces Même si vous utilisez les politiques de prévention des intrusions fournies par le système, Cisco vous recommande **fortement** de modifier les variables clés par défaut de l'ensemble par défaut. Lorsque vous utilisez des variables qui reflètent avec précision votre environnement réseau, le traitement est optimisé et le système peut surveiller les systèmes concernés pour détecter toute activité suspecte. Les utilisateurs avancés peuvent créer et utiliser des ensembles de variables personnalisés pour les jumeler avec une ou plusieurs politiques de prévention des intrusions personnalisées.

Important Si vous créez un ensemble de variables personnalisé, n'utilisez pas de chiffre comme premier caractère dans le nom d'un ensemble de variables personnalisées (par exemple, 3Snort). Cela entraînera l'échec de la validation du Snort 3 lorsque vous déployez une configuration sur le pare-feu Threat Defense sur centre de gestion.

Génération d'incidents d'intrusion

Lorsque le système détecte une intrusion possible, il génère un événement d' *intrusion ou de préprocesseur* (parfois appelés collectivement *incidents d'intrusion*). Les périphériques gérés transmettent leurs événements à centre de gestion, où vous pouvez afficher les données agrégées et acquérir une meilleure compréhension des attaques contre les ressources de votre réseau. Dans un déploiement en ligne, les périphériques gérés peuvent également abandonner ou remplacer des paquets que vous savez être dangereux.

Chaque incident d'intrusion dans la base de données comprend un en-tête d'événement et contient des informations sur le nom et la classification de l'événement; les adresses IP de source et de destination; les ports; le processus qui a généré l'événement; et la date et l'heure de l'événement, ainsi que des informations contextuelles sur la source de l'attaque et sa cible. Pour les événements par paquets, le système enregistre également une copie de l'en-tête du paquet décodé et de la charge utile du ou des paquets qui ont déclenché l'événement.

Le décodeur de paquets, les préprocesseurs et le moteur de règles de prévention des intrusions peuvent tous forcer le système à générer un événement. Par exemple :

- Si le décodeur de paquets (configuré dans la politique d'analyse de réseau) reçoit un paquet IP de moins de 20 octets, soit la taille d'un datagramme IP sans option ni charge utile, le décodeur interprète cela comme un trafic anormal. Si, ultérieurement, la règle de décodeur associée dans la politique de prévention des intrusions qui examine le paquet est activée, le système génère un événement d'inspection.
- Si le préprocesseur de défragmentation IP rencontre une série de fragments IP qui se chevauchent, l'inspecteur interprète cela comme une attaque possible et, lorsque la règle d'inspecteur associée est activée, le système génère un événement d'inspecteur.
- Dans le moteur de règles de prévention des intrusions, la plupart des règles de texte standard et des règles d'objets partagés sont écrites de manière à générer des incidents d'intrusion lorsqu'elles sont déclenchées par des paquets.

Au fur et à mesure que la base de données accumule les incidents d'intrusion, vous pouvez commencer votre analyse des attaques potentielles. Le système vous fournit les outils dont vous avez besoin pour passer en revue les incidents d'intrusion et évaluer s'ils sont importants dans le contexte de votre environnement réseau et de vos politiques de sécurité.

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées

La création d'une nouvelle politique de contrôle d'accès est l'une des premières étapes de la gestion du flux de trafic à l'aide du système. Par défaut, une politique de contrôle d'accès nouvellement créée fait appel aux politiques d'analyse de réseau et de prévention des intrusions fournies par le système pour examiner le trafic.

Le diagramme suivant montre comment une nouvelle politique de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic. Les phases de prétraitement et de prévention des intrusions sont mises en surbrillance.

Remarquez comment :

- Une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic géré par la politique de contrôle d'accès. Au départ, la *politique d'analyse du réseau de sécurité et de connectivité équilibrée* fournie par le système est la politique par défaut.
- L'action par défaut de la politique de contrôle d'accès autorise tout le trafic non malveillant, comme déterminé par la *politique de prévention des intrusions, de sécurité et connectivité équilibrées* fournie par le système. Comme l'action par défaut laisse passer le trafic, la fonction de découverte peut l'examiner à la recherche de données relatives à l'hôte, à l'application et à l'utilisateur avant que la politique de prévention des intrusions ne puisse examiner et éventuellement bloquer le trafic malveillant.
- La politique utilise les options Security Intelligence par défaut (listes globales de blocage et Ne pas bloquer uniquement), ne déchiffre pas le trafic chiffré avec une politique SSL et n'effectue pas de traitement spécial ni d'inspection du trafic réseau à l'aide des règles de contrôle d'accès.

Une mesure simple à prendre pour optimiser le déploiement de la prévention des intrusions consiste à utiliser par défaut un ensemble différent de politiques d'analyse du réseau et de prévention des intrusions fournies par le système. Cisco fournit plusieurs paires de ces politiques avec le système.

Vous pouvez aussi adapter votre déploiement de prévention des intrusions en créant et en utilisant des politiques personnalisées. Vous constaterez peut-être que les options de l'inspecteur, la règle de prévention des intrusions et d'autres paramètres avancés configurés dans ces politiques ne répondent pas aux besoins de sécurité de votre réseau. En ajustant vos politiques d'analyse de réseau et de prévention des intrusions, vous pouvez configurer, à un niveau très fin, la façon dont le système traite et inspecte le trafic sur votre réseau pour détecter les intrusions.

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées

Cisco fournit les politiques d'analyse de réseau et de prévention des intrusions suivantes avec le système : En utilisant les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos fournit des états des règles de prévention des intrusions et d'inspecteur, ainsi que des configurations initiales pour les inspecteurs et d'autres paramètres avancés.

Aucune politique fournie par le système ne couvre tous les profils de réseau, toutes les combinaisons de trafic ou toutes les postures défensives. Chacune couvre des cas et des configurations réseau courants qui fournissent un point de départ pour une politique défensive bien réglée. Bien que vous puissiez utiliser les politiques fournies par le système telles quelles, Cisco vous recommande fortement de les utiliser comme base pour des politiques personnalisées que vous ajusterez en fonction de votre réseau.

Astuces Même si vous utilisez les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous devez configurer les variables de prévention des intrusions du système pour refléter avec précision votre environnement réseau. Modifiez au minimum les variables par défaut clés dans l'ensemble par défaut.

À mesure que de nouvelles vulnérabilités sont connues, Talos publie des mises à jour des règles de prévention des intrusions, également appelées *Paquet léger de sécurité* (LSP). Ces mises à jour de règles peuvent modifier toute analyse de réseau ou politique de prévention des intrusions fournie par le système, ainsi que des règles de prévention des intrusions et d'inspecteur nouvelles ou mises à jour, des états modifiés pour les règles existantes et des paramètres de politique par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles des politiques fournies par le système et fournir de nouvelles catégories de règles, ainsi que modifier l'ensemble de variables par défaut.

Si la mise à jour d'une règle affecte votre déploiement, l'interface Web marque comme obsolètes les politiques d'analyse de réseau et de prévention des intrusions affectées, ainsi que leurs politiques parentes de contrôle d'accès. Vous devez redéployer une politique mise à jour pour que ses modifications prennent effet.

Pour plus de commodité, vous pouvez configurer des mises à jour de règles pour qu'elles redéploient automatiquement les politiques de prévention des intrusions touchées, seules ou en combinaison avec les politiques de contrôle d'accès concernées. Cela vous permet de garder facilement et automatiquement votre déploiement à jour pour vous protéger contre les intrusions et les exploits découverts récemment.

Pour garantir la mise à jour des paramètres de prétraitement, vous **devez** redéployer les politiques de contrôle d'accès, qui déploient également tout SSL associé, ainsi que les politiques d'analyse de réseau et de fichiers différentes de celles en cours d'exécution, et peuvent également mettre à jour les valeurs par défaut pour le prétraitement avancé. et les options de performance.

Cisco fournit les politiques d'analyse de réseau et de prévention des intrusions suivantes avec le système :

Politiques d'analyse des intrusions et de sécurité et de connectivité équilibrées

Ces politiques sont conçues pour la vitesse et la détection. Utilisés ensemble, ils constituent un bon point de départ pour la plupart des organisations et des types de déploiement. Le système utilise les politiques et les paramètres de sécurité et de connectivité équilibrées par défaut dans la plupart des cas.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les organisations où la connectivité (permission d'accéder à toutes les ressources) prime sur la sécurité de l'infrastructure réseau. La politique de prévention des intrusions active beaucoup moins de règles que celles activées dans la politique de sécurité avant la connectivité. Seules les règles les plus critiques qui bloquent le trafic sont activées.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les entreprises où la sécurité de l'infrastructure réseau prime sur la commodité pour l'utilisateur. La politique de prévention des intrusions permet d'appliquer de nombreuses règles de prévention des anomalies du réseau qui peuvent alerter sur le trafic légitime ou l'interrompre.

Politiques d’analyse de réseau et de prévention des intrusions

Ces politiques sont conçues pour les organisations où la sécurité de l'infrastructure du réseau est encore plus importante que celle des politiques de sécurité sur la connectivité, avec un potentiel d'impact opérationnel encore plus grand. Par exemple, la politique de prévention des intrusions active des règles dans un grand nombre de catégories de menaces, y compris les programmes malveillants, les trousses d’exploit, les vulnérabilités anciennes et courantes, et les exploits connus et répandus.

Politique de prévention des intrusions Aucune règle active

Dans la politique de prévention des intrusions Aucune règle active, toutes les règles de prévention des intrusions et tous les paramètres avancés, à l’exception des seuils de règles de prévention des intrusions, sont désactivés. La présente politique fournit un point de départ si vous souhaitez créer votre propre politique de prévention des intrusions au lieu de la baser sur les règles activées dans l’une des autres politiques fournies par le système.

Remarque Selon la politique de base sélectionnée, fournie par le système, les paramètres de la politique varient. Pour afficher les paramètres de la politique, cliquez sur l’icône **Modifier** à côté de la politique, puis cliquez sur la liste déroulante **Base Policy** (politique de base).

Avantages de l'analyse personnalisée du réseau et des politiques de prévention des intrusions

Vous constaterez peut-être que les options de l’inspecteur, les règles de prévention des intrusions et d’autres paramètres avancés configurés dans les politiques d’analyse de réseau et de prévention des intrusions fournies par le système ne répondent pas entièrement aux besoins de sécurité de votre organisation.

L’élaboration de politiques personnalisées peut améliorer les performances du système dans votre environnement et fournir un aperçu précis du trafic malveillant et des violations de politiques qui se produisent sur votre réseau. La création et le réglage de politiques personnalisées vous permettent de configurer, à un niveau très fin, la façon dont le système traite et inspecte le trafic sur votre réseau pour détecter les intrusions.

Toutes les politiques personnalisées ont une politique de base, également appelée couche de base, qui définit les paramètres par défaut pour toutes les configurations de la politique. Une couche est un bloc de construction que vous pouvez utiliser pour gérer efficacement plusieurs politiques d’analyse de réseau ou de prévention des intrusions.

Dans la plupart des cas, vous fondez les politiques personnalisées sur les politiques fournies par le système, mais vous pouvez utiliser une autre politique personnalisée. Cependant, toutes les politiques personnalisées ont une politique fournie par le système comme base potentielle dans une chaîne de politiques. Étant donné que les mises à jour de règles peuvent modifier des politiques fournies par le système, l’importation d’une mise à jour de règle peut vous affecter même si vous utilisez une politique personnalisée comme base. Si la mise à jour d’une règle affecte votre déploiement, l’interface Web marque les politiques concernées comme obsolètes.

Avantages des politiques d’analyse de réseau personnalisées

Par défaut, une politique d’analyse de réseau prétraite tout le trafic non chiffré géré par la politique de contrôle d’accès. Cela signifie que tous les paquets sont décodés et prétraités en fonction des mêmes paramètres, quelle que soit la politique de prévention des intrusions (et, par conséquent, l’ensemble de règles de prévention des intrusions) qui les examinera ultérieurement.

Au départ, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique par défaut. Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut.

Les options de réglage disponibles varient d'un inspecteur à l'autre, mais il est possible de régler les inspecteurs et les décodeurs de plusieurs façons :

- Vous pouvez désactiver les inspecteurs qui ne s'appliquent pas au trafic que vous surveillez. Par exemple, l'inspecteur HTTP Inspect normalise le trafic HTTP. Si vous êtes sûr que votre réseau n'inclut aucun serveur Web utilisant les services Internet Information Services (IIS de Microsoft), vous pouvez désactiver l'option de l'inspecteur qui recherche le trafic spécifique à IIS et ainsi réduire la surcharge de traitement du système.

Remarque Si vous désactivez un inspecteur dans une politique d'analyse de réseau personnalisée, mais que le système doit utiliser cet inspecteur pour évaluer ultérieurement les paquets par rapport à une règle de prévention des intrusions ou à une règle d'inspecteur activée, le système active et utilise automatiquement l'inspecteur, bien que l'inspecteur reste désactivé dans la politique d'analyse de réseau interface Web.

- Préciser les ports, le cas échéant, pour concentrer l'activité de certains inspecteurs. Par exemple, vous pouvez identifier des ports supplémentaires pour surveiller les réponses du serveur DNS ou les sessions SSL chiffrées, ou des ports sur lesquels vous décodez le trafic Telnet, HTTP et RPC.

Pour les utilisateurs avancés ayant des déploiements complexes, vous pouvez créer plusieurs politiques d'analyse du réseau, chacune étant conçue pour prétraiter le trafic différemment. Ensuite, vous pouvez configurer le système pour utiliser ces politiques et régir le prétraitement du trafic en utilisant différentes zones de sécurité, réseaux ou VLAN. (Notez que les modules ASA FirePOWER ne peuvent pas restreindre le prétraitement par VLAN.)

Remarque La personnalisation du prétraitement à l'aide de politiques d'analyse de réseau personnalisées, en particulier de plusieurs politiques d'analyse de réseau, est une tâche avancée. Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** veiller à ne pas autoriser les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet à se compléter.

Avantages des politiques de prévention des intrusions personnalisées

Dans une nouvelle politique de contrôle d'accès configurée initialement pour effectuer la prévention des intrusions, l'action par défaut autorise tout le trafic, mais en l'inspectant d'abord à l'aide de la politique de prévention des intrusions de sécurité et de connectivité équilibrées fournie par le système. À moins que vous ajoutiez des règles de contrôle d'accès ou changiez l'action par défaut, tout le trafic est inspecté par cette politique de prévention des intrusions.

Pour personnaliser votre déploiement de prévention des intrusions, vous pouvez créer plusieurs politiques à cet effet, chacune étant conçue pour inspecter le trafic différemment. Configurez ensuite une politique de contrôle d'accès avec des règles qui précisent quelle politique inspecte quel trafic. Les règles de contrôle d'accès peuvent être simples ou complexes : les correspondances et l'inspection du trafic se font en fonction de plusieurs critères, notamment la zone de sécurité, l'emplacement réseau ou géographique, le VLAN, le port, l'application, l'URL demandée ou l'utilisateur.

La principale fonction des politiques de prévention des intrusions est de gérer les règles de prévention des intrusions et d'inspection qui sont activées et la manière dont elles sont configurées, comme suit :

- Dans chaque politique de prévention des intrusions, vous devez vérifier que toutes les règles applicables à votre environnement sont activées et améliorer les performances en désactivant les règles qui ne sont pas applicables à ce dernier. Vous pouvez préciser les règles qui doivent abandonner ou modifier les paquets malveillants.
- Les recommandationsCisco vous permettent d'associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.
- Vous pouvez modifier les règles existantes et écrire de nouvelles règles en texte standard au besoin pour détecter de nouveaux exploits ou appliquer vos politiques de sécurité.

Voici d'autres personnalisations que vous pourriez apporter à une politique de prévention des intrusions :

- Le préprocesseur des données sensibles détecte les données sensibles telles que les numéros de cartes de crédit et les numéros de sécurité sociale dans le texte ASCII. Notez que d'autres inspecteurs qui détectent des menaces spécifiques (attaques par orifice arrière, plusieurs types de balayage de ports et attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif) sont configurés dans les politiques d'analyse de réseau.
- Les seuils globaux obligent le système à générer des événements en fonction du nombre de fois que le trafic correspondant à une règle de prévention des intrusions provient d'une adresse ou d'une plage d'adresses spécifique au cours d'une période donnée ou est ciblé vers une adresse ou une plage d'adresses donnée. Cela permet d'éviter que le système ne soit submergé par un grand nombre d'événements.
- La suppression des notifications d'incidents d'intrusion et la définition de seuils pour des règles individuelles ou des politiques complètes de prévention des intrusions peuvent également éviter que le système ne soit submergé par un grand nombre d'événements.
- En plus des différents affichages des incidents d'intrusion dans l'interface Web, vous pouvez activer la journalisation dans les installations Syslog ou envoyer des données d'événements à un serveur de déroutement SNMP. Par politique, vous pouvez préciser les limites de notification d'incidents d'intrusion, configurer la notification d'incidents d'intrusion aux installations de journalisation externes et configurer les réponses externes aux incidents d'intrusion. Notez qu'en plus de ces configurations d'alertes par politique, vous pouvez activer ou désactiver globalement les alertes par courriel sur les incidents d'intrusion pour chaque règle ou groupe de règles. Les paramètres de vos alertes par courriel sont utilisés, quelles que soient la politique de prévention des intrusions qui traite un paquet.

Limites des politiques personnalisées

Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** veiller à ce que votre configuration permette à l'analyse de réseau et à l'inspection de réseau, au traitement et à l'examen d'un seul paquet de se compléter.

Par défaut, le système utilise une politique d'analyse de réseau pour prétraiter tout le trafic géré par les périphériques gérés à l'aide d'une seule politique de contrôle d'accès. Le diagramme suivant montre comment une nouvelle politique de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic. Les phases de prétraitement et de prévention des intrusions sont mises en surbrillance.

Remarquez comment une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic géré par la politique de contrôle d'accès. Au départ, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique par défaut.

Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut. Toutefois, si vous désactivez un inspecteur dans une politique d'analyse de réseau personnalisée, mais que le système doit évaluer les paquets prétraités par rapport à une règle de prévention des intrusions ou d'inspecteur activée, le système active et utilise automatiquement l'inspecteur, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

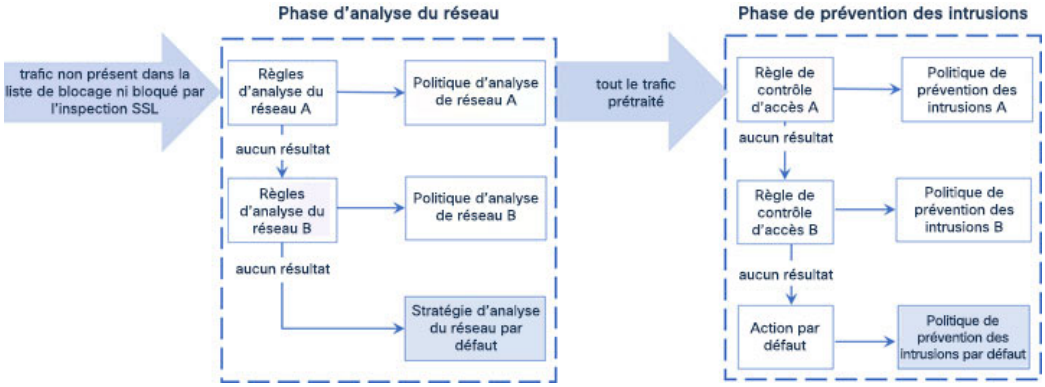
Remarque Afin de profiter des avantages liés à la désactivation d'un inspecteur en matière de performances, vous **devez** vous assurer qu'aucune de vos politiques de prévention des intrusions ne comporte de règles activées nécessitant cet inspecteur.

Un défi supplémentaire survient si vous utilisez plusieurs politiques d'analyse de réseau personnalisées. Pour les utilisateurs avancés avec des déploiements complexes, vous pouvez adapter le prétraitement à des zones de sécurité, à des réseaux et à des VLAN spécifiques en attribuant des politiques d'analyse de réseau personnalisées pour prétraiter le trafic correspondant. (Notez qu'ASA FirePOWER ne peut pas restreindre le prétraitement par VLAN.) Pour ce faire, ajoutez des *règles d'analyse de réseau* personnalisées à votre politique de contrôle d'accès. Chaque règle est associée à une politique d'analyse de réseau qui régit le prétraitement du trafic correspondant à la règle.

Astuces Vous configurez les règles d'analyse de réseau en tant que paramètre avancé dans une politique de contrôle d'accès. Contrairement à d'autres types de règles, les règles d'analyse de réseau font appel à des politiques d'analyse de réseau plutôt que d'être contenues par.

Le système fait correspondre les paquets à des règles d'analyse de réseau configurées en ordre descendant par numéro de règle. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut. Bien que cela vous permette une grande souplesse dans le prétraitement du trafic, gardez à l'esprit que tous les paquets, **quelle que soit** la politique d'analyse de réseau qui les ont prétraités, sont par la suite mis en correspondance avec les règles de contrôle d'accès, et donc à l'inspection potentielle par les politiques de prévention des intrusions, dans leur propre processus. . En d'autres termes, le prétraitement d'un paquet avec une politique d'analyse de réseau particulière ne garantit **pas** que le paquet sera examiné avec une politique de prévention des intrusions particulière. Vous **devez** configurer avec soin votre politique de contrôle d'accès afin qu'elle fasse appel aux politiques d'analyse de réseau et de prévention des intrusions appropriées pour évaluer un paquet particulier.

Le diagramme suivant montre de manière très détaillée comment la phase de sélection de la politique d'analyse de réseau (prétraitement) se produit avant la phase de prévention des intrusions (règles) et séparément. Par souci de simplicité, le diagramme élimine les phases de découverte et d'inspection des fichiers et des programmes malveillants. Il met également en évidence les politiques d'analyse de réseau et d'action par défaut contre les intrusions par défaut.



Dans ce scénario, une politique de contrôle d'accès est configurée avec deux règles d'analyse de réseau et une politique d'analyse de réseau par défaut :

- La règle d'analyse de réseau A prétraite le trafic correspondant avec la politique d'analyse de réseau A. Vous souhaitez que ce trafic soit inspecté ultérieurement par la politique de prévention des intrusions A.
- La règle d'analyse de réseau B prétraite le trafic correspondant avec la politique d'analyse de réseau B. Vous souhaitez que ce trafic soit inspecté ultérieurement par la politique de prévention des intrusions B.
- Tout le trafic restant est prétraité avec la politique d'analyse de réseau par défaut. Plus tard, vous souhaitez que ce trafic soit inspecté par la politique de prévention des intrusions associée à l'action par défaut de la politique de contrôle d'accès.

Une fois que le système a prétraité le trafic, il peut examiner le trafic pour détecter des intrusions. Le diagramme montre une politique de contrôle d'accès avec deux règles de contrôle d'accès et une action par défaut :

- La règle de contrôle d'accès A permet la mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions A.
- La règle de contrôle d'accès B permet de mettre en correspondance le trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions B.
- L'action par défaut de la politique de contrôle d'accès permet une mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions de l'action par défaut.

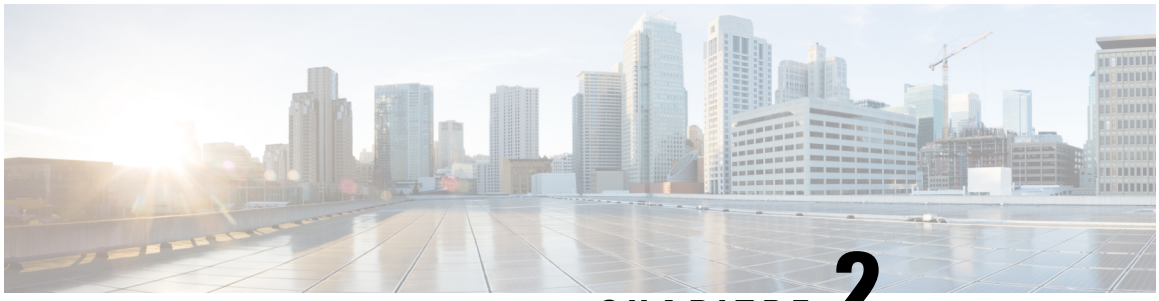
Le traitement de chaque paquet est régi par une paire de politiques d'analyse de réseau et de politiques de prévention des intrusions, mais le système ne coordonne **pas** la paire pour vous. Voici un scénario dans lequel vous configurez mal votre politique de contrôle d'accès de sorte que la règle d'analyse de réseau A et la règle de contrôle d'accès A ne traitent pas le même trafic. Par exemple, vous pouvez vouloir que les politiques jumelées régissent le traitement du trafic sur une zone de sécurité particulière, mais vous utilisez par erreur des zones différentes dans les conditions des deux règles. Cela pourrait entraîner un prétraitement incorrect du trafic. Pour cette raison, la personnalisation du prétraitement à l'aide de règles d'analyse de réseau et de politiques personnalisées est une tâche **avancée**.

Veuillez noter que pour une connexion unique, bien que le système sélectionne une politique d'analyse de réseau avant une règle de contrôle d'accès, un certain prétraitement (notamment le prétraitement de la couche d'application) a lieu après la sélection de la règle de contrôle d'accès. Cela n'affecte **pas** la façon dont vous configurez le prétraitement dans les politiques d'analyse de réseau personnalisées.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.



CHAPITRE 2

Migrer de Snort 2 vers Snort 3

À partir de la version 7.0, Snort 3 est la plateforme d'inspection par défaut des nouveaux déploiements Threat Defense avec centre de gestion. Si vous utilisez toujours la plateforme d'inspection Snort 2, optez dès à présent pour Snort 3 afin de bénéficier d'une détection et de performances améliorées.

La mise à niveau de Threat Defense vers les versions 7.2 à 7.6 met également à niveau les périphériques Snort 2 éligibles vers Snort 3. Pour les périphériques qui ne sont pas éligibles, car ils utilisent des politiques de prévention des intrusions ou d'analyse de réseau personnalisées, procédez à une mise à niveau manuelle vers Snort 3, comme décrit ici.

Bien qu'il soit possible de rétablir des périphériques individuels, cette action est déconseillée. Snort 2 sera obsolète dans une prochaine version et empêchera éventuellement la mise à niveau de Threat Defense .

Plateforme d'inspection Snort 3

Snort 3 est le moteur d'inspection par défaut pour les périphériques Threat Defense nouvellement enregistrés, avec les versions 7.0 ou ultérieures. Cependant, pour les périphériques Threat Defense de versions antérieures, Snort 2 est le moteur d'inspection par défaut. Lorsque vous mettez à niveau un périphérique géré Threat Defense vers la version 7.0 ou une version ultérieure, le moteur d'inspection reste sur Snort 2. Pour utiliser Snort 3 dans les Threat Defense mis à niveau à partir de la version 7.0 ou des versions ultérieures, vous devez l'activer explicitement. Lorsque Snort 3 est activé comme moteur d'inspection du périphérique , la version Snort 3 de la politique de prévention des intrusions qui est appliquée au périphérique (par les politiques de contrôle d'accès) est activée et appliquée à tout le trafic passant par le périphérique.

Vous pouvez changer de version de Snort au besoin. Les règles de prévention des intrusions Snort 2 et Snort 3 sont mappées et le mappage est fourni par le système. Cependant, vous pourriez ne pas trouver de mappage individuel de toutes les règles de prévention des intrusions dans Snort 2 et Snort 3. Si vous modifiez l'action de règle pour une règle dans Snort 2, cette modification n'est pas conservée si vous passez à Snort 3 sans synchroniser Snort 2 avec Snort 3. Pour plus d'informations sur la synchronisation, voir Synchroniser les règles de Snort 2 avec celles de Snort 3, à la page 27.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Comment migrer de Snort 2 vers Snort 3

La migration de Snort 2 vers Snort 3 nécessite de basculer le moteur d'inspection du périphérique Threat Defense de Snort 2 à Snort 3.

Selon vos besoins, les tâches pour terminer la migration de votre périphérique de Snort 2 vers Snort 3 sont énumérées dans le tableau suivant :

Étape	Tâche	Liens vers les procédures
1	Activer Snort 3	• Activer Snort 3 sur un périphérique individuel, à la page 23 • Activer Snort 3 sur plusieurs périphériques, à la page 23
2	Convertir les règles personnalisées de Snort 2 en Snort 3	• Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3, à la page 25 • Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 26
3	Synchroniser les règles de Snort 2 avec celles de Snort 3	Synchroniser les règles de Snort 2 avec celles de Snort 3, à la page 27

Conditions préalables à la migration de Snort 2 vers Snort 3

Voici les conditions préalables recommandées que vous devez prendre en compte avant de migrer votre périphérique de Snort 2 vers Snort 3.

- Avoir une connaissance pratique de Snort. Pour en savoir plus sur l'architecture de Snort 3, consultez la section Adoption de Snort 3.
- Sauvegardez le centre de gestion. Reportez-vous à la section Sauvegarder le centre de gestion.
- Sauvegardez votre politique de prévention des intrusions. Voir Exportation des configurations.
- Copiez votre politique de prévention des intrusions. Pour ce faire, vous pouvez utiliser une politique existante comme politique de base pour créer une copie de votre politique de prévention des intrusions. Dans la page **Intrusion Policies** (Politiques de prévention des intrusions), cliquez sur **Create Policy**

(créer une politique) et choisissez une politique de prévention des intrusions existante dans la liste déroulante **Base Policy** (Politique de base).

Activer Snort 3 sur un périphérique individuel

Important Pendant le processus de déploiement, il peut y avoir une perte de trafic momentanée car le moteur d'inspection actuel doit être arrêté.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur le périphérique pour accéder à sa page d'accueil.

Remarque
Le périphérique est marqué comme Snort 2 ou Snort 3, ce qui affiche la version actuelle sur le périphérique.

Étape 3 Cliquez sur l'onglet **Device** (appareil).

Étape 4 Dans la section Inspection Engine (moteur d'inspection), cliquez sur **Mettre à niveau**.

Remarque
Si vous souhaitez désactiver Snort 3, cliquez sur **Revert to Snort 2** (Restaurer Snort 2) dans la section Inspection Engine (moteur d'inspection).

Étape 5 Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez, Déployer les modifications de configuration, à la page 28.

Le système convertit vos configurations de politiques au cours du processus de déploiement pour les rendre compatibles avec la version sélectionnée de Snort.

Activer Snort 3 sur plusieurs périphériques

Pour activer Snort 3 sur plusieurs périphériques, assurez-vous que tous les périphériques Threat Defense requis utilisent la version 7.0 ou une version ultérieure.

Important Pendant le processus de déploiement, il peut y avoir une perte de trafic momentanée car le moteur d'inspection actuel doit être arrêté.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Sélectionnez tous les périphériques sur lesquels vous souhaitez activer ou désactiver Snort 3.

Remarque
Les périphériques sont marqués comme Snort 2 ou Snort 3 et affichent la version actuelle sur le périphérique.

Étape 3 Cliquez sur la liste déroulante **Select Bulk Action** (sélectionner une action en bloc) et choisissez **Upgrade to Snort 3**(mettre à niveau vers Snort 3).

Remarque
Pour désactiver Snort 3, cliquez sur **Downgrade to Snort 2** (Rétrograder vers Snort 2).

Étape 4 Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez, Déployer les modifications de configuration, à la page 28.

Le système convertit vos configurations de politiques au cours du processus de déploiement pour les rendre compatibles avec la version sélectionnée de Snort.

Convertir les règles IPS personnalisées de Snort 2 en Snort 3

Si vous utilisez un ensemble de règles d'un fournisseur tiers, communiquez avec ce fournisseur pour confirmer que ses règles ont été converties avec succès vers Snort 3 ou pour obtenir un ensemble de règles de remplacement écrit de manière native pour Snort 3. Si vous avez des règles personnalisées que vous avez écrites vous-même, familiarisez-vous avec la rédaction des règles de Snort 3 avant la conversion, afin de pouvoir mettre à jour vos règles et optimiser la détection de Snort 3 après la conversion. Consultez les liens ci-dessous pour en savoir plus sur l'écriture de règles dans Snort 3.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Vous pouvez consulter d'autres blogs à l'adresse https: // blog.snort.org/ pour en savoir plus sur les règles Snort 3.

Consultez les procédures suivantes pour convertir les règles Snort 2 en règles Snort 3 à l'aide de l'outil fourni par le système.

- Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3, à la page 25
- Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 26

Important Les paramètres de politique d'analyse de réseau (NAP) de Snort 2 *ne peuvent pas* être copiés dans Snort 3 automatiquement. Les paramètres de Politique d'analyse de réseau (NAP) doivent être répliqués manuellement dans Snort 3.

Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Assurez-vous que **Toutes les règles** est sélectionné dans le volet gauche.

Étape 4 Cliquez sur la liste déroulante **Tasks** (Tâches) et sélectionnez :

- (Convertir et importer) **Convert Snort 2 rules and import** (Convertir les règles de Snort 2 et les importer) : pour convertir automatiquement toutes les règles personnalisées Snort 2 dans toutes les politiques de prévention des intrusions vers Snort 3 et les importer dans centre de gestion en tant que règles personnalisées Snort 3.
- (Convertir et télécharger) **Convert Snort 2 Rules and download** (Convertir les règles Snort 2 et les télécharger) : pour convertir automatiquement toutes les règles personnalisées de Snort 2 pour toutes les politiques de prévention des intrusions vers Snort 3 et les télécharger dans votre système local.

Étape 5 Cliquez sur **OK**.

Remarque

- Si vous avez sélectionné **Convert and import** à l'étape précédente, alors toutes les règles converties sont enregistrées dans un nouveau groupe de règles **All Snort 2 Converted Global** sous **Local Rules** (Règles locales).
- Si vous avez sélectionné **Convert and download** à l'étape précédente, enregistrez le fichier de règles localement. Vous pouvez consulter les règles converties dans le fichier téléchargé et les téléverser ultérieurement en suivant les étapes décrites dans Ajouter des règles personnalisées aux groupes de règles, à la page 56.

Reportez-vous à la vidéo Conversion des règles Snort 2 en règles Snort 3 pour obtenir de l'aide et des renseignements supplémentaires.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Dans l'onglet **Intrusion Policies** (politiques de prévention des intrusions), cliquez sur **Show Snort 3 Sync status** (Afficher l'état de la synchronisation Snort).

Étape 3 Cliquez sur l'icône **Sync Désynchronisation de Snort** ( ) de la politique de prévention des intrusions.

Remarque
Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur verte**Versions Snort synchronisées** ( ). Cela indique qu'il n'y a aucune règle personnalisée à convertir.

Étape 4 Lisez le résumé et cliquez sur l'onglet **Règles personnalisées**.

Étape 5 Choisissez :

- **Importer les règles converties dans cette politique** : pour convertir les règles personnalisées de Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans centre de gestion en tant que règles personnalisées de Snort 3.
- **Télécharger les règles converties** : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les télécharger dans votre système local. Vous pouvez consulter les règles converties dans le fichier téléchargé, puis téléverser le fichier ultérieurement en cliquant sur l'icône de chargement.

Étape 6 Cliquez sur **Re-Sync** (Resynchroniser).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Afficher le mappage de politique de base Snort 2 et Snort 3

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.

Étape 3 Cliquez sur **IPS Mapping** (Mappage IPS).

Étape 4 Dans la boîte de dialogue **IPS Policy Mapping** (Mappage de politique IPS), cliquez sur **View Mappings** (Afficher les mappages) pour afficher le mappage de la politique de prévention des intrusions de Snort 3 à Snort 2.

Étape 5 Cliquez sur **OK**.

Synchroniser les règles de Snort 2 avec celles de Snort 3

Pour s'assurer que les paramètres et les règles personnalisées de la version Snort 2 sont conservés et transférés dans Snort 3, centre de gestion fournit la fonctionnalité de synchronisation. La synchronisation aide les paramètres de règles de Snort 2 à remplacer les règles et les paramètres de règles personnalisées, que vous avez peut-être modifiés et ajoutés au cours des derniers mois ou années, pour être répliqués sur la version Snort 3. Cet utilitaire sert à synchroniser la configuration de la politique de Snort 2 avec la version de Snort 3 pour commencer avec une couverture semblable.

Si centre de gestion est mis à niveau de la version 6.7 ou antérieure vers la version 7.0 ou ultérieure, le système synchronise la configuration. S'il s'agit d'une nouvelle version 7.0 ou d'une version ultérieure, vous pouvez effectuer une mise à niveau vers une version ultérieure centre de gestion. Le système ne synchronisera aucun contenu pendant la mise à niveau.

Avant de mettre à niveau un appareil vers Snort 3, si des modifications sont apportées à la version de Snort 2, vous pouvez vous servir de cet utilitaire afin d'obtenir la dernière synchronisation de la version de Snort 2 vers la version de Snort 3 et ainsi commencer avec une couverture semblable.

Remarque Après le passage vers Snort 3, il est recommandé de gérer la version Snort 3 de la politique de façon indépendante et de ne pas utiliser cet utilitaire comme fonctionnement normal.

Important

- Seuls les remplacements de règles Snort 2 et les règles personnalisées sont copiés dans Snort 3 et non le contraire. Il se peut que vous ne trouviez pas de mappage individuel de toutes les règles de prévention des intrusions dans Snort 2 et Snort 3 Vos modifications apportées aux actions liées aux règles pour les règles qui existent dans les deux versions sont synchronisées lorsque vous effectuez la procédure suivante.
- La synchronisation *ne migre pas* les paramètres de seuil et de suppression des règles personnalisées ou fournies par le système de Snort 2 vers Snort 3.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.

Étape 3 Cliquez sur **Afficher l'état de synchronisation de Snort 3**

Étape 4 Déterminez la politique de prévention des intrusions désynchronisée.

Étape 5 Cliquez sur l'icône **Sync Désynchronisation de Snort** ( ).

Remarque
Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur verte**Versions Snort synchronisées** ( ).

Étape 6 Lisez le résumé et téléchargez-en une copie si nécessaire.

Étape 7 Cliquez sur **Re-Sync** (Resynchroniser).

Remarque

- Les paramètres synchronisés ne seront applicables sur le moteur de prévention des intrusions Snort 3 que s'ils sont appliqués sur un périphérique et après un déploiement réussi.
- Les règles personnalisées Snort 2 peuvent être converties vers Snort 3 à l'aide de l'outil fourni par le système. Si vous avez des règles personnalisées Snort 2, cliquez sur l'onglet Règles personnalisées et suivez les instructions à l'écran pour convertir les règles. Pour en savoir plus, consultez Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 26.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Déployer les modifications de configuration

Après avoir modifié les configurations, déployez-les sur les appareils ciblés.

Remarque Cette rubrique couvre les étapes de base du déploiement des modifications de configuration. Nous vous recommandons *fortement* de consulter la rubrique sur le *déploiement des modifications de configuration* dans la dernière version du *Guide de configuration Cisco Secure Firewall Management Center* pour comprendre les conditions préalables et les conséquences du déploiement des modifications avant de poursuivre les étapes.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic.

Procédure

Étape 1 Dans la barre de menus Cisco Secure Firewall Management Center, cliquez sur **Deploy** (déployer) puis sélectionnez **Deployment** (déploiement).

La page de GUI répertorie les périphériques dont les configurations sont obsolètes et dont l'état est en **attente**.

- La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets. En développant la liste des appareils, vous pouvez afficher les utilisateurs qui ont modifié les politiques par rapport à chaque liste de politiques.

  Remarque
  Les noms d'utilisateur ne sont pas fournis pour les politiques et objets supprimés.

- La colonne **Inspect Interruption** (inspecter l'interruption) indique si une interruption de l'inspection du trafic peut se produire dans le périphérique pendant le déploiement.

Si cette colonne est vide pour un périphérique, cela signifie qu'il n'y aura pas d'interruption de l'inspection du trafic sur ce périphérique pendant le déploiement.

- La colonne **Last Modified Time** (heure de la dernière modification) indique la dernière fois que vous avez modifié la configuration.
- La colonne **Preview** (aperçu) vous permet de prévisualiser les modifications pour le prochain déploiement.
- La colonne **Status** (état) indique l'état de chaque déploiement.

Étape 2 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Expand (développer) : cliquez sur **Flèche Développer** ( ) pour afficher les modifications de configuration propres au périphérique à déployer.

  Lorsque vous cochez une case à côté d'un périphérique, toutes les modifications apportées au périphérique et répertoriées sous ce dernier sont transmises pour déploiement. Cependant, vous pouvez utiliser **Sélection de politique** ( ) pour sélectionner des politiques ou des configurations spécifiques à déployer tout en conservant les modifications restantes sans les déployer.

  Remarque
  - Lorsque l'état de la colonne **Inspect Interruption** (interruption de l'inspection) indique (**Yes** (oui)) que le déploiement interrompra l'inspection, et peut-être le trafic, sur un appareil Threat Defense, la liste étendue indique les configurations particulières causant l'interruption avec **Inspecter l'interruption** ( ).
  - Lorsque des changements sont apportés aux groupes d'interface, aux zones de sécurité ou aux objets, les appareils touchés sont affichés comme étant périmés sur centre de gestion. Pour vous assurer que ces modifications prennent effet, les politiques relatives à ces groupes d'interface, zones de sécurité ou objets doivent également être déployées avec les modifications. Les politiques concernées sont indiquées comme étant obsolètes sur la page **Prévisualisation** de centre de gestion.

Étape 3 Cliquez sur **Deploy** (déployer).

Étape 4 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Vous avez les choix suivants :

- Deploy (déployer) : Continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Close (fermer) : Quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

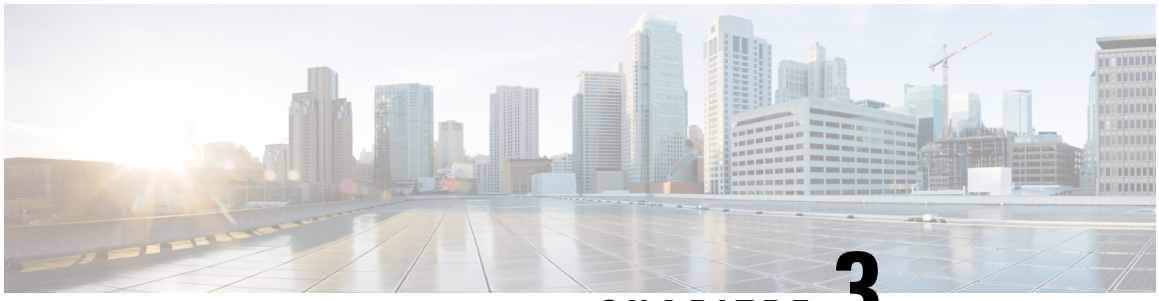
Prochaine étape

Pendant le déploiement, en cas d'échec du déploiement pour quelque raison que ce soit, il est possible que l'échec influe sur le trafic. Cependant, cela dépend de certaines conditions. S'il y a certains changements de configuration dans le déploiement, l'échec du déploiement peut entraîner une interruption du trafic. Pour en

savoir plus, consultez la rubrique sur le déploiement des modifications de la dernière version du *Guide configuration de Cisco Secure Firewall Management Center*.

PARTIE I

Prévention et détection des intrusions dans Snort 3



CHAPITRE 3

Premiers pas avec les politiques de prévention des intrusions Snort 3

Ce chapitre fournit des informations sur la gestion des politiques de prévention des intrusions de Snort 3 et la configuration des règles de contrôle d'accès pour la détection et la prévention des intrusions.

Présentation des politiques de prévention des intrusions

Les *politiques de prévention des intrusions* sont des ensembles définis de configurations de détection et de prévention des intrusions qui inspectent le trafic à la recherche de violations de la sécurité et qui, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. Les politiques de prévention des intrusions sont invoquées par votre politique de contrôle d'accès et constituent la dernière ligne de défense du système avant que le trafic ne soit autorisé à atteindre sa destination.

Les règles de prévention des intrusions sont au cœur de chaque politique de prévention des intrusions. Une règle activée oblige le système à générer des incidents d'intrusion pour le trafic correspondant à la règle (et au bloquer éventuellement). La désactivation d'une règle arrête le traitement de la règle.

Le système fournit plusieurs politiques de base en matière de prévention des intrusions, qui vous permettent de profiter de l'expérience de Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de l'inspecteur (activé ou désactivé), et fournit les configurations initiales pour d'autres paramètres avancés.

Astuces Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions.

Si vous créez une politique de prévention des intrusions personnalisée, vous pouvez :

- Optimiser la détection en activant et en désactivant les règles, ainsi qu'en écrivant et en ajoutant vos propres règles.
- Utilisez les recommandations de Cisco Secure Firewall pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.

Une politique de prévention des intrusions peut abandonner les paquets correspondants et générer des incidents d'intrusion. Pour configurer une règle de prévention des intrusions ou d'abandon de préprocesseur, définissez son état sur Block (Bloquer).

Lorsque vous adaptez votre politique de prévention des intrusions, en particulier lors de l'activation et de l'ajout de règles, gardez à l'esprit que certaines règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Avant qu'une politique de prévention des intrusions n'examine un paquet, le paquet est prétraité selon les configurations d'une politique d'analyse de réseau. Si vous désactivez un inspecteur obligatoire, le système l'utilise automatiquement avec ses paramètres actuels, bien que l'inspecteur reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Mise en garde Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet **doivent** se compléter mutuellement. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**.

Après avoir configuré une politique de prévention des intrusions personnalisée, vous pouvez l'utiliser dans le cadre de votre configuration de contrôle d'accès en associant la politique de prévention des intrusions à une ou plusieurs règles de contrôle d'accès ou à une action par défaut d'une politique de contrôle d'accès. Cela oblige le système à utiliser la politique de prévention des intrusions pour examiner une partie du trafic autorisé avant que le trafic n'atteigne sa destination finale. Un ensemble de variables que vous associez à la politique de prévention des intrusions vous permet de refléter avec précision votre réseau domestique et externe et, le cas échéant, les serveurs de votre réseau.

Notez que par défaut, le système désactive l'inspection des intrusions des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès pour laquelle l'inspection des intrusions est configurée.

Consultez la vidéo pour obtenir de l'aide et des informations supplémentaires concernant la présentation de la politique de prévention des intrusions de Snort 3.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Création d'une politique de prévention des intrusions Snort 3 personnalisée

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Créer une politique**.

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Choisissez le **Mode d'inspection**.

L'action sélectionnée détermine si les règles de prévention des intrusions bloquent et envoient une alerte (mode **prévention**) ou uniquement une alerte (mode **détection**).

Remarque
Avant de sélectionner le mode de prévention, vous pouvez souhaiter que les règles de blocage déclenchent uniquement une alerte afin de pouvoir identifier les règles qui provoquent de nombreux faux positifs.

Étape 5 Choisissez la **politique de base**.

Vous pouvez utiliser une politique fournie par le système ou une politique existante comme politique de base.

Étape 6 Cliquez sur **Save** (enregistrer).

La nouvelle politique a les mêmes paramètres que sa politique de base.

Prochaine étape

Pour personnaliser la politique, consultez Modification des politiques de prévention des intrusions Snort 3, à la page 36.

Modification des politiques de prévention des intrusions Snort 3

Lors de la modification d'une politique Snort 3, toutes les modifications sont enregistrées instantanément. Aucune action supplémentaire n'est requise pour enregistrer les modifications.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Journalisation des actions liées aux règles

À partir de la version Centre de gestion 7.2.0 , sur la page **Intrusion Events** (Événements d'intrusion), l'événement dans la colonne **Inline Result** (Résultat en ligne) affiche le même nom que l'action IPS appliquée à la règle, afin que vous puissiez voir l'action qui a été appliquée au trafic correspondant à la règle.

Pour les actions IPS, le tableau suivant présente les événements affichés dans la colonne **Inline Result** de la page **Intrusion Events** et dans la colonne **Action** pour **Intrusion Event Type** (type d'incident d'intrusion dans la page **Unified Events** (Événements unifiés).

Action IPS pour Snort 3	Résultat en ligne : Centre de gestion 7.1.0 ou versions antérieures	Résultat en ligne : Centre de gestion 7.2.0 et versions ultérieures
Alerte	Réussite	Alerte
Bloquer	Abandonné/aurait dû être abandonné/partiellement abandonné	Bloquer/bloquerait/blocage partiel
Abandonner	Abandonné/aurait abandonné	Abandon/Abandonnerait
Rejeter	Abandonné/aurait abandonné	Rejeter/rejetterait
Réécrire	Autoriser	Réécrire

Important

- Dans le cas d'une règle sans l'option « Replace » (Remplacer), l'action **Rewrite** (Réécriture) est affichée comme « **Wait Rewrite** » (En attente de réécriture).
- L'action de **réécriture** serait également affichée sous la forme **Would rewrite (réécrirait)** si l'option « Replace » est spécifiée, mais que la politique IPS est en mode de détection ou que le périphérique est en mode TAP en ligne/passif.

Remarque

En cas de compatibilité ascendante (Centre de gestion 7.2.0 assurant la gestion d'un périphérique Threat Defense 7.1.0), les événements mentionnés s'appliquent uniquement à l'action Alert IPS (Alerter IPS) (où la mention **Pass** (Réussite) est affichée comme **Alerte** pour les événements. Pour toutes les autres actions, les événements de Centre de gestion 7.1.0 s'appliquent.

Modifier la politique de base d'une politique de prévention des intrusions

Vous pouvez choisir une autre politique personnalisée ou fournie par le système comme politique de base.

Vous pouvez enchaîner jusqu'à cinq politiques personnalisées, quatre d'entre elles utilisant comme politique de base l'une des quatre autres politiques créées précédemment; la cinquième doit utiliser comme base une politique fournie par le système.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Modifier** ( ) à côté de la politique de prévention des intrusions que vous souhaitez configurer.

Étape 3 Choisissez une politique dans la liste déroulante **Base Policy** (politique de base).

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Gérer les politiques de prévention des intrusions

Sur la page de prévention des intrusions (**Policies** > **Intrusion**), vous pouvez afficher vos politiques de prévention des intrusions personnalisées actuelles, ainsi que les informations suivantes :

- Nombre de politiques de contrôle d'accès et de périphériques utilisant la politique de prévention des intrusions pour inspecter le trafic
- Dans un déploiement multidomaine, le domaine dans lequel la politique a été créée

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.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Gérez votre politique de prévention des intrusions :

- Create (créer) : cliquez sur **Create Policy**(créer une politique). voir Création d'une politique de prévention des intrusions Snort 3 personnalisée , à la page 35.

- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté de la politique que vous souhaitez supprimer. Le système vous demande de confirmer et vous informe si un autre utilisateur a des modifications non enregistrées dans la politique. Cliquez sur **OK** pour confirmer.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

- Modifiez les détails de la politique de prévention des intrusions – Cliquez sur **Modifier** ( ) à côté de la politique que vous souhaitez modifier. Vous pouvez modifier le **nom**, le **mode d'inspection** et la **politique de base** de la politique de prévention des intrusions.

- Modifiez les paramètres de politique de prévention des intrusions : cliquez sur **Snort 3 Version** (version Snort 3); voir Modification des politiques de prévention des intrusions Snort 3, à la page 36.

- Exporter : si vous souhaitez exporter une politique de prévention des intrusions pour l'importer sur un autre centre de gestion, cliquez sur Exporter; Reportez-vous à la rubrique *Exportation des configurations* dans la dernière version du Guide de configuration de Cisco Firepower Management Center*Guide de configuration Cisco Secure Firewall Management Center*.

- Deploy (déployer) : choisissez **Deploy** > **Deployment**(déployer > déploiement); voir Déployer les modifications de configuration, à la page 28.

- Report (Rapport) : cliquez sur **Report**(Rapport). ; Consultez la rubrique *Génération des rapports sur les politiques actuelles* dans la dernière version du *Guide de configuration de Cisco Secure Firewall Management Center*. Génère deux rapports, un pour chaque version de politique.

Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions

Une politique de contrôle d'accès peut avoir plusieurs règles de contrôle d'accès associées à des politiques de prévention des intrusions. Vous pouvez configurer l'inspection de prévention des intrusions pour toute règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif), ce qui vous permet de faire correspondre différents profils d'inspection des intrusions avec différents types de trafic sur votre réseau avant qu'il n'atteigne sa destination finale.

Chaque fois que le système utilise une politique de prévention des intrusions pour évaluer le trafic, il utilise un *ensemble de variables* associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles de prévention des intrusions pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles et de règles dynamiques.

Astuces Même si vous utilisez les politiques de prévention des intrusions fournies par le système, Cisco vous recommande **fortement** de configurer les variables du système relatives aux intrusions pour refléter avec exactitude votre environnement réseau. Au minimum, modifiez les variables par défaut dans l'ensemble par défaut.

Comprendre les politiques de prévention des intrusions fournies par le système et personnalisées

Cisco fournit plusieurs politiques de prévention des intrusions avec le système. En utilisant les politiques de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience du Cisco Talos Intelligence Group (Talos). Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les paramètres avancés. Vous pouvez utiliser les politiques fournies par le système telles quelles ou vous pouvez les utiliser comme base pour des politiques personnalisées. L'élaboration de politiques personnalisées peut améliorer les performances du système dans votre environnement et fournir un aperçu plus précis du trafic malveillant et des violations de politiques qui se produisent sur votre réseau.

Journalisation des événements de connexion et d'intrusion

Lorsqu'une politique de prévention des intrusions appelée par une règle de contrôle d'accès détecte une intrusion et génère un incident d'intrusion, elle enregistre cet événement dans le centre de gestion (Management Center). Le système consigne également automatiquement la fin de la connexion où l'intrusion s'est produite dans la base de données du centre de gestion, quelle que soit la configuration de journalisation de la règle de contrôle d'accès.

Configuration des règles de contrôle d'accès et politiques de prévention des intrusions

Le nombre de politiques de prévention des intrusions uniques que vous pouvez utiliser dans une seule politique de contrôle d'accès dépend du modèle des machines cibles; des périphériques plus puissants peuvent en gérer plus. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique. Bien que vous puissiez associer une paire d'ensembles de variables de politique de prévention des intrusions différente à chaque règle d'autorisation et de blocage interactif (ainsi qu'à l'action par défaut), vous ne pouvez pas déployer de politique de contrôle d'accès si les machines cibles disposent de ressources insuffisantes pour effectuer l'inspection configurée.

Configurer une règle de contrôle d'accès pour effectuer la prévention des intrusions

Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, créez une règle ou modifiez une règle existante; Consultez la rubrique *Composants de la règle de contrôle d'accès* dans la dernière version du *Guide de configuration de Cisco Secure Firewall Management Center*.

Étape 2 Assurez-vous que l'action de règle est définie sur **Allow** (autorisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset (blocage interactif) avec réinitialisation**.

Étape 3 Cliquez sur **Inspection**.

Étape 4 Choisissez une politique de prévention des intrusions fournie par le système ou personnalisée, ou choisissez **Aucun** pour désactiver l'inspection de prévention des intrusions pour le trafic qui correspond à la règle de contrôle d'accès.

Étape 5 Si vous souhaitez modifier l'ensemble de variables associé à la politique de prévention des intrusions, choisissez une valeur dans la liste déroulante **Ensemble de variables**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la règle.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Déployer les modifications de configuration

Après avoir modifié les configurations, déployez-les sur les appareils ciblés.

Remarque Cette rubrique couvre les étapes de base du déploiement des modifications de configuration. Nous vous recommandons *fortement* de consulter la rubrique sur le *déploiement des modifications de configuration* dans la dernière version du *Guide de configuration Cisco Secure Firewall Management Center* pour comprendre les conditions préalables et les conséquences du déploiement des modifications avant de poursuivre les étapes.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic.

Procédure

Étape 1 Dans la barre de menus Cisco Secure Firewall Management Center, cliquez sur **Deploy** (déployer) puis sélectionnez **Deployment** (déploiement).

La page de GUI répertorie les périphériques dont les configurations sont obsolètes et dont l'état est en **attente**.

- La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets. En développant la liste des appareils, vous pouvez afficher les utilisateurs qui ont modifié les politiques par rapport à chaque liste de politiques.

  Remarque
  Les noms d'utilisateur ne sont pas fournis pour les politiques et objets supprimés.

- La colonne **Inspect Interruption** (inspecter l'interruption) indique si une interruption de l'inspection du trafic peut se produire dans le périphérique pendant le déploiement.

  Si cette colonne est vide pour un périphérique, cela signifie qu'il n'y aura pas d'interruption de l'inspection du trafic sur ce périphérique pendant le déploiement.

- La colonne **Last Modified Time** (heure de la dernière modification) indique la dernière fois que vous avez modifié la configuration.
- La colonne **Preview** (aperçu) vous permet de prévisualiser les modifications pour le prochain déploiement.
- La colonne **Status** (état) indique l'état de chaque déploiement.

Étape 2 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Expand (développer) : cliquez sur **Flèche Développer** ( ) pour afficher les modifications de configuration propres au périphérique à déployer.

  Lorsque vous cochez une case à côté d'un périphérique, toutes les modifications apportées au périphérique et répertoriées sous ce dernier sont transmises pour déploiement. Cependant, vous pouvez utiliser **Sélection de politique** ( ) pour sélectionner des politiques ou des configurations spécifiques à déployer tout en conservant les modifications restantes sans les déployer.

  Remarque
  - Lorsque l'état de la colonne **Inspect Interruption** (interruption de l'inspection) indique (**Yes** (oui)) que le déploiement interrompra l'inspection, et peut-être le trafic, sur un appareil Threat Defense, la liste étendue indique les configurations particulières causant l'interruption avec **Inspecter l'interruption** ( ).
  - Lorsque des changements sont apportés aux groupes d'interface, aux zones de sécurité ou aux objets, les appareils touchés sont affichés comme étant périmés sur centre de gestion. Pour vous assurer que ces modifications prennent effet, les politiques relatives à ces groupes d'interface, zones de sécurité ou objets doivent également être déployées avec les modifications. Les politiques concernées sont indiquées comme étant obsolètes sur la page **Prévisualisation** de centre de gestion.

Étape 3 Cliquez sur **Deploy** (déployer).

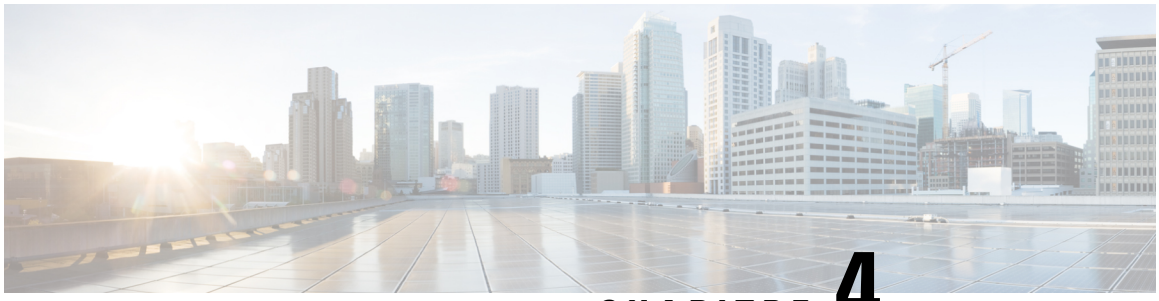
Étape 4 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Vous avez les choix suivants :

- Deploy (déployer) : Continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Close (fermer) : Quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Prochaine étape

Pendant le déploiement, en cas d'échec du déploiement pour quelque raison que ce soit, il est possible que l'échec influe sur le trafic. Cependant, cela dépend de certaines conditions. S'il y a certains changements de configuration dans le déploiement, l'échec du déploiement peut entraîner une interruption du trafic. Pour en savoir plus, consultez la rubrique sur le déploiement des modifications de la dernière version du *Guide configuration de Cisco Secure Firewall Management Center*.



CHAPITRE 4

Régler les politiques de prévention des intrusions à l'aide de règles

Ce chapitre fournit des informations sur les règles personnalisées dans Snort 3, les actions liées aux règles de prévention des intrusions, les filtres de notification d'incidents d'intrusion dans une politique de prévention des intrusions, la conversion des règles personnalisées de Snort 2 vers Snort 3 et l'ajout de groupes de règles avec des règles personnalisées à une politique de prévention des intrusions.

Présentation du réglage des règles de prévention des intrusions

Vous pouvez configurer des états de règles et d'autres paramètres pour les règles d'objets partagés, les règles de texte standard et les règles d'inspecteur.

Vous activez une règle en réglant son état à Alerte ou à Bloquer. L'activation d'une règle permet au système de générer des événements sur le trafic correspondant à la règle. La désactivation d'une règle arrête le traitement de la règle. Vous pouvez également définir votre politique de prévention des intrusions de sorte qu'un ensemble de règles comme Block (Bloquer) génère des événements et abandonne le trafic correspondant.

Vous pouvez filtrer les règles pour afficher un sous-ensemble de règles, ce qui vous permet de sélectionner l'ensemble de règles exact pour lequel vous souhaitez modifier l'état ou les paramètres des règles.

Lorsqu'une règle de prévention des intrusions ou un arguments de règle nécessite un inspecteur désactivé, le système l'utilise automatiquement avec sa configuration actuelle, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Remarque Nous vous recommandons de ne pas modifier les règles d'objets partagés et d'activer ou de désactiver ces règles pour votre périphérique Threat Defense. Pour créer des règles Snort personnalisées, contactez le service d'assistance Cisco.

Règles de prévention des intrusions

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments que le système utilise pour détecter les tentatives d'exploitation des vulnérabilités de votre réseau. Lorsque le système analyse le trafic réseau, il compare les paquets aux conditions spécifiées dans chaque règle et déclenche la règle si le paquet de données répond à toutes les conditions spécifiées dans cette dernière.

Une politique de prévention des intrusions contient :

- *les règles de prévention des intrusions*, qui sont subdivisées en *règles d'objets partagés* et en *règles de texte standard.*
- *les règles de l' inspecteur*, qui sont associées à une option de détection du décodeur de paquets ou à l'un des inspecteurs inclus avec le système

Le tableau suivant résume les attributs de ces types de règles :

Tableau 2 : Règles de prévention des intrusions

Type	ID de générateur (GID)	ID Snort (SID)	Source	Puis-je copier?	Puis-je effectuer des modifications?
Règle des objets partagés	3	inférieur à 1000000	Cisco Talos Intelligence Group (Talos)	oui	limité
Règle de texte standard	1 (Domaine global ou GID existant)	inférieur à 1000000	Talos	oui	limité
	1000 - 2000 (domaine descendant)	1000000 ou plus	Créé ou importé par l'utilisateur	oui	oui
règle de préprocesseur	propre au décodeur ou au préprocesseur	inférieur à 1000000	Talos	Non	Non
		1000000 ou plus	Généré par le système lors de la configuration des options	Non	Non

Vous ne pouvez pas enregistrer les modifications d'une règle créée par Talos, mais vous pouvez enregistrer une copie d'une règle modifiée en tant que règle personnalisée. Vous pouvez modifier les variables utilisées dans la règle ou les informations d'en-tête de règle (comme les ports source et de destination et les adresses IP). Dans un déploiement multidomaine, les règles créées par Talos appartiennent au domaine global. Les administrateurs des domaines descendants peuvent enregistrer des copies locales des règles, qu'ils peuvent ensuite modifier.

Pour les règles qu'il crée, Talos attribue des états de règles par défaut dans chaque politique de prévention des intrusions par défaut. La plupart des règles de préprocesseur sont désactivées par défaut et doivent être activées si vous souhaitez que le système génère des événements pour les règles de préprocesseur et, dans un déploiement en ligne, abandonne les paquets fautifs.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Règles personnalisées dans Snort 3

Vous pouvez créer une règle de prévention des intrusions personnalisée en important un fichier de règle local. Le fichier de règles peut avoir une extension `.txt` ou `.rules`. Le système enregistre la règle personnalisée dans la catégorie de règle locale, quelle que soit la méthode que vous avez utilisée pour la créer. Une règle personnalisée doit appartenir à un groupe de règles. Cependant, une règle personnalisée peut également faire partie de deux groupes ou plus.

Lorsque vous créez une règle de prévention des intrusions personnalisée, le système lui attribue un numéro de règle unique, qui a le format `GID:SID:Rev`. Les éléments composant ce numéro sont les suivants :

- **GID** : ID de générateur. Pour les règles personnalisées, il n'est pas nécessaire de préciser le GID. Le système génère automatiquement le GID lors du chargement des règles selon que vous vous trouvez dans le domaine global ou dans un sous-domaine. Pour toutes les règles de texte standard, cette valeur est de 2 000 pour un domaine global.
- **SID** : ID Snort. Indique s'il s'agit d'une règle locale d'une règle système. Lorsque vous créez une règle, attribuez-lui un SID unique.

  Les numéros SID des règles locales commencent à 1000000 et le SID de chaque nouvelle règle locale est incrémenté de un.
- **Rev** : le numéro de la révision. Pour une nouvelle règle, le numéro de révision est de 1. Chaque fois que vous modifiez une règle personnalisée, le numéro de révision doit être incrémenté de un.

Dans une règle de texte standard personnalisée, vous définissez les paramètres d'en-tête de règle ainsi que les mots-clés et les arguments de la règle. Vous pouvez utiliser les paramètres d'en-tête de règle pour axer la règle de manière à ce qu'elle ne corresponde qu'au trafic utilisant un protocole spécifique et circulant vers ou à partir d'adresses IP ou de ports spécifiques.

Pour vérifier si un SID est activé ou désactivé, consultez les entrées du fichier snort.lua situé dans le répertoire `./file-contents/ngfw/var/sf/detection_engines/<id>/ips/<id>`.

- Si le SID est désactivé par défaut, aucune entrée n'est présente dans le fichier.
- Si le SID est activé manuellement, vous noterez la présence d'une entrée **enable:yes**.
- Si le SID est désactivé après avoir été activé manuellement, l'entrée reste dans le fichier et affiche **enable:no**.

Remarque

- Les règles personnalisées Snort 3 ne peuvent pas être modifiées. Assurez-vous que les règles personnalisées comportent un message de classification valide pour `classtype` dans le texte de la règle. Si vous importez une règle sans classification ou avec une mauvaise classification, supprimez et recréez la règle.
- Vous pouvez créer des règles de prévention des intrusions personnalisées dans Snort 3. Cependant, la prise en charge du réglage et de la résolution de problèmes liés à ces règles n'est pas disponible pour le moment.

Afficher les règles de prévention des intrusions Snort 3 dans une politique de prévention des intrusions

Vous pouvez régler l'affichage des règles dans la politique de prévention des intrusions. Vous pouvez également afficher les détails d'une règle spécifique pour voir les paramètres de la règle, la documentation de la règle et d'autres caractéristiques de la règle.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Version Snort 3** à côté de la politique.

Étape 3 Lors de l'affichage des règles, vous pouvez :

- Filtrer les règles.
- Choisir un groupe de règles pour afficher les règles associées à ce groupe.
- Afficher les détails d'une règle de prévention des intrusions.
- Afficher les commentaires des règles.
- Afficher la documentation de la règle.

Consultez Modification des politiques de prévention des intrusions Snort 3, à la page 36 pour en savoir plus sur l'exécution de ces tâches.

Action de règle de prévention des intrusions

Intrusion Rule action (action de règle de prévention des intrusions) vous permet d'activer ou de désactiver la règle dans une politique de prévention des intrusions individuelle, ainsi que de spécifier l'action que le système entreprend si des conditions surveillées déclenchent l'application de la règle.

Le groupe Intelligence Cisco Talos (Talos) définit l'action par défaut de chaque règle de prévention des intrusions et d'inspecteur dans chaque politique par défaut. Par exemple, une règle peut être activée dans la politique par défaut de Sécurité avant la connectivité et désactivée dans la politique par défaut de Connectivité avant la sécurité. Talos utilise parfois une mise à jour de règle pour modifier l'action par défaut d'une ou plusieurs règles dans une politique par défaut. Si vous autorisez les mises à jour de règles à mettre à jour votre politique de base, vous autorisez également la mise à jour de règles à modifier l'action par défaut d'une règle de votre politique lorsque l'action par défaut change dans la politique par défaut que vous avez utilisée pour créer votre politique (ou dans la politique par défaut sur laquelle elle est basée). Notez, cependant, que si vous avez modifié l'action de règle, la mise à jour de la règle ne remplace pas votre modification.

Lorsque vous créez une règle de prévention des intrusions, elle hérite des actions par défaut des règles de la politique par défaut que vous utilisez pour créer votre politique.

Options d'actions liées aux règles de prévention des intrusions

Dans une politique de prévention des intrusions, vous pouvez définir l'action d'une règle sur les valeurs suivantes :

Alerte

Vous souhaitez que le système détecte une tentative de prévention des intrusions spécifique et génère un incident d'intrusion lorsqu'il trouve le trafic correspondant. Lorsqu'un paquet malveillant traverse votre réseau et déclenche la règle, le paquet est envoyé à sa destination et le système génère un incident d'intrusion. Le paquet malveillant atteint sa cible, mais vous en êtes averti par la journalisation des événements.

Bloquer

Vous souhaitez que le système détecte une tentative de prévention des intrusions spécifique, abandonne le paquet contenant l'attaque et génère un incident d'intrusion lorsqu'il trouve le trafic correspondant. Le paquet malveillant n'atteint jamais sa cible et vous en êtes averti par la journalisation des événements.

Désactiver

Vous ne voulez pas que le système évalue le trafic correspondant.

Remarque Choisissez les options **Alerte** ou **Bloquer** pour activer la règle. Choisir **Désactiver** désactive la règle.

Nous vous recommandons **vivement** de **ne pas** activer toutes les règles d'intrusion dans une politique de prévention des intrusions. Les performances de votre périphérique géré sont susceptibles de se dégrader si toutes les règles sont activées. Au lieu de cela, ajustez votre ensemble de règles pour qu'il se conforme le plus possible à votre environnement réseau.

Définir une action de règle de prévention des intrusions

Les états des règles de prévention des intrusions sont propres à la politique.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Snort 3 Version** à côté de la politique que vous souhaitez modifier.

Astuces

Cette page affiche le nombre total de :

- Règles désactivées
- Règles activées définies sur Alerte
- Règles activées définies sur Blocage
- Règles remplacées

Étape 3 Choisissez la ou les règles pour lesquelles vous souhaitez définir l'action de la règle.

Étape 4 Choisissez une des actions liées à une règle dans la liste déroulante **Rule Action** (Actions des règles). Consultez Modification des politiques de prévention des intrusions Snort 3, à la page 36 pour plus d'informations sur les différentes actions de règle.

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

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Filtres de notification d'incident d'intrusion dans une politique d'intrusion

L'importance d'un incident d'intrusion peut être fonction de sa fréquence ou de l'adresse IP source ou de destination. Dans certains cas, vous pouvez ne pas vous soucier d'un événement tant qu'il ne se produit pas un certain nombre de fois. Par exemple, vous pourriez ne pas être concerné si quelqu'un tente de se connecter à un serveur avant d'échouer un certain nombre de fois. Dans d'autres cas, vous n'aurez peut-être besoin que de quelques occurrences pour savoir qu'il y a un problème généralisé. Par exemple, si une attaque DoS est lancée contre votre serveur Web, vous n'aurez peut-être besoin de voir que quelques occurrences d'un incident d'intrusion pour savoir que vous devez corriger la situation. Le fait de constater des centaines d'événements identiques ne fait que submerger votre système.

Seuils de incidents d'intrusion

Vous pouvez définir des seuils pour des règles individuelles, afin de limiter le nombre de fois où le système enregistre et affiche un incident d'intrusion, en fonction du nombre de fois où l'événement est généré au cours d'une période donnée. Cela peut vous éviter d'être submergé par un grand nombre d'événements identiques. Vous pouvez définir des seuils par règle d'objet partagé, règle de texte standard ou règle d'inspecteur.

Définir les seuils d'incidents d'intrusion

Pour définir un seuil, spécifiez d'abord le type de seuil.

Tableau 3 : Options de seuil

Option	Description
Limite	Consigne et affiche les événements à propos du nombre de paquets spécifiés (spécifiés par la quantité d'arguments) qui déclenchent la règle pendant la période spécifiée. Par exemple, si vous définissez le type sur **Limite**, le **nombre** sur `10` et les **Secondes** sur `60`, et que 14 paquets déclenchent la règle, le système arrête de consigner les événements de la règle après avoir affiché les 10 premiers qui se produisent dans la même minute.
Seuil	Journalise et affiche un événement unique lorsque le nombre spécifié de paquets (spécifié par l'argument Nombre) déclenche la règle au cours de la période spécifiée. Notez que le compteur de l'heure redémarre une fois que vous avez atteint le nombre seuil d'événements et que le système enregistre cet événement. Par exemple, vous définissez le type sur **Seuil**, le **Nombre** sur `10` et **Secondes** à `60`, et la règle se déclenche 10 fois avant la 33ème seconde. Le système génère un événement, puis réinitialise les compteurs des secondes et du nombre à zéro. La règle se déclenche ensuite 10 autres fois dans les 25 secondes suivantes. Comme les compteurs sont réinitialisés à 0 à la 33ème seconde, le système enregistre un autre événement.
Les deux	Enregistre et affiche un événement une fois par période spécifiée, après qu'un nombre spécifié (le nombre) de paquets déclenche l'application de la règle. Par exemple, si vous définissez le type sur **Les deux**, **Nombre** sur deux, et **Secondes** sur `10`, il en résulte le décompte des événements suivants : • Si la règle est déclenchée une fois toutes les 10 secondes, le système ne génère aucun événement (le seuil n'est pas atteint) • Si la règle est déclenchée deux fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche pour la deuxième fois). • Si la règle est déclenchée quatre fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche la deuxième fois, et les événements suivants sont ignorés)

Ensuite, spécifiez le suivi, qui détermine si le seuil d'événement est calculé par adresse IP source ou de destination.

Tableau 4 : Options IP de seuil

Option	Description
Source	Calcule le nombre d'instances d'événement par adresse IP source.
Destination	Calcule le nombre d'instances d'événement par adresse IP de destination.

Enfin, spécifiez le nombre d'instances et la période qui définissent le seuil.

Tableau 5 : Options de durée/instance de seuil

Option	Description
Quantité	Le nombre d'instances d'événement par période spécifiée et par adresse IP de suivi requise pour atteindre le seuil.
Secondes	Nombre de secondes qui s'écoulent avant la réinitialisation du nombre. Si vous définissez le type de seuil sur **limite**, le suivi sur **l'adresse IP source**, le **nombre** sur `10` et les **secondes** sur `10`, le système journalise et affiche les 10 premiers événements qui se produisent durant 10 secondes à partir d'un port source donné. Si seulement 7 événements se produisent dans les 10 premières secondes, le système les consigne et les affiche; si 40 événements se produisent dans les 10 premières secondes, le système se connecte et en affiche 10, puis recommence le décompte lorsque la période de 10 secondes est écoulée.

Notez que vous pouvez utiliser le seuillage des incidents d'intrusion seul ou en combinaison avec la prévention des attaques basée sur le débit, le mot-clé `Detection_filter` et la suppression des incidents d'intrusion.

Astuces Vous pouvez également ajouter des seuils à partir de la vue de paquets d'un incident d'intrusion.

Définir un seuil pour une règle de prévention des intrusions dans Snort 3

Vous pouvez définir un seuil unique pour une règle à partir de la page Rule Detail (détails de la règle). L'ajout d'un seuil remplace tout seuil existant pour la règle. Le seuil que vous définissez pour une règle de prévention des intrusions est appliqué à chaque flux de paquets. Cependant, la configuration n'est pleinement appliquée que dans le contexte d'un flux unique Il peut y avoir plus d'alertes sur différents flux de réseau, mais il n'y en aura pas moins que le nombre configuré.

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Dans la colonne Configuration des alertes d'une règle de prévention des intrusions, cliquez sur le lien **None** (Aucune).

Étape 4 Cliquez sur **Modifier** ( ).

Étape 5 Dans la fenêtre Alert Configuration (configuration des alertes), cliquez sur l'onglet **Threshold** (Seuil).

Étape 6 Dans la liste déroulante **Type** (Type), choisissez le type de seuil que vous souhaitez définir :

- Choisissez **Limit** pour limiter la notification au nombre spécifié d'instances d'événement par période.
- Choisissez **Threshold** (Seuil) pour fournir une notification pour chaque nombre spécifié d'instances d'événement par période.
- Choisissez**Both** (les deux) pour fournir une notification une fois par période après un nombre spécifié d'instances d'événement.

Étape 7 Choisissez **Source** ou **Destination** dans le champ **Track By** (Suivre par) pour indiquer si vous souhaitez que les instances d'événement soient suivies par adresse IP source ou de destination.

Étape 8 Saisissez le nombre d'instances d'événement que vous souhaitez utiliser comme seuil dans le champ **Nombre**.

Étape 9 Dans le champ **Secondes**, saisissez une valeur numérique spécifiant la période, en secondes, pendant laquelle les instances d'événement sont suivies.

Étape 10 Cliquez sur **Save** (enregistrer).

Reportez-vous à la vidéo Snort 3 Suppression and Threshold (Suppression et seuil Snort 3) pour obtenir de l'aide et des renseignements supplémentaires.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration.

Afficher et supprimer les seuils d'incidents d'intrusion

Pour afficher ou supprimer un paramètre de seuil existant pour une règle, utilisez la vue Rules Details (détails des règles) afin d'afficher les paramètres configurés pour un seuil et voir s'ils sont appropriés pour votre système. Si ce n'est pas le cas, vous pouvez ajouter un nouveau seuil pour remplacer les valeurs existantes.

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Choisissez la règle avec un seuil configuré, comme indiqué dans la colonne **Alert Configuration** (Configuration d'alerte) (la colonne **Alert Configuration** affiche **Seuil** comme lien pour la règle).

Étape 4 Pour supprimer le seuil de la règle, cliquez sur le lien **Threshold** (Seuil) dans la colonne **Alert Configuration** (Configuration d'alerte).

Étape 5 Cliquez sur **Modifier** ( ).

Étape 6 Cliquez sur l'onglet **Threshold** (seuil).

Étape 7 Cliquez sur **Réinitialiser**.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Configuration de la suppression des politiques de prévention des intrusions

Vous pouvez supprimer la notification d'incidents d'intrusion dans les cas où une adresse IP spécifique ou une plage d'adresses IP déclenche une règle ou un préprocesseur spécifique. C'est utile pour éliminer les faux positifs. Par exemple, si vous avez un serveur de messagerie qui transmet des paquets qui semblent être une exploitation spécifique, vous pouvez supprimer la notification d'événement pour cet événement lorsqu'il est

déclenché par votre serveur de messagerie. La règle se déclenche pour tous les paquets, mais vous ne voyez que les événements des attaques légitimes.

Types de suppression des politiques de prévention des intrusions

Notez que vous pouvez utiliser la suppression des incidents d'intrusion seule ou en combinaison avec la prévention des attaques basée sur le débit, le mot-clé `detection_filter` et le seuillage des incidents d'intrusion.

Astuces Vous pouvez ajouter des suppressions à partir de la vue de paquets d'un incident d'intrusion. Vous pouvez également accéder aux paramètres de suppression en utilisant la colonne **Alert Configuration** de la page de l'éditeur de règles de prévention des intrusions (**Objets** > **Règles de prévention des intrusions** > **Toutes les règles Snort 3**).

Définir la suppression pour une règle de prévention des intrusions dans Snort 3

Vous pouvez définir une ou plusieurs suppressions pour une règle dans votre politique de prévention des intrusions.

Avant de commencer

Assurez-vous de créer les objets réseau requis à ajouter pour la suppression de source ou de destination.

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Cliquez sur le lien **Aucun** dans la colonne Alert Configuration (Configuration des alertes) de la règle de prévention des intrusions.

Étape 4 Cliquez sur **Modifier** ( ).

Étape 5 Sous l'onglet **Suppressions** (suppressions), cliquez sur l'icône Ajouter **Ajouter** ( ) à côté de l'une des options suivantes :

- Choisissez **Source Networks** (réseaux sources) pour supprimer les événements générés par les paquets provenant d'une adresse IP source spécifiée.
- Choisissez **Destination Networks** (réseaux de destination) pour supprimer les événements générés par les paquets allant à une adresse IP de destination spécifiée.

Étape 6 Sélectionnez l'un des réseaux prédéfinis dans la liste déroulante **Network** (réseau).

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 (Facultatif) Répétez les trois dernières étapes si nécessaire.

Étape 9 Cliquez sur **Save** (Enregistrer) dans la fenêtre Alert Configuration.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Afficher et supprimer les conditions de suppression

Vous souhaiterez peut-être afficher ou supprimer une condition de suppression existante. Par exemple, vous pouvez supprimer la notification d'événement pour les paquets provenant d'une adresse IP de serveur de messagerie, car ce serveur transmet normalement des paquets qui ressemblent à des exploits. Si vous désactivez ensuite ce serveur de messagerie et réaffectez l'adresse IP à un autre hôte, vous devez supprimer les conditions de suppression pour cette adresse IP source.

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Choisissez la règle pour laquelle vous souhaitez afficher ou supprimer les suppressions.

Étape 4 Cliquez sur **Suppression** dans la colonne **Alert Configuration** (configuration des alertes).

Étape 5 Cliquez sur **Modifier** ( ).

Étape 6 Cliquez sur l'onglet **Suppressions**.

Étape 7 Supprimez la suppression en cliquant sur **Effacer** ( ) à côté de la suppression.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Ajouter des commentaires sur la règle de prévention des intrusions

Vous pouvez ajouter des commentaires aux règles de votre politique de prévention des intrusions. Les commentaires ajoutés de cette façon sont propres à la politique; c'est-à-dire que les commentaires que vous ajoutez à une règle dans une politique de prévention des intrusions ne sont pas visibles dans d'autres politiques de prévention des intrusions.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquez sur **Snort 3 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Dans la partie droite de la page, où toutes les règles sont répertoriées, choisissez la règle pour laquelle vous souhaitez ajouter un commentaire.

Étape 4 Cliquez sur **Commentaires** (💬) dans la colonne **Commentaires**.

Étape 5 Dans le champ **Comments** (Commentaires), saisissez un commentaire pour la règle.

Étape 6 Cliquez sur **Add comment** (ajouter un commentaire).

Étape 7 Cliquez sur **Save** (enregistrer).

Astuces

Le système affiche un **Commentaires** (💬) à côté de la règle dans la colonne Commentaires.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Conversion des règles personnalisées de Snort 2 vers Snort 3

Si vous utilisez des règles personnalisées, assurez-vous que vous êtes prêt à gérer cet ensemble de règles pour Snort 3 avant la conversion de Snort 2 vers Snort 3. Si vous utilisez un ensemble de règles d'un fournisseur tiers, communiquez avec ce fournisseur pour confirmer que ses règles seront converties avec succès vers Snort 3 ou pour obtenir un ensemble de règles de remplacement écrit de manière native pour Snort 3. Si vous avez des règles personnalisées que vous avez écrites vous-même, familiarisez-vous avec la rédaction des règles de Snort 3 avant la conversion, afin de pouvoir mettre à jour vos règles et optimiser la détection de Snort 3 après la conversion. Consultez les liens ci-dessous pour en savoir plus sur l'écriture de règles dans Snort 3.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Vous pouvez consulter d'autres blogs à l'adresse https: // blog.snort.org/ pour en savoir plus sur les règles Snort 3.

Important Les paramètres de politique d'analyse de réseau (NAP) de Snort 2 *ne peuvent pas* être copiés dans Snort 3 automatiquement. Les paramètres de Politique d'analyse de réseau (NAP) doivent être répliqués manuellement dans Snort 3.

Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Assurez-vous que **Toutes les règles** est sélectionné dans le volet gauche.

Étape 4 Cliquez sur la liste déroulante **Tasks** (Tâches) et sélectionnez :

- (Convertir et importer) **Convert Snort 2 rules and import** (Convertir les règles de Snort 2 et les importer) : pour convertir automatiquement toutes les règles personnalisées Snort 2 dans toutes les politiques de prévention des intrusions vers Snort 3 et les importer dans centre de gestion en tant que règles personnalisées Snort 3.
- (Convertir et télécharger) **Convert Snort 2 Rules and download** (Convertir les règles Snort 2 et les télécharger) : pour convertir automatiquement toutes les règles personnalisées de Snort 2 pour toutes les politiques de prévention des intrusions vers Snort 3 et les télécharger dans votre système local.

Étape 5 Cliquez sur **OK**.

Remarque

- Si vous avez sélectionné **Convert and import** à l'étape précédente, alors toutes les règles converties sont enregistrées dans un nouveau groupe de règles **All Snort 2 Converted Global** sous **Local Rules** (Règles locales).
- Si vous avez sélectionné **Convert and download** à l'étape précédente, enregistrez le fichier de règles localement. Vous pouvez consulter les règles converties dans le fichier téléchargé et les téléverser ultérieurement en suivant les étapes décrites dans Ajouter des règles personnalisées aux groupes de règles, à la page 56.

Reportez-vous à la vidéo Conversion des règles Snort 2 en règles Snort 3 pour obtenir de l'aide et des renseignements supplémentaires.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Dans l'onglet **Intrusion Policies** (politiques de prévention des intrusions), cliquez sur **Show Snort 3 Sync status** (Afficher l'état de la synchronisation Snort).

Étape 3 Cliquez sur l'icône **Sync Désynchronisation de Snort** ( ) de la politique de prévention des intrusions.

Remarque
Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur verte**Versions Snort synchronisées** ( ). Cela indique qu'il n'y a aucune règle personnalisée à convertir.

Étape 4 Lisez le résumé et cliquez sur l'onglet **Règles personnalisées**.

Étape 5 Choisissez :

- **Importer les règles converties dans cette politique** : pour convertir les règles personnalisées de Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans centre de gestion en tant que règles personnalisées de Snort 3.

- **Télécharger les règles converties** : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les télécharger dans votre système local. Vous pouvez consulter les règles converties dans le fichier téléchargé, puis téléverser le fichier ultérieurement en cliquant sur l'icône de chargement.

Étape 6 Cliquez sur **Re-Sync** (Resynchroniser).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Ajouter des règles personnalisées aux groupes de règles

Le téléversement de règles personnalisées dans le centre de gestion ajoute les règles personnalisées que vous avez créées localement à la liste de toutes les règles Snort 3.

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Cliquez sur la liste déroulante **Tasks** (Tâches) et sélectionnez :

Étape 4 Cliquez sur **Upload Snort 3 Rules** (Téléverser les règles de Snort 3).

Étape 5 Glissez et déposez le fichier `.txt` ou `.rules` qui contient les règles personnalisées de Snort 3 que vous avez créées.

Étape 6 Cliquez sur **OK**.

Remarque
S'il y a des erreurs dans le fichier sélectionné, vous ne pouvez pas continuer. Vous pouvez télécharger le fichier d'erreur et **remplacer le fichier** pour téléverser la version 2 du fichier, après avoir corrigé les erreurs.

Étape 7 Associez des règles à un groupe de règles pour ajouter les nouvelles règles à ce groupe.

Vous pouvez également créer un groupe de règles personnalisées (en cliquant sur le lien **Créer un nouveau groupe de règles personnalisées**), puis ajouter les règles au nouveau groupe.

Remarque
S'il n'y a aucun groupe de règles locales, continuez en cliquant sur **Créer un nouveau groupe de règles personnalisées pour continuer**. Saisissez un **nom** pour le modèle et cliquez sur **Save** (Enregistrer).

Étape 8 Effectuez l'une des opérations suivantes :

- **Merge Rules (Fusionner les règles)** pour fusionner les nouvelles règles que vous ajoutez avec les règles existantes dans le groupe de règles.
- **Replace all rules in the group with file contents (Remplacez toutes les règles du groupe par le contenu du fichier)** pour remplacer toutes les règles existantes par les nouvelles règles que vous ajoutez.

Remarque
Si vous avez choisi plusieurs groupes de règles à l'étape précédente, seule l'option **Merge Rules** (Fusionner les règles) est disponible.

Étape 9 Cliquez sur **Next** (suivant).

Consultez le résumé pour connaître les nouveaux ID de règles qui sont ajoutés et téléchargez-le éventuellement.

Étape 10 Cliquez sur **Finish** (terminer).

Important L'action de règle de toutes les règles téléversées est à l'état désactivé. Vous devez les faire passer à l'état requis pour vous assurer que les règles sont actives.

Prochaine étape

- Le téléversement de règles personnalisées dans le centre de gestion ajoute les règles personnalisées que vous avez créées à la liste de toutes les règles Snort 3. Pour appliquer ces règles personnalisées au trafic, ajoutez et activez ces règles dans les politiques de prévention des intrusions requises. Pour en savoir plus sur l'ajout de groupes de règles avec des règles personnalisées à une politique de prévention des intrusions, consultez Ajouter des groupes de règles avec des règles personnalisées à une politique de prévention des intrusions, à la page 57. Pour en savoir plus sur l'activation des règles personnalisées, consultez Gérer les règles personnalisées dans Snort 3, à la page 58.
- Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Ajouter des groupes de règles avec des règles personnalisées à une politique de prévention des intrusions

Les règles personnalisées qui sont téléversées dans le système doivent être activées dans une politique de prévention des intrusions pour appliquer ces règles au trafic. Après avoir téléversé les règles personnalisées sur centre de gestion, ajoutez le groupe de règles avec les nouvelles règles personnalisées dans la politique de prévention des intrusions.

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Dans l'onglet **Intrusion Policies** (politiques de prévention des intrusions), cliquez sur la **version Snort 3** de la politique de prévention des intrusions.

Étape 3 Cliquez sur **Ajouter** (+) à côté de la barre de recherche des groupes de règles.

Étape 4 Dans la fenêtre **Add Rule Groups** (ajouter des groupes de règles), cliquez sur l'icône **Flèche Développer** (›) à côté d'un groupe de règles pour développer le groupe de règles local.

Étape 5 Cochez la case à côté du groupe de règles personnalisées téléversé.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Gérer les règles personnalisées dans Snort 3

Les règles personnalisées qui sont téléchargées dans le système doivent être ajoutées à une politique de prévention des intrusions et activées pour appliquer ces règles au trafic. Vous pouvez activer les règles personnalisées téléchargées pour toutes les politiques ou de manière sélective pour des politiques individuelles.

Suivez les étapes ci-dessous pour activer les règles personnalisées dans une ou plusieurs politiques de prévention des intrusions :

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Développez **Règles locales**.

Étape 4 Sélectionnez le groupe de règles requis.

Étape 5 Sélectionnez les règles en cochant les cases correspondantes.

Étape 6 Sélectionnez **Per Intrusion Policy** (par politique de prévention des intrusions) dans la liste déroulante **Rule Actions** (Actions de règles).

Étape 7 Choisissez :

- **All Policies** (toutes les politiques) : pour que toutes les règles à ajouter utilisent les mêmes actions.
- **Per Intrusion Policy** (par politique de prévention des intrusions) : pour avoir des actions de règle différentes pour chaque politique de prévention des intrusions.

Étape 8 Définissez les actions de règle :

- Si vous avez sélectionné All Policies (Toutes les politiques à l'étape précédente, sélectionnez l'action de règle requise dans la liste déroulante **Select Override state** (Sélectionner l'état de remplacement).
- Si vous avez sélectionné Par politique de prévention des intrusions à l'étape précédente, sélectionnez l'**action de la règle** en fonction du nom de la politique. Pour ajouter d'autres politiques, cliquez sur **Add Another** (Ajouter une autre).

Étape 9 Ajoutez éventuellement un commentaire dans la zone de texte **Comments** (Commentaires).

Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez, Déployer les modifications de configuration, à la page 28.

Supprimer des règles personnalisées

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Développez **Local Rules** (règles locales) dans le volet gauche.

Étape 4 Cochez les cases des règles que vous souhaitez supprimer.

Étape 5 Assurez-vous que l'action de règle pour toutes les règles que vous sélectionnez est **Disable** (désactiver).

Si nécessaire, suivez les étapes ci-dessous pour désactiver l'action de règle pour plusieurs règles sélectionnées :

a) Dans la liste déroulante **Rule Actions** (actions liées aux règles), sélectionnez **Per Intrusion Policy** (par politique de prévention des intrusions).
b) Sélectionnez le bouton radio **All Policies** (toutes les politiques).
c) Sélectionnez **Disable** (désactiver) dans la liste déroulante **Select Override state** (sélectionner l'état de remplacement).
d) Cliquez sur **Save** (enregistrer).
e) Cochez les cases des règles que vous souhaitez supprimer.

Étape 6 Dans la liste déroulante **Rule Actions** (actions de règles) , sélectionnez **Delete** (supprimer).

Étape 7 Cliquez sur **Delete** (supprimer) dans la fenêtre contextuelle Delete Rules (supprimer les règles).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

Supprimer le groupe de règles

Avant de commencer

Excluez le groupe de règles que vous souhaitez supprimer de toutes les politiques de prévention des intrusions où vous l'avez inclus. Pour savoir comment exclure un groupe de règles d'une politique de prévention des intrusions, consultez Modification des politiques de prévention des intrusions Snort 3, à la page 36.

Procédure

Étape 1 Choisissez **Objets** > **Règles de prévention des intrusions**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Développez **Local Rules** (règles locales) dans le volet gauche.

Étape 4 Sélectionnez le groupe de règles à supprimer.

Étape 5 Assurez-vous que l'action de règle pour toutes les règles du groupe est **désactivée** avant de continuer.

Si l'action de règle pour l'une des règles est autre que **Désactivée**, vous ne pouvez pas supprimer le groupe de règles. Si nécessaire, suivez les étapes ci-dessous pour désactiver l'action de règle pour toutes les règles :

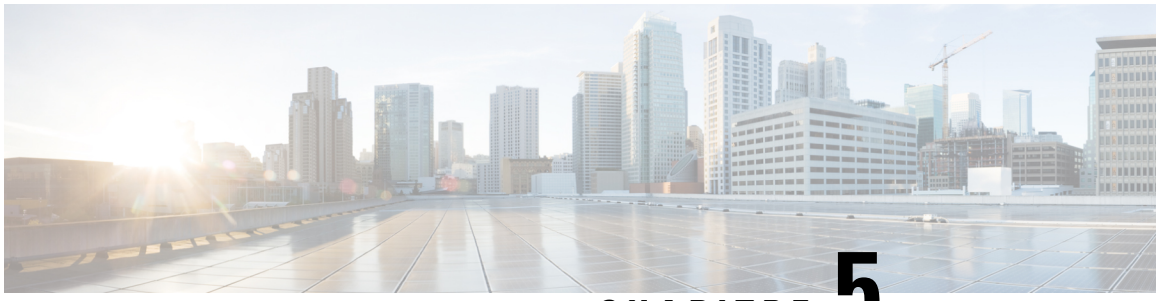
a) Cochez la case sous la liste déroulante **Rule Actions** (actions liées aux règles) pour sélectionner toutes les règles du groupe.
b) Dans la liste déroulante **Rule Actions** (actions liées aux règles), sélectionnez **Per Intrusion Policy** (par politique de prévention des intrusions).
c) Sélectionnez le bouton radio **All Policies** (toutes les politiques).
d) Sélectionnez **Disable** (désactiver) dans la liste déroulante **Select Override state** (sélectionner l'état de remplacement).
e) Cliquez sur **Save** (enregistrer).

Étape 6 Cliquez sur **Supprimer** ( ) à côté du groupe de règles.

Étape 7 Cliquez sur **OK** dans la fenêtre contextuelle Delete Rule Group (supprimer le groupe de règles).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.



CHAPITRE 5

Personnaliser la protection contre les intrusions de vos ressources réseau

Ce chapitre fournit un aperçu des règles recommandées par Cisco Secure Firewall ainsi que la génération et l'application des règles recommandées par Cisco Secure Firewall.

Modifications des règles Snort 3 dans les mises à jour des LSP

Lors des mises à jour régulières de Snort 3 pour le progiciel de sécurité léger (LSP), une règle de prévention des intrusions définie par le système existante peut être remplacée par une nouvelle règle de prévention des intrusions. Il est possible qu'une même règle soit remplacée par plusieurs règles ou que plusieurs règles soient remplacées par une seule règle. Cela se produit lorsqu'une meilleure détection est possible pour quelles règles sont combinées ou développées. Pour une meilleure gestion, certaines règles existantes définies par le système peuvent également être supprimées dans le cadre de la mise à jour du LSP.

Pour recevoir des notifications des modifications apportées à des règles définies par le système *remplacées* lors des mises à jour des LSP, assurez-vous que la case **Retain user overrides for deleted Snort 3 rules** (Conserver les remplacements de l'utilisateur pour les règles du Snort 3 supprimées) est cochée.

Pour accéder à la case à cocher **Conserver les dérogations s'appliquant aux utilisateurs pour les règles supprimées dans Snort 3**, cliquez sur **Système** (⚙), puis sélectionnez **Configuration** > **Préférences pour les politiques d'intrusion**.

Par défaut, cette case est cochée. Lorsque cette case est cochée, le système conserve les remplacements de règles cliquez sur l'icône d'engrenage dans les nouvelles règles de remplacement qui sont ajoutées dans le cadre de la mise à jour du LSP. Les notifications s'affichent sous l'onglet **Tâches**, sous l'icône Notifications située à côté de **Système** (⚙).

Présentation des règles recommandées parde Cisco Secure Firewall

Vous pouvez utiliser les règles de prévention des intrusions recommandées par Cisco pour cibler les vulnérabilités associées aux ressources hôtes détectées dans le réseau. Définir, par exemple, les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes. Cela vous permet d'adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé.

Le système formule un ensemble individuel de recommandations pour chaque politique de prévention des intrusions. Il recommande généralement des modifications d'état de règles pour les règles de texte standard et les règles d'objet partagé. Cependant, il peut également recommander des modifications pour les règles des inspecteurs et des décodeurs.

Lorsque vous générez des recommandations d'état de règles, vous pouvez utiliser les paramètres par défaut ou configurer des paramètres avancés. Les paramètres avancés vous permettent de :

- Redéfinir les hôtes de votre réseau que le système surveille pour détecter les vulnérabilités
- Influencer les règles recommandées par le système en fonction du surdébit des règles
- Préciser s'il faut générer des recommandations pour désactiver les règles

Vous pouvez également choisir d'utiliser les recommandations immédiatement ou de passer en revue les recommandations (et les règles touchées) avant de les accepter.

Choisir d'utiliser les états de règles recommandés ajoute une couche de recommandations Cisco Secure en lecture seule à votre politique de prévention des intrusions, puis choisir de ne pas utiliser les états de règles recommandés supprime la couche.

Vous pouvez planifier une tâche pour générer automatiquement des recommandations en fonction des derniers paramètres de configuration enregistrés dans votre politique de prévention des intrusions.

Les états des règles du système ne modifient pas que vous définissez manuellement, tels que :

- La définition manuelle des états de règles spécifiées *avant* de générer des recommandations empêche le système de modifier les états de ces règles à l'avenir.
- La définition manuelle des états de règles spécifiées *après* la génération de recommandations remplace les états recommandés de ces règles.

Astuces Le rapport sur les politiques de prévention des intrusions peut inclure une liste de règles avec des états de règles différents de l'état recommandé.

Lorsque vous affichez la page des règles filtrées par les recommandations, ou après avoir accédé à la page Rules (Règles) directement à partir du panneau de navigation ou de la page Policy Information (Renseignements sur les politiques), vous pouvez définir manuellement l'état des règles, trier les règles et effectuer toute autre action disponible dans la page Rules, telle que que la suppression de règles, la définition de seuils de règles, etc.

Remarque Le Cisco Talos Intelligence Group (Talos) détermine l'état approprié de chaque règle dans les politiques fournies par le système. Si vous utilisez une politique fournie par le système comme politique de base et que vous permettez au système de définir vos règles selon l'état de règle recommandé par Cisco Secure Firewall, les règles de votre politique de prévention des intrusions correspondent aux paramètres recommandés pour vos actifs réseau.

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Générer de nouvelles recommandationsde Cisco Secure Firewall dans Snort 3

Générez les recommandations de Cisco Secure Firewall pour la politique de prévention des intrusions, puis suivez les étapes répertoriées ici pour créer les nouveaux paramètres de règle recommandés dans Snort 3. Les surcharges de règles sont interprétées comme **des niveaux de sécurité** basés sur les politiques de seuil que vous avez sélectionnées dans Snort 3. L'action recommandée est basée sur le niveau de sécurité sélectionné. S'il est supérieur à la politique de base, la recommandation ne se limite pas à la génération des événements.

Avant de définir les recommandations de Cisco Secure Firewall, vous devez vous demander lequel des trois points ci-dessous correspond le mieux à l'objectif visé :

- Protection accrue : active des règles supplémentaires en fonction des vulnérabilités trouvées dans la base de données hôte et ne désactive aucune règle automatiquement. Cela entraînera probablement un ensemble de règles plus important.
- Protection ciblée : active des règles supplémentaires et désactive les règles existantes en fonction des vulnérabilités trouvées dans la base de données hôte. Cela peut augmenter ou diminuer le nombre de règles en fonction des vulnérabilités découvertes.
- Efficacité élevée : utilisez l'ensemble de règles actuellement activé et désactivez toutes les règles pour les vulnérabilités que l'on ne trouve pas dans la base de données hôte. Cela se traduira probablement par un ensemble de règles activées plus restreint.

En fonction de la réponse, les actions recommandées sont les suivantes :

- Définissez les recommandations au niveau de sécurité le plus élevé suivant et décochez les règles de désactivation.
- Définissez les recommandations au niveau de sécurité le plus élevé suivant et vérifiez les règles de désactivation.

- Définissez les recommandations au niveau de sécurité actuel et vérifiez les règles de désactivation.

Avant de commencer

Les recommandations de CiscoSecure Firewall comportent les exigences suivantes :

- Assurez-vous que des hôtes sont présents dans le système pour générer des recommandations.
- Les réseaux protégés configurés pour les recommandations doivent être mappés aux hôtes présents dans le système

Procédure

Étape 1 Choisissez **Politiques** > **Intrusion**.

Étape 2 Cliquer sur le bouton de la **version Snort 3** de la politique de prévention des intrusions.

Étape 3 Cliquez sur la couche **Recommendations (Not in Use)** pour configurer les recommandations de règles.

Dans la fenêtre Recommandations de règlesde Cisco Secure Firewall, vous pouvez définir les éléments suivants :

- **Security Level** (niveau de sécurité) : cliquez pour sélectionner le niveau de sécurité. Vous pouvez éventuellement cocher la case **Accept Recommendation to Disable Rules** (accepter la recommandation pour désactiver les règles) pour désactiver les règles qui ne sont pas activées au niveau de sécurité d'entrée et dans les réseaux protégés. N'activez cette option que si vous devez supprimer votre ensemble de règles en raison d'un nombre élevé d'alertes ou pour améliorer les performances d'inspection. Les niveaux de sécurité sont les suivants :
  - Niveau de sécurité 1 : la connectivité prédomine sur la sécurité

    Aucune incidence : aucune nouvelle règle ne sera activée et aucune règle existante ne sera désactivée. Pour augmenter les protections, sélectionner un niveau de sécurité plus élevé.

    Sécurité inférieure (la case est cochée) : toutes les règles sont désactivées, à l'exception des règles de l'ensemble de règles Connectivité avant sécurité qui correspondent à des vulnérabilités potentielles sur les hôtes détectés. Il est plutôt recommandé d'ajuster la politique de base.
  - Niveau de sécurité 2 : équilibre entre sécurité et connectivité

    Aucune incidence : aucune nouvelle règle ne sera activée et aucune règle existante ne sera désactivée. Pour augmenter les protections, sélectionner un niveau de sécurité plus élevé.

    Efficacité accrue (la case est cochée) : conserve les règles existantes qui correspondent aux vulnérabilités potentielles sur les hôtes découverts et désactive les règles pour les vulnérabilités introuvables sur le réseau.
  - Niveau de sécurité 3 : la sécurité prime sur la connectivité

    Sécurité accrue : active des règles supplémentaires qui correspondent aux vulnérabilités potentielles des hôtes découverts, sur la base de l'ensemble de règles de détection maximale.

    Sécurité ciblée (la case est cochée) : active des règles supplémentaires qui correspondent aux vulnérabilités des hôtes découverts sur la base du jeu de règles La sécurité prime sur la connectivité, tout en désactivant les règles existantes qui ne correspondent pas aux vulnérabilités potentielles des hôtes découverts.
  - Niveau de sécurité 4 : détection maximale

    Sécurité accrue : active des règles supplémentaires qui correspondent aux vulnérabilités potentielles des hôtes découverts, sur la base du jeu de règles La sécurité prime sur la connectivité.

Sécurité ciblée (la case est cochée) : active des règles supplémentaires qui correspondent aux vulnérabilités des hôtes découverts sur la base du jeu de règles détection maximale, tout en désactivant les règles existantes qui ne correspondent pas aux vulnérabilités potentielles des hôtes découverts.

Remarque
La détection maximale active un très grand nombre de règles et peut avoir une incidence sur la performance. Nous vous recommandons de vérifier ce paramètre et de le tester avant de le déployer dans un environnement de production.

- **Protected Networks** (réseaux protégés) : spécifie les réseaux surveillés ou les hôtes individuels à examiner pour les recommandations. Vous pouvez sélectionner un ou plusieurs objets système ou réseau définis de façon personnalisée dans la liste déroulante. Par défaut, tous les réseaux IPv4 ou IPv6 sont sélectionnés, si aucune sélection n'est effectuée.

  Important
  Les recommandations de règles de Cisco Secure Firewall dépendent de la découverte de réseau. Les réseaux protégés s'appliquent à tous les hôtes découverts dans les plages configurées dans votre politique de découverte de réseaux. Pour la version Snort 2, consultez le chapitre Politiques de découverte du réseau dans le *Guide de configuration du périphérique de Cisco Secure Firewall Management Center*.

  Cliquez sur le bouton **Add +** (ajouter) pour créer un nouvel objet réseau de type Hôte ou Réseau et cliquez sur **Enregistrer**.

Étape 4 Générer et appliquer les recommandations :

- **Générer** : génère les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous Règles recommandées (non utilisées).
- **Générer et appliquer** : génère et applique les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous Règles recommandées (en cours d'utilisation).

Les recommandations ont été générées avec succès. Un nouvel onglet de recommandation apparaît avec toutes les règles recommandées avec leurs actions recommandées correspondantes. Des filtres d'action de règle prédéfinis sont également disponibles pour cet onglet, en plus de nouvelles recommandations.

Étape 5 Vous pouvez vérifier les recommandations, puis choisir de les appliquer en conséquence :

- **Accepter** : applique les recommandations générées précédemment pour une politique de prévention des intrusions.
- **Actualiser** : régénère et met à jour les recommandations de règles pour une politique de prévention des intrusions.
- **Modifier** : ouvre la boîte de dialogue Recommendations, qui vous permet de fournir les valeurs d'entrée de recommandation, puis de générer les recommandations.
- **Supprimer tout** : rétablit ou supprime les règles recommandées appliquées de la politique et supprime également l'onglet de recommandation.

Sous **Toutes les règles**, il y a une section Recommended Rules (règles recommandées) qui affiche les règles recommandées.

Remarque
L'action finale pour une règle de prévention des intrusions est appliquée en fonction de l'ordre de priorité des actions liées aux règles.

Remplacement de règle > Recommandations générées > Remplacement de groupe > Action par défaut de la politique de base

Pour les recommandations activées, centre de gestion considère l'état actuel : remplacements de groupes, politique de base et configurations de recommandation, et l'ordre de priorité des actions est :

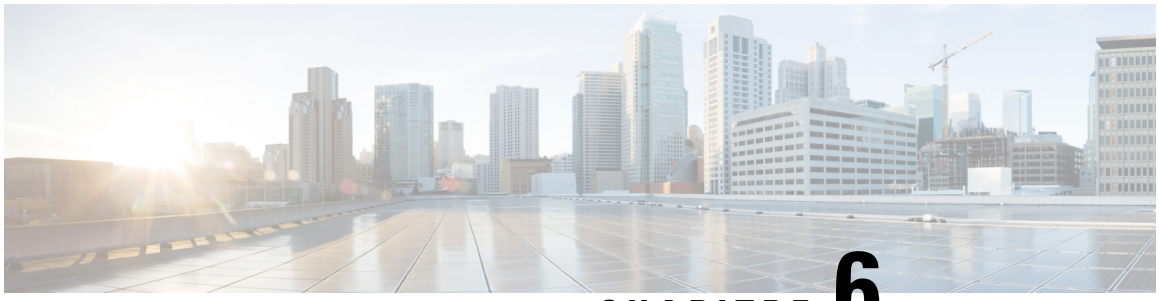
réussite > blocage > refus > abandon > réécriture > alerte

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 28.

PARTIE II

Analyse avancée de réseau dans Snort 3



CHAPITRE 6

Premiers pas avec – Politiques d'analyse de réseau

Ce chapitre présente les principes de base des politiques d'analyse de réseau, les conditions préalables et la manière de gérer les politiques d'analyse de réseau. Il fournit également des informations sur la création de politiques d'analyse de réseau personnalisées et les paramètres de politique d'analyse de réseau.

Aperçu des politiques d'analyse de réseau

Les *politiques d'analyse de réseau* régissent de nombreuses options de prétraitement du trafic et sont appelées par les paramètres avancés de votre politique de contrôle d'accès. Le prétraitement lié à l'analyse de réseau a lieu après la mise en correspondance Security Intelligence et le déchiffrement SSL, mais avant le début de l'intrusion ou de l'inspection des fichiers.

Par défaut, le système utilise la politique d'analyse de réseau *Sécurité et connectivité équilibrées* pour prétraiter tout le trafic géré par une politique de contrôle d'accès. Cependant, vous pouvez choisir une autre politique d'analyse de réseau par défaut pour effectuer ce prétraitement. Pour votre commodité, le système offre un choix entre plusieurs politiques d'analyse de réseau non modifiables, qui sont réglées par Cisco Talos Intelligence Group (Talos). Vous pouvez également créer une politique d'analyse de réseau personnalisée avec des paramètres de prétraitement personnalisés.

Astuces Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions. Les politiques d'analyse de réseau et de prévention des intrusions travaillent ensemble pour examiner votre trafic.

Vous pouvez également adapter les options de prétraitement du trafic à des zones de sécurité, à des réseaux et à des VLAN spécifiques en créant plusieurs politiques d'analyse de réseau personnalisées, puis en les affectant au prétraitement du trafic. (Notez que ASA FirePOWER ne peut pas restreindre le prétraitement par VLAN.)

Gérer les politiques d'analyse du réseau

Sous votre nom d'utilisateur dans la barre d'outils, le système affiche une arborescence des domaines disponibles. Pour changer de domaine, choisissez le domaine auquel vous souhaitez accéder.

Procédure

Étape 1 Choisissez un des chemins d'accès suivants pour accéder à la politique d'analyse de réseau.

- **Politiques** > **En-tête Contrôle d'accès** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux**
- **Politiques** > **En-tête Contrôle d'accès** > **Intrusion**, puis cliquez sur **Politiques d'analyse des réseaux**
- **Politiques** > **Intrusions** > **Politiques d'analyse de réseau**

Remarque
Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Gérer vos politiques d'analyse du réseau

- Create (créer) : Si vous souhaitez créer une nouvelle politique d'analyse de réseau, cliquez sur **Create Policy** (Créer une politique).

  Deux versions de la politique d'analyse de réseau sont créées, une **version Snort 2 et une versionSnort 3**.

  - Pour la version Snort 2, consultez *Création de politique d'analyse de réseau personnalisée pour Snort 2* dans le *Guide de configuration de Cisco Secure Firewall Management Center*.
  - Pour la version Snort 3, consultez Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 73.

- Delete (supprimer) : Si vous souhaitez supprimer une politique d'analyse de réseau, cliquez sur l'icône **Delete** (supprimer), puis confirmez que vous souhaitez supprimer la politique. Vous ne pouvez pas supprimer une politique d'analyse de réseau si une politique de contrôle d'accès y fait référence.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

- Edit (modifier) : Si vous souhaitez modifier une politique d'analyse de réseau existante, cliquez sur l'icône **Edit** (modifier).

  Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Report (rapport) : Cliquez sur l'icône **Report** (rapport); Consultez la section *Génération des rapports sur les politiques actuelles* dans le *Guide de configuration de Cisco Secure Firewall Management Center*.

Définitions et terminologies pour la politique d'analyse de réseau Snort 3

Le tableau suivant dresse la liste des concepts et termes de Snort 3 utilisés dans la politique d'analyse de réseau.

Tableau 6 : Définitions et terminologies pour la politique d'analyse de réseau Snort 3

Terme	Description
Inspecteurs	Les inspecteurs sont des modules d'extension qui traitent les paquets (semblables au préprocesseur Snort 2).
Inspecteur de classeur	L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et prendre en compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur de classeur, ce n'est qu'alors que les valeurs/configurations de cet inspecteur prennent effet. Pour en savoir plus, consultez la section *Inspecteur de classeur* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 73.
Inspecteurs Singleton	Les inspecteurs Singleton contiennent une instance. Ces inspecteurs ne prennent pas en charge l'ajout d'instances, comme les inspecteurs Multiton. Les paramètres de l'inspecteur Singleton sont appliqués à l'ensemble du trafic correspondant à cet inspecteur et non à un segment de trafic spécifique. Pour en savoir plus, consultez la section *Inspecteurs Singleton* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 73.

Terme	Description
Inspecteurs Multiton	Les inspecteurs Multiton contiennent plusieurs instances que vous pouvez configurer selon vos besoins. Ces inspecteurs prennent en charge la configuration de paramètres en fonction de conditions spécifiques, telles que le réseau, le port et le VLAN. Un ensemble de paramètres pris en charge s'appelle une instance. Pour en savoir plus, consultez *Inspecteurs Multiton* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 73.
Schéma	Le fichier de schéma est basé sur la spécification OpenAPI JSON et valide le contenu que vous chargez ou téléchargez. Vous pouvez télécharger le fichier de schéma et l'ouvrir à l'aide de n'importe quel éditeur JSON tiers, tel que l'éditeur Swagger. Le fichier de schéma vous aide à identifier les paramètres pouvant être configurés pour les inspecteurs ainsi que les valeurs autorisées, la plage et les modèles acceptés correspondants. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 80.
Exemple de fichier	Il s'agit d'un modèle préexistant qui contient des exemples de configuration pour vous aider à configurer les inspecteurs. Vous pouvez consulter les exemples de configuration inclus dans le fichier exemple et apporter les modifications nécessaires. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 80.
Configuration complète	Vous pouvez télécharger la configuration complète de l'inspecteur dans un seul fichier. Tous les renseignements concernant la configuration de l'inspecteur sont disponibles dans ce fichier. La configuration complète est une configuration fusionnée de la configuration par défaut (déployée dans le cadre des mises à jour des LSP par Cisco Talos) et des configurations de l'inspecteur Politique d'analyse de réseau (NAP) personnalisé. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 80.

Terme	Description
Configuration remplacée	Dans la **version Snort 3** de la page de politiques d'analyse de réseau : • Sous **Actions** > **Upload** (Actions > Téléverser), vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour téléverser le fichier JSON qui contient la configuration remplacée. • Sous **Actions** > **Télécharger**, vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour télécharger la configuration de l'inspecteur qui a été remplacée. Si vous n'avez remplacé aucune configuration d'inspecteur, cette option est désactivée. Lorsque vous remplacez la configuration de l'inspecteur, cette option est activée automatiquement pour vous permettre d'effectuer le téléchargement. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 80.

Sujets connexes

Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 73
Personnaliser la politique d'analyse de réseau, à la page 80
Mappage de la stratégie d'analyse du réseau, à la page 77

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Threat Defense.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Création d'une politique d'analyse de réseau personnalisée pour Snort 3

La politique d'analyse de réseau par défaut est réglée pour les exigences de réseau typiques et des performances optimales. Généralement, la politique d'analyse de réseau par défaut répond à la plupart des exigences du réseau et vous n'aurez peut-être pas besoin de la personnaliser. Toutefois, lorsque vous avez des besoins particuliers en matière de réseau ou lorsque vous faites face à des problèmes de rendement, la politique d'analyse de réseau par défaut peut être personnalisée. Notez que la personnalisation de la politique d'analyse

de réseau est une configuration avancée qui ne doit être effectuée que par des utilisateurs avancés ou par le service d'assistance Cisco.

La configuration de la politique d'analyse de réseau pour Snort 3 est un modèle basé sur les données, qui repose sur JSON et le schéma JSON. Le schéma est basé sur la spécification OpenAPI et vous aide à obtenir un aperçu des inspecteurs, des paramètres, des types de paramètres et des valeurs valides pris en charge. Les inspecteurs Snort 3 sont des modules d'extension qui traitent les paquets (comme le préprocesseur Snort 2). La configuration de la politique d'analyse de réseau est disponible pour téléchargement au format JSON.

Dans Snort 3, la liste des inspecteurs et des paramètres ne correspond pas exactement à la liste des préprocesseurs et des paramètres de Snort 2. De plus, le nombre d'inspecteurs et de paramètres disponibles dans centre de gestion est un sous-ensemble des inspecteurs et des paramètres pris en charge par Snort 3. Consultez https://snort.org/snort3 pour de plus amples renseignements sur Snort 3. Consultez https://www.cisco.com/go/snort3-inspectors pour en savoir plus sur les inspecteurs disponibles dans centre de gestion.

Remarque

- Lors de la mise à niveau de centre de gestion à la version 7.0, les modifications effectuées dans la version Snort 2 de la politique d'analyse de réseau ne sont pas migrées vers Snort 3 après la mise à niveau.
- Contrairement à la politique de prévention des intrusions, il n'y a pas d'option pour synchroniser les paramètres de politique d'analyse de réseau Snort 2 avec Snort 3.

Mises à jour de l'inspecteur par défaut

Les mises à jour du progiciel de sécurité allégé (LSP) peuvent contenir de nouveaux inspecteurs ou des modifications de plages d'entiers pour les configurations d'inspecteurs existantes. À la suite de l'installation d'un LSP, de nouveaux inspecteurs ou des plages mises à jour seront disponibles sous la section **Inspecteurs** dans la **version Snort 3** de votre politique d'analyse de réseau.

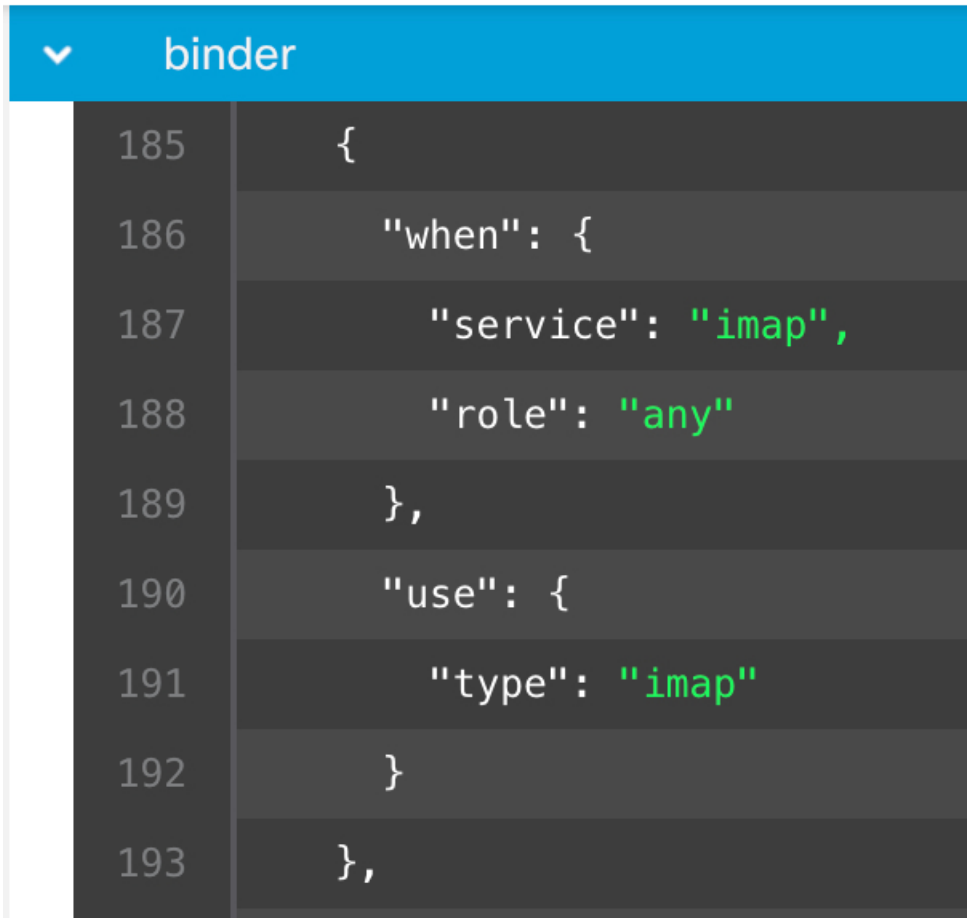
Inspecteur Binder

L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et prendre en compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur Binder, alors seulement les valeurs ou configurations de cet inspecteur entrent en vigueur. Par exemple :

Pour l'inspecteur *imap*, le binder définit la condition suivante lorsqu'il doit être accédé. C'est lorsque :

- Le service est égal à imap.
- Le rôle est égal à Tout.

Si ces conditions sont remplies, utilisez le type imap.



Inspecteurs Singleton

Les inspecteurs Singleton ne contiennent qu'une seule instance. Ces inspecteurs ne prennent pas en charge l'ajout d'instances, comme les inspecteurs Multiton. Les paramètres de l'inspecteur Singleton sont appliqués à l'ensemble du trafic et non à un segment de trafic en particulier.

Par exemple :

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

Inspecteurs Multiton

Les inspecteurs Multiton contiennent plusieurs instances que vous pouvez configurer selon vos besoins. Ces inspecteurs prennent en charge la configuration de paramètres en fonction de conditions spécifiques, telles

que le réseau, le port et le VLAN. Un ensemble de paramètres pris en charge s'appelle une instance. Il existe une instance par défaut, et vous pouvez également ajouter des instances supplémentaires en fonction de conditions spécifiques. Si le trafic correspond à cette condition, les paramètres de cette instance sont appliqués. Sinon, les paramètres de l'instance par défaut sont appliqués. En outre, le nom de l'instance par défaut est le même que le nom de l'inspecteur.

Pour un inspecteur Multiton, lorsque vous téléversez la configuration de l'inspecteur remplacée, vous devez également inclure ou définir une condition binder correspondante (conditions dans lesquelles l'accès à l'inspecteur ou l'utilisation de celui-ci doit être effectué) pour chaque instance du fichier JSON, sinon le téléversement produira une erreur. Vous pouvez également créer de nouvelles instances, mais veillez à inclure une condition binder pour chaque nouvelle instance que vous créez pour éviter les erreurs.

Par exemple :

- L'inspecteur Multiton, où l'instance par défaut est modifiée.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- L'inspecteur Multiton où l'instance par défaut et le binder par défaut sont modifiés.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
```

```
    }
}
```

- Un inspecteur Multiton où une instance personnalisée et un binder personnalisés sont ajoutés.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

Mappage de la stratégie d'analyse du réseau

Pour les politiques d'analyse de réseau, Cisco Talos fournit des informations de mappage, qui sont utilisées pour trouver la version Snort 2 correspondante des politiques pour la version Snort 3.

Ce mappage garantit que les politiques de la version Snort 3 contiennent les politiques équivalentes de la version Snort 2.

Afficher le mappage de la politique d'analyse des réseaux

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Mappage NAP**.

Étape 3 Développez la flèche **Afficher les mappages**.

Les politiques d'analyse de réseau Snort 3 qui sont automatiquement mappées à une politique équivalente Snort 2 s'affichent.

Étape 4 Cliquez sur **OK**.

Créer une politique d'analyse de réseau

Toutes les politiques d'analyse de réseau existantes sont disponibles dans centre de gestion avec leurs versions Snort 2 et Snort 3 correspondantes. Lorsque vous créez une nouvelle politique d'analyse de réseau, elle est créée avec la version 2 et la version Snort 3.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Créer une politique**.

Étape 3 Remplissez les champs **Nom** et **Description**.

Étape 4 Choisir le **mode d'inspection** parmi les choix disponibles.

- **Détection**
- **Prévention**

Étape 5 Sélectionnez une **politique de base** et cliquez sur **Save** (Enregistrer).

Remarque
Configurez la politique d'analyse de réseau (NAP) en mode **prévention** si vous utilisez Snort 3 et le déchiffrement SSL ou l'identité du serveur TLS.

La nouvelle politique d'analyse de réseau est créée avec ses **versions Snort 2** et **Snort 3**correspondantes.

Modifier la politique d'analyse de réseau

Vous pouvez modifier la politique d'analyse de réseau pour changer son nom, sa description ou sa politique de base.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Edit** (Modifier) pour changer le nom, la description, le mode d'inspection ou la politique de base.

Remarque
Si vous modifiez le nom, la description, la politique de base et le mode d'inspection de la politique d'analyse de réseau, les modifications sont appliquées aux versions Snort 2 et Snort 3. Si vous souhaitez modifier le mode d'inspection pour une version spécifique, vous pouvez le faire à partir de la page de politique d'analyse de réseau pour cette version respective.

Étape 3 Cliquez sur **Save** (enregistrer).

Recherchez un inspecteur dans la page des politiques d'analyse de réseau.

Dans la version Snort 3 de la page de politique d'analyse de réseau, vous devrez peut-être rechercher un inspecteur en saisissant tout texte pertinent dans la barre de recherche.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Saisissez le nom d'un inspecteur ou tout autre texte pertinent à rechercher dans la barre de **recherche**.

Tous les inspecteurs correspondant au texte que vous recherchez s'affichent.

Par exemple, si vous saisissez `pop`, l'inspecteur pop et l'inspecteur de classeurs s'affichent comme des résultats correspondants à l'écran.

Sujets connexes

Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 88
Afficher la liste des inspecteurs avec remplacements, à la page 85
Définitions et terminologies pour la politique d'analyse de réseau Snort 3 , à la page 71
Personnaliser la politique d'analyse de réseau, à la page 80
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 83

Copier la configuration de l'inspecteur

Vous pouvez copier la configuration de l'inspecteur pour la version Snort 3 de la politique d'analyse de réseau en fonction de vos besoins.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis dont vous souhaitez copier la configuration.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Cliquez sur l'icône **Copier dans le presse-papier** pour copier la configuration de l'inspecteur dans le presse-papier de l'un des éléments suivants ou des deux.

- **Configuration par défaut** dans la colonne de gauche
- **Configuration remplacée** dans la colonne de droite

Étape 5 Collez la configuration de l'inspecteur copiée dans un éditeur JSON pour apporter les modifications nécessaires.

Sujets connexes

Personnaliser la politique d'analyse de réseau, à la page 80

Personnaliser la politique d'analyse de réseau

Vous pouvez personnaliser la version Snort 3 de la politique d'analyse de réseau en fonction de vos besoins.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

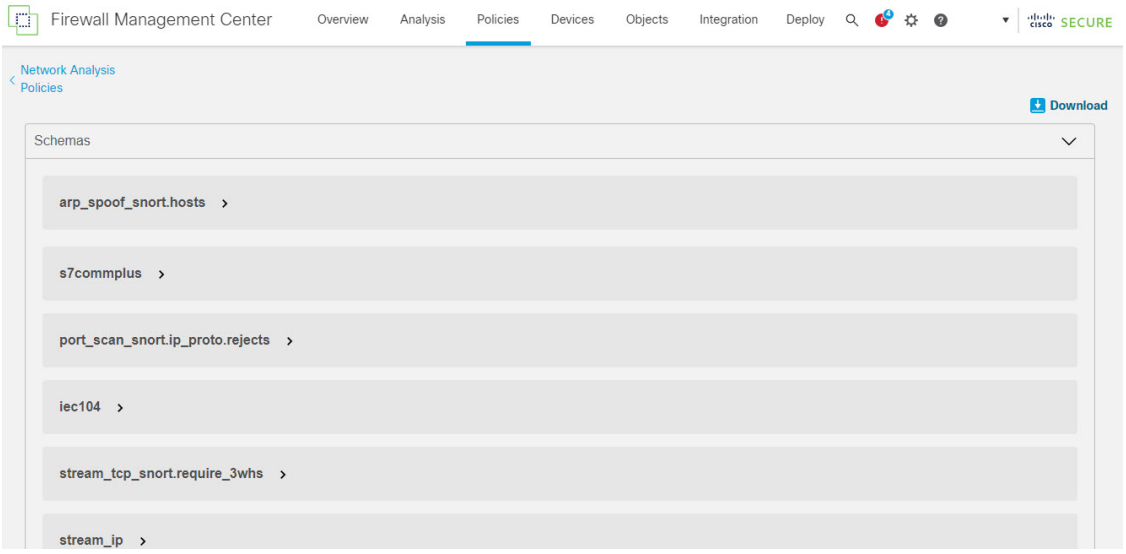
Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Cliquez sur le menu déroulant **Actions** .

Les options suivantes s'affichent.

- Afficher le schéma
- Télécharger un schéma, télécharger un exemple de fichier ou de modèle
- Télécharger la configuration complète
- Télécharger la configuration remplacée
- Téléverser la configuration remplacée

Étape 4 Cliquez sur **Afficher le schéma** pour ouvrir le fichier de schéma directement dans un navigateur.



Étape 5 Vous pouvez télécharger le fichier de schéma, un exemple de fichier/modèle, la configuration complète ou la configuration remplacée au besoin.

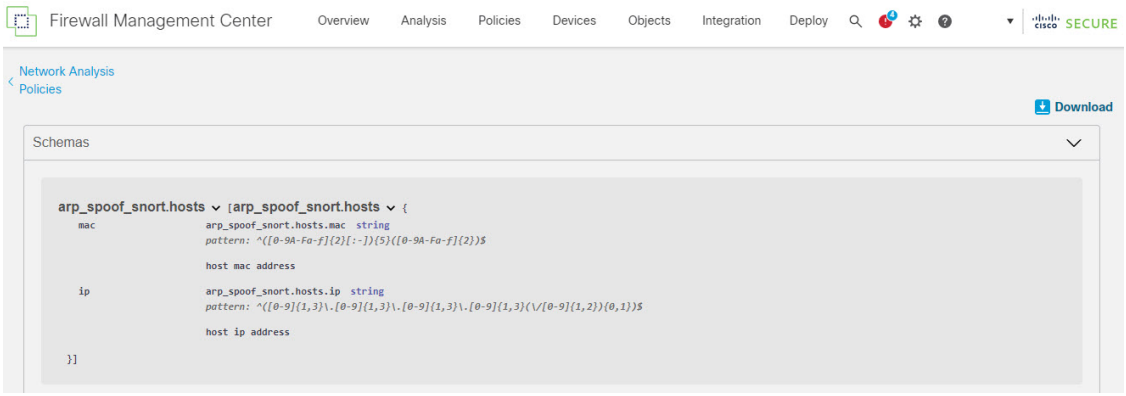
Ces options vous donnent un aperçu des valeurs autorisées, de la plage et des modèles, des configurations de l'inspecteur existantes et par défaut et des configurations de l'inspecteur remplacées.

a) Cliquez sur **Télécharger le schéma** pour télécharger le fichier de schéma.

Le fichier de schéma valide le contenu que vous chargez ou téléchargez. Vous pouvez télécharger le fichier de schéma et l'ouvrir à l'aide de n'importe quel éditeur JSON tiers. Le fichier de schéma vous aide à identifier les paramètres pouvant être configurés pour les inspecteurs ainsi que les valeurs autorisées, la plage et les modèles acceptés correspondants.

Par exemple, pour l'inspecteur *arp_spoof_snort*, vous pouvez configurer les hôtes. Les hôtes comprennent les valeurs d'adresses *mac* et *ip*. Le fichier de schéma présente le modèle accepté suivant pour ces valeurs.

- **mac** – `pattern: ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **IP** – `modèle : ^([0-9] {1,3}.[0-9] {1,3}.[0-9] {1,3}.[0-9] {1,3}( /[0-9] {1,2}) {0,1})$`



Vous devez fournir les valeurs, la plage et les modèles conformément à ceux acceptés dans le fichier de schéma pour pouvoir remplacer la configuration de l'inspecteur avec succès, sinon, vous obtenez un message d'erreur.

b) Cliquez sur **télécharger un exemple de fichier / modèle** pour utiliser un modèle préexistant qui contient des exemples de configuration pour vous aider à configurer les inspecteurs.

Vous pouvez consulter les exemples de configuration inclus dans le fichier exemple et apporter les modifications nécessaires.

c) Cliquez sur **Télécharger la configuration complète** pour télécharger les configurations complètes de l'inspecteur dans un seul fichier JSON.

Au lieu de développer les inspecteurs séparément, vous pouvez télécharger la configuration complète pour rechercher les informations dont vous avez besoin. Tous les renseignements concernant la configuration de l'inspecteur sont disponibles dans ce fichier.

d) Cliquez sur **Chargement de la configuration remplacée** pour télécharger la configuration de l'inspecteur qui a été remplacée.

Étape 6 Pour remplacer la configuration existante, suivez les étapes.

Vous pouvez choisir de remplacer une configuration de l'inspecteur des manières suivantes.

- Apportez des modifications en ligne pour un inspecteur directement dans centre de gestion. Consultez la section **Modifier en ligne un inspecteur pour remplacer la configuration** dans le chapitre **Premiers pas avec les politiques d'analyse de réseau** du *Guide de configuration Snort 3 de Cisco Secure Firewall Management Center*.

- Continuez à suivre la procédure actuelle qui consiste à utiliser le menu déroulant**Actions**pour téléverser le fichier de configuration remplacé.

Si vous avez choisi d'effectuer les modifications en ligne directement dans centre de gestion, vous n'avez pas besoin de suivre plus avant la procédure actuelle. Sinon, vous devez suivre cette procédure entièrement.

a) Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez remplacer la configuration par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Vous devrez peut-être rechercher un inspecteur en saisissant tout texte pertinent dans dans la barre de recherche.

b) Cliquez sur l'icône **Copier dans le presse-papier** pour copier la configuration de l'inspecteur par défaut dans le presse-papier.

c) Créez un fichier JSON et collez-y la configuration par défaut.

d) Conservez la configuration de l'inspecteur que vous souhaitez remplacer et supprimez toutes les autres configurations et instances du fichier JSON.

Vous pouvez également utiliser le **fichier ou le modèle exemple** pour comprendre comment remplacer la configuration par défaut. Il s'agit d'un exemple de fichier qui comprend des extraits de code JSON expliquant comment personnaliser la politique d'analyse de réseau pour Snort 3.

e) Apporter des modifications à la configuration de l'inspecteur au besoin.

Validez les modifications et assurez-vous qu'elles sont conformes au fichier de schéma. Pour les inspecteurs multiton, assurez-vous que les conditions de classeur pour toutes les instances sont incluses dans le fichier JSON. Pour obtenir de plus amples renseignements, consultez *Inspecteurs Multiton* dans la rubrique **Création de politique d'analyse de réseau personnalisée pour Snort 3** dans le *Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center*.

f) Si vous copiez d'autres configurations de l'inspecteur par défaut, ajoutez cette configuration de l'inspecteur au fichier existant qui contient la configuration remplacée.

Remarque
La configuration de l'inspecteur copiée doit être conforme aux normes JSON.

g) Enregistrez le fichier de configuration remplacé sur votre système.

Étape 7 dans le menu déroulant **Actions**, choisissez Upload Overridden Configuration pour téléverser le fichier JSON qui contient la configuration remplacée.

Mise en garde
Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants et, par conséquent, toute modification ultérieure à la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Vous pouvez faire glisser et déposer un fichier ou cliquer pour naviguer jusqu'au fichier JSON enregistré dans votre système qui contient la configuration de l'inspecteur remplacée.

- **Fusionner les remplacements de l'inspecteur** : Le contenu du fichier téléversé est fusionné avec la configuration existante en l'absence d'inspecteur commun. S'il y a présence d'inspecteurs communs, le contenu du fichier téléversé (pour les inspecteurs communs) prévaut sur le contenu précédent et remplace la configuration pour ces inspecteurs.
- **Remplacer les remplacements de l'inspecteur** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier téléversé.

Attention

Choisir cette option supprime tous les remplacements précédents. Faites un choix avisé avant de remplacer la configuration à l'aide de cette option.

Si une erreur se produit lors du chargement des inspecteurs remplacés, elle est visible dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé). Vous pouvez également télécharger le fichier avec l'erreur, corriger l'erreur et téléverser de nouveau le fichier.

Étape 8 Dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé), cliquez sur **Importer** pour téléverser la configuration de l'inspecteur remplacée.

Après avoir téléversé la configuration de l'inspecteur remplacée, vous verrez une icône jaune à côté de l'inspecteur qui signifie qu'il s'agit d'un inspecteur remplacé.

En outre, la colonne **Overridden Configuration** (Configuration remplacée) sous l'inspecteur affiche la valeur remplacée.

Vous pouvez également afficher tous les inspecteurs remplacés en cochant la case **Afficher les remplacements uniquement** à côté de la barre de recherche.

Remarque
Assurez-vous de toujours télécharger la configuration remplacée, d'ouvrir le fichier JSON et d'ajouter les nouvelles modifications ou remplacements aux configurations de l'inspecteur à ce fichier. Cette action est nécessaire pour ne pas perdre les anciennes configurations remplacées.

Étape 9 (Facultatif) Effectuez une sauvegarde du fichier de configuration remplacé sur votre système avant d'apporter de nouvelles modifications à la configuration de l'inspecteur.

Astuces
Nous vous recommandons d'utiliser la sauvegarde de temps à autre lorsque vous remplacez la configuration de l'inspecteur.

Sujets connexes

Rétablir la configuration par défaut de la configuration remplacée, à la page 85
Afficher la liste des inspecteurs avec remplacements, à la page 85
Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 79
Copier la configuration de l'inspecteur , à la page 79

Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration

Pour la version Snort 3 de la politique d'analyse de réseau, vous pouvez apporter une modification en ligne à la configuration de l'inspecteur afin de remplacer la configuration selon vos besoins.

Vous pouvez également utiliser le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez Personnaliser la politique d'analyse de réseau, à la page 80 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez remplacer le paramètre par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Edit Inspector** (Modifier l'inspecteur) (en forme de crayon) pour apporter des modifications à la configuration de l'inspecteur.

La fenêtre contextuelle Override Configuration (remplacer la configuration) s'affiche dans laquelle vous pouvez apporter les modifications nécessaires.

Remarque

- Conserver seulement les paramètres à remplacer. Si vous conservez la même valeur dans un paramètre, ce champ devient rémanent. Cela signifie que, si Talos modifie ultérieurement ce paramètre, la valeur actuelle est conservée.
- Si vous ajoutez ou supprimez toute instance personnalisée, assurez-vous d'ajouter ou supprimer une règle de classeur pour cette instance dans le classeur inspecteur.

Étape 5 Cliquez sur **OK**.

S'il y a des erreurs selon les normes JSON, un message d'erreur s'affiche.

Étape 6 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Si les modifications sont conformes à la spécification de schéma OpenAPI, centre de gestion vous permet d'enregistrer la configuration, sinon, la fenêtre contextuelle **d'erreur lors de l'enregistrement de la configuration remplacée** apparaît pour afficher les erreurs. Vous pouvez également télécharger le fichier avec les erreurs.

Sujets connexes

Personnaliser la politique d'analyse de réseau, à la page 80
Annuler les modifications non enregistrées lors des modifications en ligne , à la page 84
Rétablir la configuration par défaut de la configuration remplacée, à la page 85
Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 88

Annuler les modifications non enregistrées lors des modifications en ligne

Lorsque vous apportez des modifications en ligne pour remplacer la configuration pour un inspecteur, , vous pouvez annuler des modifications non enregistrées. Notez que cette action rétablit toutes les modifications non enregistrées aux dernières valeurs enregistrées, mais ne rétablit pas la configuration à la configuration par défaut pour un inspecteur.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez annuler les modifications non enregistrées.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône en forme de **croix** ✕ pour annuler les modifications non enregistrées pour l'inspecteur.

Vous pouvez également cliquer sur **Cancel** (Annuler) pour annuler l'opération.

Si aucune modification non enregistrée a été apportée à la configuration de l'inspecteur, cette option n'est pas visible.

Sujets connexes

Rétablir la configuration par défaut de la configuration remplacée, à la page 85
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 83

Afficher la liste des inspecteurs avec remplacements

Vous pouvez afficher une liste de tous les inspecteurs remplacés.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Cochez la case **Show Overrides Only** (afficher les remplacements uniquement) à côté de la barre de recherche pour afficher la liste des inspecteurs remplacés.

Tous les inspecteurs remplacés sont affichés avec une icône orange à côté de leur nom pour vous aider à les identifier.

Sujets connexes

Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 79
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 83
Personnaliser la politique d'analyse de réseau, à la page 80

Rétablir la configuration par défaut de la configuration remplacée

Vous pouvez annuler les modifications que vous avez apportées pour remplacer la configuration par défaut d'un inspecteur. Cette action rétablit la configuration remplacée à la configuration par défaut pour un inspecteur.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez rétablir la configuration remplacée.

Les inspecteurs remplacés sont signalés par une icône jaune à côté de leur nom.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur. Sous **Overridden Configuration** (configuration remplacée) dans la colonne de

droite, cliquez sur l'icône **Revenir à la configuration par défaut** (flèche de retour) pour rétablir la configuration remplacée pour l'inspecteur à la configuration par défaut.

Si vous n'avez apporté aucune modification à la configuration par défaut de l'inspecteur, cette option est désactivée.

Étape 4 Cliquez sur **Revert** (Rétablir) pour confirmer la décision.

Étape 5 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Si vous ne souhaitez pas enregistrer les modifications, vous pouvez cliquer sur **Annuler** ou sur l'icône **X**.

Sujets connexes

Annuler les modifications non enregistrées lors des modifications en ligne , à la page 84
Personnaliser la politique d'analyse de réseau, à la page 80
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 83
Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 88

Valider les politiques Snort 3

Pour valider les politiques Snort 3, voici une liste d'informations de base que l'utilisateur peut prendre en note :

- La version actuelle de centre de gestion peut gérer plusieurs versions de Threat Defense.
- La version actuelle de centre de gestion prend en charge les configurations Politique d'analyse de réseau (NAP) qui ne sont pas applicables aux versions précédentes de Threat Defense.
- La politique Politique d'analyse de réseau (NAP) et les validations actuelles fonctionneront selon la version actuelle prise en charge.
- Les modifications peuvent inclure du contenu qui n'est pas valide pour les versions précédentes des Threat Defense.
- Les modifications de configuration de la politique sont acceptées s'il s'agit d'une configuration valide pour la version actuelle et si elle est effectuée à l'aide du binaire Snort 3 et du schéma Politique d'analyse de réseau (NAP) actuels.
- Pour les versions précédentes de Threat Defense, la validation est effectuée lors du déploiement à l'aide du schéma Politique d'analyse de réseau (NAP) et du binaire Snort 3 pour cette version spécifique. S'il y a une configuration qui n'est pas applicable à la version donnée, l'utilisateur est informé ou averti que nous ne déploierons pas la configuration qui n'est pas prise en charge sur la version donnée et que la configuration restante sera déployée.

Dans cette procédure, lorsque nous associons la politique Politique d'analyse de réseau (NAP) à une politique de contrôle d'accès et la déployons sur un périphérique, par exemple, une configuration de filtre de débit comme celle d'un inspecteur est appliquée pour valider les politiques Snort 3.

Procédure

Étape 1 **Étapes pour remplacer la configuration de la politique Politique d'analyse de réseau (NAP) :** sous **Inspecteurs** dans la **version Snort 3** de la politique d'analyse de réseau, développez l'inspecteur requis pour lequel vous souhaitez remplacer le paramètre par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 2 Sous la section **Overridden Configuration (configuration remplacée)** dans la colonne de droite, cliquez sur l'icône **Edit Inspecteur** (Modifier l'inspecteur, en forme de crayon) pour apporter des modifications à un inspecteur comme rate_filter.

La fenêtre contextuelle Override Configuration (Remplacer la configuration) s'affiche dans laquelle vous pouvez apporter les modifications nécessaires à l'inspecteur rate_filter.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Vous pouvez également utiliser le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé.

Étape 5 Cliquez sur le menu déroulant **Actions** dans la section **Version 3 de Snort** de la politique d'analyse de réseau.

Étape 6 Sous **Téléverser**, vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour téléverser le fichier JSON qui contient la configuration remplacée.

Mise en garde
Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants et, par conséquent, toute modification ultérieure de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Vous pouvez faire glisser et déposer un fichier ou cliquer pour naviguer jusqu'au fichier JSON enregistré dans votre système qui contient la configuration de l'inspecteur remplacée.

- **Fusionner les remplacements de l'inspecteur** : Le contenu du fichier téléversé est fusionné avec la configuration existante en l'absence d'inspecteur commun. S'il y a présence d'inspecteurs communs, le contenu du fichier téléversé (pour les inspecteurs communs) prévaut sur le contenu précédent et remplace la configuration pour ces inspecteurs.
- **Remplacer les remplacements de l'inspecteur** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier téléversé.

  Attention
  Comme le choix de cette option supprime tous les remplacements précédents, prenez une décision éclairée avant de remplacer la configuration à l'aide de cette option.

Si une erreur se produit lors du chargement des inspecteurs remplacés, elle est visible dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé). Vous pouvez également télécharger le fichier avec l'erreur, puis corriger l'erreur et télécharger à nouveau le fichier.

Étape 7 **Étapes pour associer la Politique d'analyse de réseau (NAP) à la politique de contrôle d'accès :** dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé), puis sur **Edit** (modifier) à côté de la section Network Analysis and Intrusion Policies (Politiques d'analyse des réseaux et de prévention des intrusions).

Étape 8 Dans la liste déroulante **Default Network Analysis Policy** (politique d'analyse de réseau par défaut), sélectionnez une politique d'analyse de réseau par défaut.

Si vous choisissez une politique créée par l'utilisateur, vous pouvez cliquer sur **Edit** (modifier) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Étape 11 Sinon, dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé), puis sur **Edit** (modifier) à côté de la section Network Analysis and Intrusion Policies (Politiques d'analyse des réseaux et de prévention des intrusions).

Étape 12 Cliquez sur **Add Rule** (ajouter une règle).

Étape 13 Configurez les conditions de la règle en cliquant sur les conditions que vous souhaitez ajouter.

Étape 14 Cliquez sur **Network Analysis** (analyse de réseau) et choisissez la **politique d'analyse de réseau** que vous souhaitez utiliser pour prétraiter le trafic correspondant à cette règle.

Étape 15 Cliquez sur **Add** (ajouter).

Étape 16 **Déploiement :** Dans la barre de menu centre de gestion, cliquez sur **Déployer**, puis sélectionnez **Déploiement**.

Étape 17 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Développer : cliquez sur **Expand Arrow** (développer la flèche) pour afficher les modifications de configuration propres au périphérique à déployer.

  En sélectionnant la case à cocher du périphérique, toutes les modifications à apporter au périphérique, qui sont répertoriées sous le périphérique, sont poussées pour le déploiement. Cependant, vous pouvez utiliser **sélection de politique** pour sélectionner des politiques ou des configurations à déployer tout en conservant les modifications restantes sans les déployer.

  Facultativement, utilisez **Afficher ou masquer la politique** pour afficher ou masquer sélectivement les politiques non modifiées connexes.

Étape 18 Cliquez sur **Deploy** (déployer).

Étape 19 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Remarque
Il affiche un avertissement indiquant que la politique d'analyse réseau de Snort 3 contient des inspecteurs ou des attributs qui ne sont pas valides pour cette version Threat Defense, et que les paramètres non valides seront ignorés lors du déploiement : les inspecteurs non valides sont : ["rate_filter"] uniquement pour les périphériques inférieurs à la version 7.1.

Exemples de configuration de politique d'analyse de réseau personnalisée

Il s'agit d'un exemple de fichier qui comprend des extraits de code JSON expliquant comment personnaliser la politique d'analyse de réseau pour Snort 3. Vous pouvez choisir de remplacer une configuration de l'inspecteur des manières suivantes :

- Apportez des modifications en ligne pour un inspecteur directement dans centre de gestion. Consultez Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 83.
- Utilisez le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez Personnaliser la politique d'analyse de réseau, à la page 80.

Avant de choisir l'une de ces options, consultez tous les détails et exemples suivants qui vous aideront à définir les remplacements de politique d'analyse de réseau avec succès. Vous devez lire et comprendre les exemples des différents scénarios expliqués ici afin d'éviter tout risque et toute erreur.

Si vous choisissez de remplacer une configuration de l'inspecteur dans le menu déroulant **Actions**, vous devez créer un fichier JSON pour les remplacements de politique d'analyse de réseau, puis téléverser le fichier.

Pour remplacer une configuration d'inspecteur dans la politique d'analyse de réseau, vous devez téléverser uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants par nature et, par conséquent, toute modification ultérieure des valeurs ou de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Voici des exemples pour différents scénarios :

Activation d'un inspecteur Singleton lorsque l'état par défaut dans la politique de base est désactivé

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

Désactivation d'un inspecteur Singleton lorsque l'état par défaut dans la politique de base est activé

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

Activation d'un inspecteur Multiton lorsque l'état par défaut dans la politique de base est désactivé

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

Désactivation d'un inspecteur Multiton lorsque l'état par défaut dans la politique de base est activé

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

Remplacement de la valeur par défaut de paramètres spécifiques pour l'inspecteur Singleton

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

Remplacement des paramètres spécifiques d'une instance par défaut (lorsque le nom de l'instance correspond au type d'inspecteur) dans l'inspecteur Multiton

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

Ajout d'une règle de classeur pour une instance par défaut avec les modifications requises

Remarque Les règles du classeur par défaut ne peuvent pas être modifiées, elles sont toujours ajoutées à la fin.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

Ajout d'une nouvelle instance personnalisée

Remarque L'entrée de règle de classeur correspondante doit être définie dans l'inspecteur de classeur.

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

Remplacement d'une instance Singleton, d'une instance par défaut de Multiton et de la création d'une nouvelle instance Multiton dans un remplacement JSON unique

Exemple pour afficher les éléments suivants dans un seul remplacement JSON :

- Remplacement d'une instance Singleton (inspecteur **`du normalisateur`**)
- Remplacement d'une instance par défaut de Multiton (inspecteur **`http_inspect`**)
- Création d'une nouvelle instance Multiton (inspecteur **`Telnet`**)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
```

```
      "instances": [
        {
          "data": {
            "unzip": false,
            "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
          },
          "name": "http_inspect"
        }
      ]
    },
    "telnet": {
      "enabled": true,
      "type": "multiton",
      "instances": [
        {
          "name": "telnet_my_instance",
          "data": {
            "encrypted_traffic": true
          }
        }
      ]
    },
    "binder": {
      "enabled": true,
      "type": "binder",
      "rules": [
        {
          "when": {
            "role": "any",
            "service": "telnet"
          },
          "use": {
            "type": "telnet",
            "name": "telnet_my_instance"
          }
        },
        {
          "use": {
            "type": "http_inspect"
          },
          "when": {
            "role": "server",
            "service": "http",
            "dst_nets": "10.1.1.0/24"
          }
        }
      ]
    }
}
```

Remarque Vous n'avez pas besoin de fournir l'attribut de **nom** pour l'instance par défaut dans les règles de classeur.

Configuration de arp_spoof

Exemple de configuration de **arp_spoof** :

L'inspecteur **arp_spoof** n'a aucune configuration par défaut pour aucun attribut. Cela montre un cas où vous pouvez fournir les remplacements.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

Configuration de rate_filter

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

Configuration des règles de classeur lors de l'utilisation de la politique d'analyse de réseau à plusieurs hiérarchies

Cet exemple illustre l'ajout d'une nouvelle instance personnalisée dans la politique enfant et la façon dont les règles de classeur doivent être écrites. Les règles du classeur sont définies sous forme de liste et, par conséquent, il est important de reprendre les règles définies dans la politique parente et de construire les nouvelles règles par-dessus, car les règles ne seront pas fusionnées automatiquement. Les règles de classeur disponibles dans la politique enfant sont une source de réalité en entier.

Dans Threat Defense, les règles de politique par défaut de Cisco Talos sont ajoutées pour ces remplacements définis par l'utilisateur.

Politique parente :

Nous avons défini une instance personnalisée sous le nom **`telnet_parent_instance`** et la règle de classeur correspondante.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
```

```
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Politique enfant :

Cette politique d'analyse de réseau a la politique susmentionnée comme politique de base. Nous avons défini une instance personnalisée sous le nom **`telnet_child_instance`** et avons également défini les règles de classeur pour cette instance. Les règles de classeur de la politique parente doivent être copiées ici, puis les règles de classeur de la politique enfant peuvent être ajoutées au début ou par-dessus en fonction de la nature de la règle.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
```

```
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Configuration de l'attribut de l'inspecteur de listes en général

Lors de la modification des remplacements pour un attribut de type liste, il est important de transmettre le contenu complet plutôt que le remplacement partiel. Cela signifie que si les attributs de politique de base sont définis comme :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Si vous souhaitez modifier **`value1`** en **`value1-new`**, la charge utile de remplacement doit ressembler à ce qui suit :

Méthode correcte :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Méthode incorrecte :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
```

```
  ]
}
```

Vous pouvez comprendre cette configuration en prenant les valeurs diminuées de l'attribut **alt_max_command_line_len** dans l'inspecteur **smtp**. Supposons que la configuration de politique par défaut (de base) pour l'inspecteur **smtp** soit la suivante :

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "ignore_data": false,
          "max_command_line_len": 512,
          "max_header_line_len": 1000,
          "log_rcptto": false,
          "decompress_swf": false,
          "max_response_line_len": 512,
          "b64_decode_depth": -1,
          "max_auth_command_line_len": 1000,
          "log_email_hdrs": false,
          "xlink2state": "alert",
          "binary_data_cmds": "BDAT XEXCH50",
          "auth_cmds": "AUTH XAUTH X-EXPS",
          "log_filename": false,
          "uu_decode_depth": -1,
          "ignore_tls_data": false,
          "data_cmds": "DATA",
          "bitenc_decode_depth": -1,
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            }
          ],
          "log_mailfrom": false,
          "decompress_pdf": false,
          "normalize": "none",
          "email_hdrs_log_depth": 1464,
          "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
```

```
            ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
            XSTA XTRN XUSR",
           "qp_decode_depth": -1
         }
       }
    ],
    "enabled": true
  }
}
```

Maintenant, si vous souhaitez ajouter deux autres objets à la liste **alt_max_command_line_len** :

```
{
    "length": 246,
    "command": "XEXCH50"
},
{
    "length": 246,
    "command": "X-EXPS"
}
```

Le JSON de la politique d'analyse personnalisée du réseau ressemblerait alors à ce qui suit :

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

Configuration des remplacements lorsque la politique d'analyse de réseau multi-hiérarchisation est utilisée dans l'inspecteur Multiton

Cet exemple illustre le remplacement des attributs dans la politique enfant et la façon dont la configuration fusionnée sera utilisée dans la politique enfant pour toute instance. Tous les remplacements définis dans la politique enfant seront fusionnés avec la politique parent. Par conséquent, si attribut1 et attribut2 sont remplacés dans la politique parente et que les attribut2 et attribut3 sont remplacés dans la politique enfant, les configurations fusionnées sont pour la politique enfant. Cela signifie que l'attribut1 (défini dans la politique parente), l'attribut2 (défini dans la politique enfant) et l'attribut3 (défini dans la politique enfant) seront configurés sur le périphérique.

Politique parente :

Ici, nous avons défini une instance personnalisée sous le nom **`telnet_parent_instance`** et remplacé deux attributs, à savoir **`normalize`** et **`encrypted_traffic`** dans l'instance personnalisée.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Politique enfant :

Cette politique d'analyse de réseau a la politique susmentionnée comme politique de base. Nous avons remplacé l'attribut **`encrypted_traffic`** de la politique parente et remplacé le nouvel attribut **`ayt_attack_thresh`**.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
```

```
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

Avec le JSON de politique ci-dessus, lorsque vous déployez la politique d'analyse de réseau, le JSON fusionné suivant sera configuré sur le périphérique.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Cet exemple illustre les détails de la politique d'analyse de réseau personnalisée. Le même comportement se produit dans l'instance par défaut. En outre, une fusion similaire serait effectuée pour les inspecteurs Singleton.

Suppression de tous les remplacements de l'inspecteur pour la politique d'analyse de réseau :

Chaque fois que vous souhaitez supprimer tous les remplacements pour une politique d'analyse de réseau spécifique, vous pouvez téléverser un fichier JSON vide. Lors du chargement des remplacements, choisissez l'option **Remplacer les remplacements de l'inspecteur**.

```
{
}
```

Sujets connexes

Définitions et terminologies pour la politique d'analyse de réseau Snort 3 , à la page 71
Mappage de la stratégie d'analyse du réseau, à la page 77
Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 73
Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 79
Copier la configuration de l'inspecteur , à la page 79

Personnaliser la politique d'analyse de réseau, à la page 80
Afficher la liste des inspecteurs avec remplacements, à la page 85

Paramètres de politique d'analyse de réseau et modifications en cache

Lorsque vous créez une politique d'analyse de réseau, elle utilise les mêmes paramètres que sa politique de base.

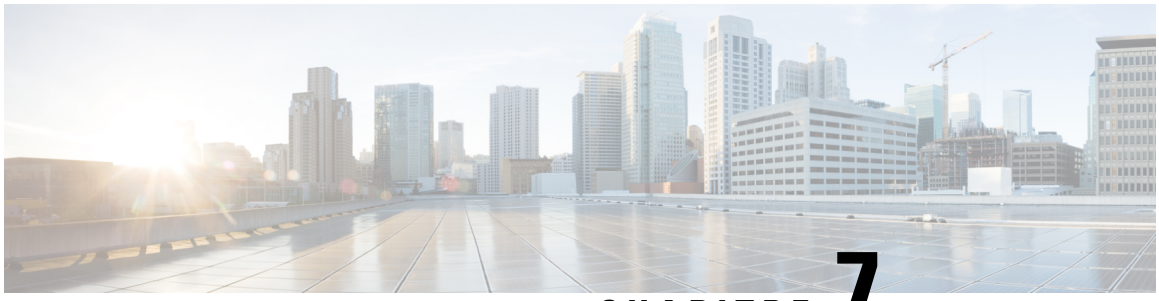
Lorsque vous adaptez une politique d'analyse de réseau, en particulier lorsque vous désactivez les inspecteurs, gardez à l'esprit que certains inspecteurs et certaines règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Si vous désactivez un inspecteur obligatoire, le système l'utilise automatiquement avec ses paramètres actuels, bien que l'inspecteur reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Remarque Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet **doivent** se compléter mutuellement. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**.

Le système met en cache une politique d'analyse de réseau par utilisateur. Lors de la modification d'une politique d'analyse de réseau, si vous sélectionnez un menu ou un autre chemin vers une autre page, vos modifications restent dans le cache système même si vous quittez la page.

PARTIE III

Moteur de visibilité chiffré pour Snort 3



CHAPITRE 7

Moteur de visibilité chiffré

Le moteur de visibilité chiffrée (EVE) est utilisé pour identifier les applications et les processus clients à l'aide du chiffrement TLS. Il active la visibilité et permet aux administrateurs de prendre des mesures et d'appliquer des politiques au sein de leurs environnements. La technologie EVE peut également être utilisée pour identifier et arrêter les programmes malveillants.

Présentation du moteur de visibilité chiffrée

Le moteur de visibilité chiffrée (EVE, Encrypted Visibility Engine) est utilisé pour offrir plus de visibilité sur les sessions chiffrées sans qu'il soit nécessaire de les déchiffrer. Ces informations sur les sessions chiffrées sont obtenues par la bibliothèque de logiciels libres de Cisco, qui est présente dans la base de données de vulnérabilités (VDB) de Cisco. La bibliothèque prend et analyse les empreintes des sessions chiffrées entrantes et les compare à un ensemble d'empreintes connues. Cette base de données d'empreintes digitales connues est également disponible dans la base de données de Cisco VDB.

Remarque La fonctionnalité de moteur de visibilité chiffrée n'est prise en charge que sur les périphériques gérés par centre de gestion exécutant Snort 3. Cette fonctionnalité n'est pas prise en charge sur les périphériques Snort 2 ni les périphériques gérés par gestionnaire d'appareil.

Certaines des caractéristiques importantes d'EVE sont les suivantes :

- Vous pouvez appliquer des actions de politique de contrôle d'accès sur le trafic en utilisant les informations dérivées d'EVE.
- La VDB incluse dans Cisco Secure Firewall a la capacité d'affecter des applications à certains processus détectés par EVE avec une valeur de confiance élevée. Vous pouvez également créer des détecteurs d'application personnalisés pour :
  - Mettre en correspondance des processus détectés par EVE pour les nouvelles applications définies par l'utilisateur.

- Remplacer la valeur intégrée de niveau de confiance de processus qui est utilisée pour affecter des applications aux processus détectés par EVE.

  Reportez-vous aux sections **Configuration des détecteurs d'application personnalisés** et **Spécification des affectations de processus EVE** dans le chapitre sur la **détection d'applications** du Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

- EVE peut détecter le type et la version du système d'exploitation du client qui a créé un paquet Client Hello dans le trafic chiffré.
- EVE prend également en charge l'empreinte et l'analyse du trafic QUIC (Quick UDP Internet Connections). Le nom du serveur du paquet Client Hello s'affiche dans le champ URL de la page des **événements de connexion**.

Attention Pour utiliser la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) sur centre de gestion, vous devez avoir une licence Menace valide sur votre périphérique. En l'absence de licence Menace , la politique affiche un avertissement et le déploiement n'est pas autorisé.

Remarque

- La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le type et la version des sessions SSL du système d'exploitation. L'utilisation normale du système d'exploitation, comme l'exécution d'applications et d'un logiciel de gestion des paquets, peut déclencher la détection du système d'exploitation. Pour afficher la détection du système d'exploitation client, en plus d'activer le bouton à bascule EVE, vous devez activer **Hôtes** sous **Politiques** > **Détection du réseau**. Pour afficher une liste des systèmes d'exploitation possibles sur l'adresse IP de l'hôte, cliquez sur **Analyse** > **Hôtes** > **Carte du réseau**, puis choisissez l'hôte requis.
- EVE ne fournit pas de visibilité ni d'observations sur le trafic encapsulé.

Liens connexes

Configurer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée), à la page 105

Comment fonctionne EVE

Le moteur de visibilité chiffrée (EVE) inspecte la partie Client Hello de l'établissement de liaison TLS pour identifier les processus clients. Le Client Hello est le paquet de données initial qui est envoyé au serveur. Cela donne une bonne indication du processus client sur l'hôte. Cette empreinte, combinée à d'autres données telles que l'adresse IP de destination, fournit la base pour l'identification de l'application d'EVE. En identifiant des empreintes d'applications précises lors de l'établissement de session TLS, le système peut identifier le processus client et prendre les mesures appropriées (autoriser/bloquer).

La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut identifier plus de 5 000 processus clients. Le système mappe un certain nombre de ces processus aux applications clientes afin de les utiliser comme critères dans les règles de contrôle d'accès. Cela donne au système la capacité d'identifier et de contrôler ces applications sans activer le déchiffrement TLS. En utilisant les empreintes de processus malveillants connus, la technologie EVE peut également être utilisée pour identifier et bloquer le trafic malveillant chiffré sans déchiffrement sortant.

Grâce à la technologie d'apprentissage automatique, Cisco traite plus d'un milliards d'empreintes TLS et plus de 10 000 échantillons de programmes malveillants par jour pour créer et mettre à jour des empreintes EVE. Ces mises à jour sont ensuite fournies aux clients au moyen de l'offre groupée de la base de données de vulnérabilités (VDB) Cisco.

Si EVE ne reconnaît pas une empreinte, il identifie l'application client et estime le score de dangerosité d'une menace du premier flux à l'aide des détails de destination, tels que l'adresse IP, le port et le nom du serveur. À ce stade, l'état des empreintes est aléatoire et peut être affiché dans les journaux de débogage. Pour les flux ultérieurs avec la même empreinte, EVE ignore la réanalyse et marque l'état de l'empreinte comme non étiquetée. Si vous envisagez de bloquer le trafic en fonction des seuils de score faible ou très faible EVE, le flux initial est bloqué. Cependant, les flux ultérieurs seront autorisés une fois l'empreinte de l'application mise en cache.

Configurer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée)

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Modifier** ( ) à côté de la politique de contrôle d'accès que vous souhaitez modifier.

Étape 3 Choisissez **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 4 Cliquez sur **Modifier** ( ) à côté de **Moteur de visibilité chiffrée**.

Étape 5 Sur la page **Moteur de visibilité chiffrée**, activez le bouton à bascule **Moteur de visibilité chiffrée**.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployer les modifications de configuration

Afficher les événements EVE

Après avoir activé l'**Encrypted Visibility Engine** (moteur de visibilité chiffrée) et déployé votre politique de contrôle d'accès, vous pouvez commencer à envoyer du trafic en direct par votre système. Vous pouvez afficher les événements de connexion enregistrés sur la page **Événements de connexion** ou **Événements unifiés**.

Procédez comme suit pour accéder aux événements de connexion, dans le centre de gestion.

Procédure

Étape 1 Cliquez sur **Analyse** > **En-tête des connexions** > **Événements**.

Étape 2 Cliquez sur l'onglet **Table View of Connection Events** (Vue de tableau des événements de connexion).

Vous pouvez également afficher les champs d'événement de connexion sur la page **Événements unifiés**. Cliquez sur **Analyse** > **Événements unifiés** pour accéder à la page **Événements unifiés**.

Le moteur de chiffrée peut identifier le processus client qui a lancé une connexion, le système d'exploitation du client et si le processus contient ou non des programmes malveillants.

Sur la page **Événements de connexion**, vous devez explicitement activer les colonnes suivantes, qui sont ajoutées pour la prise d', Moteur de visibilité chiffrée.

- Nom du processus de visibilité chiffrée
- Note de confiance du processus de visibilité chiffrée
- Niveau de confiance des menaces pour la visibilité chiffrée
- Note de confiance des menaces pour la visibilité chiffrée
- Type de détection

Pour plus de renseignements sur ces champs, consultez *Connexion et renseignements de sécurité Event Fields* dans le Guide d'administration Cisco Secure Firewall Management Center.

Remarque Sur la page **Événements de connexion**, si les processus sont affectés à des applications, la colonne **Type de détection** affiche **Moteur de visibilité chiffrée**, indiquant que l'application client a été identifiée par EVE. Sans affectations d'applications aux noms de processus, la colonne **Detection Type** affiche **AppID** indiquant que le moteur qui a identifié l'application client était AppID.

Afficher le tableau de bord EVE

Vous pouvez afficher les informations de l'analyse EVE dans les tableaux de bord suivants.

Avant de commencer

- Dans une politique de contrôle d'accès, le **moteur de visibilité chiffrée (EVE)** doit être activé dans les **paramètres avancés**.

Procédure

Étape 1 Accédez à **Présentation** > **Tableaux de bord**, puis cliquez sur **Tableau de bord**.

Étape 2 Dans la fenêtre **Summary Dashboard** (tableau de bord résumé), cliquez sur le lien **Switch Dashboard** (Changer de tableau de bord) et choisissez **Application Statistics** (Statistiques de l'application) dans la liste déroulante.

Étape 3 Choisissez l'onglet **Digital Visibility Engine** (moteur de visibilité chiffrée par empreintes) pour afficher les deux tableaux de bord suivants :

- **Principaux processus découverts par le moteur de visibilité chiffrée** : affiche les principaux processus clients utilisés sur votre réseau et le nombre de connexions. Vous pouvez cliquer sur le nom du processus dans le tableau pour voir la vue filtrée de la page des **événements de connexion**, qui est filtrée par nom de processus.
- **Connexions par moteur de visibilité chiffrée de confiance dans la menace** : affiche les connexions en fonction des niveaux de confiance (très élevé, très faible, etc.). Vous pouvez cliquer sur le niveau de confiance des menaces dans le tableau pour afficher la vue filtrée de la page des **événements de connexion**, qui est filtrée par niveau de confiance.

Configurer les règles d'exception de la fonctionnalité EVE

Vous pouvez créer une règle d'exception pour un moteur de visibilité chiffrée (EVE) afin d'assurer la continuité des connexions et des services de confiance en contournant l'action de blocage d'EVE. Vous pouvez ajouter des attributs tels que des noms de processus et une adresse IP de destination à une règle d'exception. Par exemple, vous pouvez contourner le verdict de blocage d'EVE pour les réseaux de confiance. Toutes les connexions dans les réseaux contournés sont exemptées du verdict de blocage d'EVE en fonction du niveau de confiance à l'égard des menaces.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Modifier** ( ) à côté de la politique de contrôle d'accès que vous souhaitez modifier.

Étape 3 Choisissez **Paramètres avancés** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Étape 4 À côté de **Moteur de visibilité chiffrée (EVE)**, cliquez sur **Modifier** ( ).

Étape 5 Sur la page **Moteur de visibilité chiffrée**, cliquez sur le bouton à bascule **Moteur de visibilité chiffrée** pour activer EVE.

Étape 6 Activez le bouton à bascule **Bloquer le trafic en fonction du score de l'EVE** pour bloquer le trafic en fonction du score de confiance à l'égard des menaces de l'EVE.

Étape 7 Cliquez sur **Ajouter une règle d'exception** et ajoutez un ou plusieurs des attributs suivants.

a) Sous l'onglet **Nom du processus**, saisissez un nom de processus identifié par EVE et cliquez sur **Ajouter au processus** sur le côté droit de la fenêtre.

Vous pouvez ajouter plusieurs noms de processus à la même règle d'exception. La liste d'exceptions EVE basée sur les noms de processus ne fonctionne qu'avec les noms de processus identifiés par EVE, qui sont sensibles à la casse et aux espaces.

b) Sous l'onglet **Objets de réseau**, effectuez l'une des opérations suivantes :

- Choisissez une ou plusieurs adresses IP dans la liste et ajoutez à la liste des **réseaux sélectionnés**.

- Sous **Réseaux sélectionnés**, saisissez manuellement l'adresse IP et cliquez sur l'icône **+** pour l'ajouter à la liste des réseaux sélectionnés.

c) (Facultatif) Dans le champ **Commentaire** disponible sur tous les onglets, vous pouvez saisir le motif de l'ajout des attributs requis à la règle d'exception EVE.

Étape 8 Cliquez sur **Enregistrer** pour enregistrer la règle d'exception EVE.

Étape 9 Enregistrez et déployez la stratégie de contrôle d'accès sur les périphériques.

Remarque Lorsqu'une connexion correspond à une règle d'exception, elle contourne le verdict de blocage de la veille. Vous pouvez afficher l'action EVE sur la page **Événements de connexion** ou **Événements unifiés**. L'en-tête de la colonne **Raison** indique **Exempté EVE** pour l'identification du trafic contourné EVE.

Ajouter une règle d'exception à partir d'événements unifiés

Vous pouvez utiliser la page **Événements unifiés** pour ajouter des règles d'exception pour les connexions bloquées par EVE.

Avant de commencer

La liste des exceptions n'est prise en charge qu'à partir de la version 7.6.0 de Threat Defense.

Procédure

Étape 1 Cliquez sur **Analyse** > **Événements unifiés**.

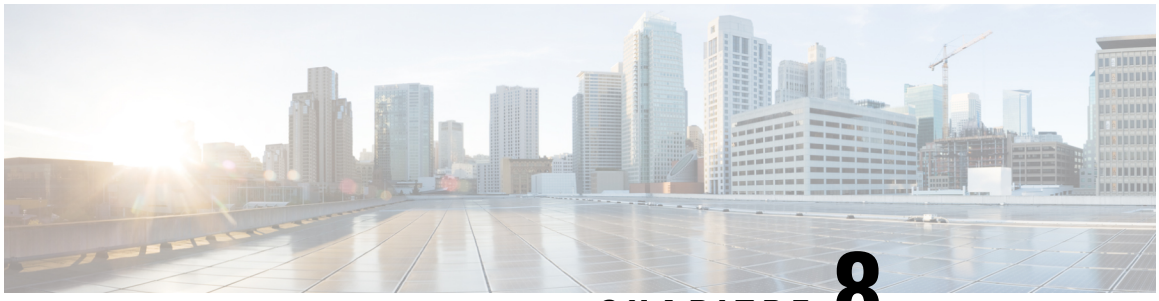
Étape 2 Dans la colonne **Motif** indiquant **Blocage par visibilité chiffrée**, cliquez sur l'icône **Points de suspension(** ⋮ **)** dans la cellule.

Étape 3 Choisissez **Ajouter une règle d'exception EVE** dans la liste déroulante.

Étape 4 Dans la fenêtre **Moteur de visibilité chiffrée** qui s'affiche, la règle est automatiquement ajoutée au bas de la liste d'exceptions. Vous pouvez examiner et modifier la règle ajoutée avant d'enregistrer et de déployer la configuration.

PARTIE IV

Détection des flux d'éléphants pour Snort 3



CHAPITRE 8

Détection de flux d'éléphants

Les flux d'éléphants sont des flux extrêmement volumineux (en octets totaux) et continus configurés par un flux TCP (ou d'autres protocoles) mesurés sur une liaison réseau. Par défaut, les flux d'éléphants sont ceux dont la taille est supérieure à 1 Go/10 secondes. Ils peuvent nuire aux performances des cœurs Snort. Les flux d'éléphants ne sont pas nombreux, mais ils peuvent occuper une part disproportionnée de la bande passante totale sur une période de temps. Ils peuvent entraîner des problèmes comme une utilisation élevée du processeur, des pertes de paquets, etc.

À partir de la version centre de gestion 7.2.0 (périphériques Snort 3 uniquement), vous pouvez utiliser la fonctionnalité de flux d'éléphants pour détecter et corriger les flux d'éléphants, ce qui aide à réduire la pression du système et à résoudre les problèmes mentionnés.

À propos de la détection de flux d'éléphants et de la correction

Vous pouvez utiliser la fonctionnalité de détection de flux d'éléphants pour détecter et corriger des flux d'éléphants. Les actions correctives suivantes peuvent être appliquées :

- **Bypass elephant flow** (Contourner le flux d'éléphants) : vous pouvez configurer le flux d'éléphants pour contourner l'inspection Snort. Si cette option est configurée, Snort ne reçoit aucun paquet de ce flux.
- **Throttle elephant flow** (Limitation du flux d'éléphants) : vous pouvez appliquer une limite de débit au flux et continuer à inspecter les flux. Le débit est calculé dynamiquement et 10 % du débit est réduit. Snort envoie le verdict (flux de qualité de service avec 10 % de débit en moins) au moteur du pare-feu. Si vous choisissez de contourner toutes les applications, y compris les applications non identifiées, vous ne pouvez pas configurer l'action de limitation (rate-limit) pour aucun flux.

Remarque Pour que la détection de flux d'éléphants fonctionne, Snort 3 doit être le moteur de détection.

Mise à niveau de flux d'éléphants à partir du contournement intelligent des applications

Intelligent Application Bypass (IAB) est obsolète à partir de la version 7.2.0 pour les dispositifs Snort 3.

Pour les périphériques exécutant la version 7.2.0 ou une version ultérieure, vous devez configurer les paramètres de flux d'éléphants dans la section des **paramètres de flux** d'éléphants dans la politique de CA (onglet Paramètres avancés).

Après la mise à niveau vers la version 7.2.0 (ou ultérieure), si vous utilisez un périphérique Snort 3, les paramètres de configuration du flux d'éléphants seront choisis et déployés à partir de la section des **paramètres de flux d'éléphants** et non à partir de la section des **paramètres de contournement de l'application intelligente**. n'ont pas migré vers les paramètres de configuration d'Elephant Flow, votre appareil perdra la configuration de flux d'éléphants lors du prochain déploiement.

Le tableau suivant présente les configurations de l'IAB ou de flux d'éléphants qui peuvent être appliquées à la version 7.2.0 ou ultérieure et à la version 7.1.0 ou antérieure qui exécutent des moteurs Snort 3 ou 2.

Centre de gestion	Threat Defense	Flux d'éléphants ou configuration IAB
Centre de gestion 7.0 ou 7.1	Périphérique Snort 2	La configuration de l'IAB s'applique.
	Périphérique Snort 3	La configuration de l'IAB s'applique.
Centre de gestion 7.2.0	Périphérique Snort 2	La configuration de l'IAB s'applique.
	Périphérique Snort 3 (7.1.0 et versions antérieures)	La configuration de l'IAB s'applique.
	Périphérique Snort 3 (7.2.0 ou ultérieure)	La configuration d'Elephant Flow s'applique.

Configurer le flux d'éléphants

Vous pouvez configurer le flux d'éléphants pour qu'il agisse sur les flux d'éléphants, ce qui aide à résoudre des problèmes tels que la contraintes du système, une utilisation élevée du processeur, les abandons de paquets, etc.

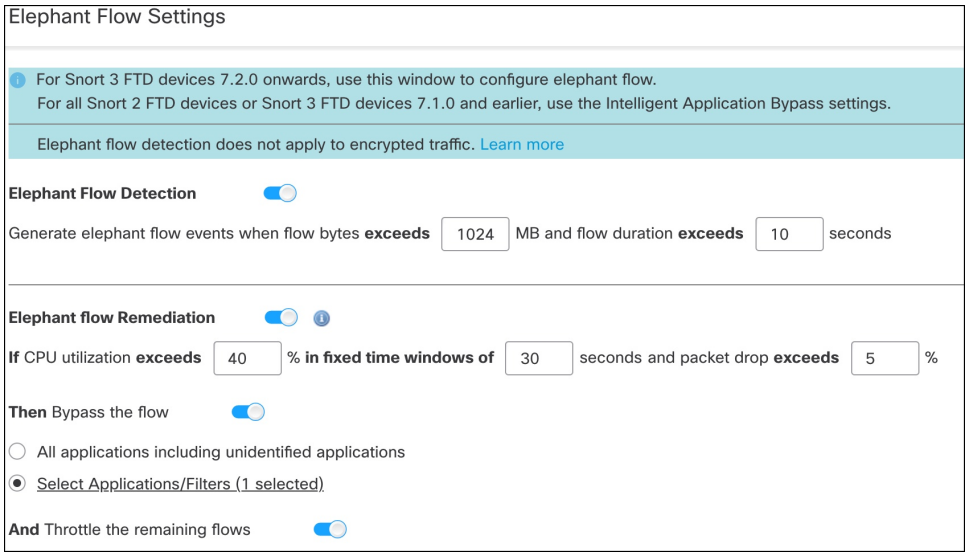
Attention La détection de flux d'éléphants ne s'applique pas aux flux préfiltrés, de confiance ou à avance rapide, qui ne passent pas par Snort. Étant donné que les flux d'éléphants sont détectés par Snort, la détection de flux d'éléphants ne s'applique pas au trafic chiffré.

Procédure

Étape 1 Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Illustration 1 : Configurer la détection du flux d'éléphants

Illustration 2 : Configurer la détection du flux d'éléphants



Étape 2 Le bouton à bascule **de détection de flux d'éléphants** est activé par défaut. Vous pouvez configurer les valeurs des octets de flux et de la durée du flux. Lorsqu'elles dépassent vos valeurs configurées, des événements de flux d'éléphants sont générés.

Étape 3 Pour corriger les flux d'éléphants, activez le bouton à bascule **Elephant Flow Remédiation** (correction du flux d'éléphants).

Étape 4 Pour définir les critères de correction du flux d'éléphants, configurez les valeurs du % d'utilisation de la CPU, de la durée des fenêtres horaires fixes et du % d'abandon de paquets.

L'utilisation du CPU est calculée par flux d'éléphants et dérivée de la latence du flux. Si l'utilisation du CPU franchit le seuil configuré et que d'autres configurations, telles que les fenêtres temporelles fixes et les abandons de paquets, correspondent également, les actions de correction de flux d'éléphants sont appliquées. De même, le calcul des abandons de paquets est basé sur le nombre de paquets abandonnés par CPU. Lorsque le pourcentage des abandons de paquets dépasse la valeur configurée sur un CPU donné, les actions de correction sont appliquées. Par exemple, considérons que les configurations sont définies par défaut, c'est-à-dire une utilisation du CPU de 40 %, une fenêtre temporelle fixe de 30 secondes et des abandons de paquets de 5 %. Sur un CPU donné, si plus de 5 % d'abandons de paquets sont détectés et que l'utilisation du CPU par flux dépasse 40 % pendant la période fixe de 30 secondes, les flux sont contournés ou régulés.

Étape 5 Vous pouvez effectuer les actions suivantes pour la correction de flux d'éléphants lorsqu'il répond aux critères configurés :

1. **Contourner le flux** : activez ce bouton pour contourner l'inspection Snort pour les applications ou les filtres sélectionnés. Choisissez parmi :

- **Toutes les applications, y compris les applications non identifiées :**sélectionnez cette option pour contourner tout le trafic des applications. Si vous configurez cette option, vous ne pouvez pas configurer l'action de limitation (taux-limite) pour aucun flux.
- **sélectionner les applications et les filtres** : sélectionnez cette option pour sélectionner les applications ou les filtres dont vous souhaitez contourner le trafic; Consultez la section **Configuration des conditions d'application et des filtres** dans le chapitre **Règles de contrôle d'accès du**Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

2. **Limitez le flux** : activez ce bouton pour appliquer la limite de débit au flux et continuer à inspecter les flux. Notez que vous pouvez sélectionner les applications ou les filtres pour contourner l'inspection Snort et limiter les flux restants.

Remarque
La suppression automatique de la limitation d'un flux d'éléphants limité se produit lorsque le système est protégé, c'est-à-dire que le pourcentage d'abandons de paquets Snort est inférieur au seuil configuré. Par conséquent, la limitation de débit est également supprimée.

Vous pouvez également supprimer manuellement la limitation d'un flux d'éléphants limité à l'aide des commandes Threat Defense suivantes :

- **clear efd-throttle <5-tuple/all> bypass** : cette commande supprime la limitation du flux d'éléphants et contourne l'inspection Snort.
- **clear efd-throttle <5-tuple/all>** : Cette commande supprime la limitation du flux d'éléphants et l'inspection Snort se poursuit. La correction de flux d'éléphants est ignorée après l'utilisation de cette commande.

  Pour en savoir plus sur ces commandes, consultez le Guide de référence des commandes de Cisco Secure Firewall Threat Defense.

Remarque
La prise de mesures sur la détection de flux d'éléphants n'est pas prise en charge sur les périphériques Cisco Firepower de la série 2100.

Étape 6 Cliquez sur **OK** pour enregistrer les paramètres de flux d'éléphants.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

Déployer les changements de configuration.

Après avoir configuré vos paramètres de flux d'éléphants, surveillez vos événements de connexion pour voir si des flux sont détectés, contournés ou limités. Vous pouvez le voir dans le champ **Reason** de votre événement de connexion. Les trois raisons des connexions de flux d'éléphants sont les suivantes :

- Flux d'éléphants
- Flux d'éléphants limité
- Flux d'éléphants de confiance

Attention L'activation de la détection de flux d'éléphants à elle seule n'entraîne pas la génération d'événements de connexion pour les flux d'éléphants. Si un événement de connexion est déjà enregistré pour une autre raison et que le flux est également un flux éléphant, le champ **Reason** (motif) contient cette information. Cependant, pour vous assurer que vous enregistrez tous les flux d'éléphants, vous devez activer la journalisation des connexions dans les règles de contrôle d'accès applicables.

Reportez-vous à Détection de flux d'éléphants dans Cisco Secure Firewall pour en savoir plus.

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.