



Politiques de prévention des intrusions personnalisées pour Snort 3

Dernière modification : 2026-10-28

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. Tous droits réservés.



TABLE DES MATIÈRES

CHAPITRE 1

Survol de la prévention des intrusions 1

Prévention contre les intrusions 1

Moteur d'inspection Snort 3

Snort 3 3

Prise en charge de plusieurs processus Snort 3 6

Désactiver la prise en charge multiprocessus de Snort 3 6

Inspection multicouche 7

Inspection d'en-tête 7

Fonctionnalités de la couche 7 8

Exemples de scénarios : 8

Limites de la couche d'encapsulation et comportement de l'inspection 9

Protocoles pris en charge et capacités d'inspection de LINA et Snort 3 9

Lignes directrices et limites relatives aux politiques d'analyse de réseau et de prévention des intrusions 10

Conditions préalables pour l'analyse de réseau et les politiques de prévention des intrusions 11

Comment les politiques examinent le trafic à la recherche d'intrusions 11

Décodage, normalisation et prétraitement : politiques d'analyse de réseau 13

Règles de contrôle d'accès : sélection de la politique de prévention des intrusions 14

Inspection d'intrusion : politiques, règles et ensembles de variables de prévention d'intrusion 15

Génération d'incidents de prévention des intrusions 17

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées 18

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système 19

Avantages de l'analyse personnalisée du réseau et des politiques de prévention des intrusions 21

Avantages des politiques d'analyse de réseau personnalisées 21

Avantages des politiques de prévention des intrusions personnalisées 22

Limites des politiques personnalisées 24

CHAPITRE 2**Migrer de Snort 2 vers Snort 3 27**

Plateforme d'inspection Snort 3 27

Snort 2 par rapport à Snort 3 28

Migration de Snort 2 vers Snort 3 28

Conditions préalables à la migration de Snort 2 vers Snort 3 29

Activer Snort 3 sur un périphérique individuel 29

Activer Snort 3 sur plusieurs périphériques 30

Convertir les règles IPS personnalisées de Snort 2 en Snort 3 31

Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3. 31

Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3 32

Afficher le mappage de politique de base Snort 2 et Snort 3 33

Synchroniser les règles de Snort 2 avec celles de Snort 3 34

Déploiement des modifications de configuration 36

Exemples de migration 38

Migrer de Snort 2 vers Snort 3 38

Avantages de la migration vers Snort 3 38

Exemple de scénario d'entreprise 38

Bonnes pratiques pour la migration de Snort 2 à Snort 3 39

Préalables pour la migration 39

Flux de travail de migration de bout en bout 39

Activer Snort 3 sur le périphérique de protection contre les menaces 40

Convertir les règles Snort 2 d'une politique de prévention des intrusions unique en Snort 3 41

CHAPITRE 3**Stratégies de prévention des intrusions 49**

Politique de prévention des intrusions 49

Création d'une politique de prévention des intrusions Snort 3 personnalisée 51

Modification des politiques de prévention des intrusions Snort 3 52

Rapport de groupe de règles 56

Journalisation des actions liées aux règles 57

Modifier la politique de base d'une politique de prévention des intrusions 58

Afficher le mappage de politique de base Snort 2 et Snort 3 59

Synchroniser les règles de Snort 2 avec celles de Snort 3	59
Gérer les politiques de prévention des intrusions	61
Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions	62
Configuration des règles de contrôle d'accès et politiques de prévention des intrusions	63
Configurer une règle de contrôle d'accès pour effectuer la prévention des intrusions	63
Régler les politiques de prévention des intrusions à l'aide de règles	64
Réglage des règles de prévention des intrusions	64
Types de règles de prévention des intrusions	65
Règles personnalisées dans Snort 3	66
Afficher les règles de prévention des intrusions Snort 3 dans une politique de prévention des intrusions	69
Actions des règles de prévention des intrusions	70
Options d'actions liées aux règles de prévention des intrusions	70
Définir une action de règle de prévention des intrusions	71
Filtres de notification d'incident d'intrusion dans une politique de prévention des intrusions	72
Seuils d'incidents d'intrusion	72
Configuration de la suppression des politiques de prévention des intrusions	75
Ajouter des commentaires sur les règles de prévention des intrusions	77
Préparer des règles personnalisées pour la conversion de SNORT 3	78
Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3.	79
Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3	80
Ajouter des règles personnalisées aux groupes de règles	81
Ajouter des groupes de règles avec des règles personnalisées à une politique de prévention des intrusions	82
Gérer les règles personnalisées dans Snort 3	83
Supprimer des règles personnalisées	84
Supprimer les groupes de règles	85
Règles recommandées	85
Modifications des règles Snort 3 dans les mises à jour des LSP	86
Règles conseillées pour Secure Firewall	86
Générer de nouvelles recommandations Secure Firewall dans Snort 3	87
Atténuer les menaces à l'aide du cadre MITRE dans les politiques de prévention des intrusions Snort 3	91

cadre MITRE	91
Avantages du cadre MITRE	91
Exemple de scénario d'entreprise pour le réseau MITER	92
Préalables pour le cadre MITRE	92
Afficher et modifier votre politique de prévention des intrusions Snort 3	92
Afficher les incidents d'intrusion	98
Références supplémentaires	101

CHAPITRE 4

Réglage du rendement de la prévention des intrusions	103
Réglage du rendement de la prévention des intrusions	103
Licence requise pour le réglage du rendement de la prévention des intrusions	104
Exigences et conditions préalables pour le réglage du rendement de la prévention des intrusions	104
Limitation de la mise en correspondance de modèles pour les intrusions	105
Remplacements des limites de l'expression régulière pour les règles d'intrusion	106
Remplacements des limites de l'expression régulière pour les règles de prévention des intrusions	107
Limites de génération d'incidents d'intrusion par paquet	108
Limitation des incidents de prévention des intrusions générés par paquet	109
Configuration du seuil de latence des paquets et des règles d'intrusion	109
Paramètres de performance en fonction de la latence	110
Seuil de latence des paquets	111
Remarques sur le seuil de latence des paquets	112
Activer le seuil de latence des paquets	112
Configuration du seuil de latence des paquets	113
Seuil de latence des règles	114
Remarques sur le seuil de latence des règles	116
Configurer le seuil de latence des règles	116
Configuration de la journalisation des statistiques de rendement en cas d'intrusion	117
Configuration de la journalisation des statistiques de rendement de la prévention des intrusions	118

CHAPITRE 5

Stratégies d'analyse de réseau	121
Analyse du réseau	121
Gérer les politiques d'analyse de réseau	122
Définitions et terminologies pour les politiques d'analyse de réseau Snort 3	123
Création d'une politique d'analyse de réseau personnalisée pour Snort 3	126

Sécurité du Protocole industriel commun (CIP)	129
Détection et blocage des segments de sécurité dans les paquets CIP	130
Mappage de la stratégie d'analyse du réseau	131
Afficher le mappage de la politique d'analyse des réseaux	131
Créer une politique d'analyse de réseau	132
Modifier la politique d'analyse de réseau	132
Rechercher un inspecteur dans la page des politiques d'analyse de réseau.	133
Copier la configuration de l'inspecteur	134
Personnaliser la politique d'analyse de réseau	134
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration	138
Annuler les modifications non enregistrées lors des modifications en ligne	140
Afficher la liste des inspecteurs avec remplacements	140
Rétablir la configuration remplacée à la configuration par défaut	141
Valider les politiques Snort 3	142
Exemples de configuration de politique d'analyse de réseau personnalisée	144
Paramètres de politique d'analyse de réseau et modifications en cache	155
Générer des recommandations Snort 3	156
Recommandations de règles Snort 3	156
Avantages	156
Exemple de scénario d'entreprise	156
Bonnes pratiques	157
Conditions préalables à la génération de recommandations	157
Générer des recommandations Snort 3	157

CHAPITRE 6

Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion 161

Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion	161
Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion	162
Exigences et conditions préalables pour les paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion	162
Inspection des paquets qui passent avant que le trafic ne soit identifié	163
Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic	163
Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic	164

Paramètres avancés pour les politiques d'analyse de réseau	165
Définir la politique d'analyse du réseau par défaut	166
Règles d'analyse du réseau	167
Conditions des règles de politique d'analyse de réseau	167
Configuration des règles d'analyse du réseau	169
Gestion des règles d'analyse du réseau	170



CHAPITRE 1

Survol de la prévention des intrusions

Le moteur d'inspection Snort fait partie intégrale de Firewall Threat Defense. Dans la plupart des cas, les politiques fournies par le système sont tout ce dont vous avez besoin. Pour les utilisateurs avancés ayant des besoins spécifiques, vous pouvez créer des règles personnalisées.



Remarque

Pour configurer des règles Snort 2 personnalisées, voir [Politiques de prévention des intrusions personnalisées pour Snort 2](#).

- [Prévention contre les intrusions, à la page 1](#)
- [Moteur d'inspection Snort, à la page 3](#)
- [Snort 3, à la page 3](#)
- [Inspection multicouche, à la page 7](#)
- [Lignes directrices et limites relatives aux politiques d'analyse de réseau et de prévention des intrusions, à la page 10](#)
- [Conditions préalables pour l'analyse de réseau et les politiques de prévention des intrusions, à la page 11](#)
- [Comment les politiques examinent le trafic à la recherche d'intrusions, à la page 11](#)
- [Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées, à la page 18](#)

Prévention contre les 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. Il est parfois appelé « système de détection d'intrusion (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. Il est parfois appelé « système de prévention des intrusions (IPS) ».
- utilise des politiques d'analyse de réseau et de prévention des intrusions pour fournir une inspection complète des paquets et une protection contre les menaces.

Composants et fonctionnement de la prévention des intrusions

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](#)

**Attention**

Obsolescence du mode de détection : à partir de la version 7.4.0 du centre de gestion, pour une politique d'analyse de réseau (NAP), le mode d'inspection de détection est obsolète et sera supprimé dans une prochaine version.

Le mode de détection était destiné à être utilisé comme mode de test afin que vous puissiez activer les inspections et voir comment elles se comportent dans votre réseau avant de le configurer pour abandonner le trafic, c'est-à-dire pour afficher le trafic qui serait abandonné.

Ce comportement est amélioré lorsque tous les abandons de l'inspecteur sont contrôlés par l'état de la règle et que vous pouvez définir chacun d'eux pour générer des événements. Ceci est fait pour les tester avant de configurer l'état de la règle pour abandonner le trafic. Comme nous avons maintenant un contrôle fin des pertes de trafic dans Snort 3, le mode de détection ne fait qu'ajouter plus de complexité au produit et n'est pas nécessaire, le mode de détection est donc obsolète.

Si vous modifiez une Politique d'analyse de réseau (NAP) de détection à Prévention, la Politique d'analyse de réseau (NAP) qui traite le trafic des incidents d'intrusion qui « sera abandonnée » est « abandonnée », et le trafic correspondant abandonnera le trafic de ces événements. Cela s'applique aux règles dont les GID ne sont pas 1 ou 3. Les GID 1 et 3 sont des règles de texte ou compilées (généralement fournies par Talos ou à partir de vos règles personnalisées ou importées), et tous les autres GID sont des inspections pour détecter des anomalies. Il s'agit de règles moins courantes à déclencher dans un réseau. Il est peu probable que le passage en mode de prévention ait un impact sur le trafic. Il vous suffit de désactiver la règle de prévention des intrusions qui s'applique au trafic abandonné et de la régler sur généré ou désactivé.

Nous vous recommandons de choisir Prévention comme mode d'inspection, mais si vous choisissez Prévention, vous ne pouvez pas revenir au mode Détection.

Moteur d'inspection Snort

Un moteur d'inspection Snort est un composant intégré d'analyse du trafic qui

- analyse le trafic en temps réel pour fournir une inspection approfondie des paquets,
- fonctionne dans le cadre du périphérique Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense), et
- active les politiques d'analyse de réseau et de prévention des intrusions pour détecter les intrusions et les protéger.

Snort 3

Snort 3 est un moteur d'inspection de réseau qui

- fournit de vastes améliorations par rapport à la version précédente de Snort,
- offre un fonctionnement plus efficace avec de meilleures performances et une plus grande évolutivité, et
- dont l'architecture a été repensée pour inspecter plus de trafic avec des ressources équivalentes par rapport à Snort 2.

Modifications et améliorations de Snort 3

L'ancienne version de Snort est Snort 2, qui n'est plus prise en charge. 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 Firewall Threat Defense : le moteur d'inspection Snort est spécifique à Firewall Threat Defense et non au Cisco Secure Firewall Management Center (anciennement le centre de gestion Cisco Firepower Management Center). Firewall Management Center peut gérer plusieurs Firewall 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 Firewall Management Centers soient 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 Firewall Threat Defense la version 7.0 ou ultérieure. Elle n'est pas prise en charge par ASA FirePOWER ou NGIPSv.
- Périphériques gérés—Un Firewall Management Center avec 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 Firewall Threat Defenses, et la version 7.0 de Snort 3 Firewall Threat Defenses.
- 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 Firewall 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 Firewall Management Center 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 Firewall Management Center 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 Firewall Management Center et Firewall Threat Defense version 7.0 ou supérieure. Lorsque vous mettez à niveau un Firewall Management Center 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.
- Annulation des règles de remplacement Snort 2 et Snort 3 : lorsqu'un Firewall Threat Defense est mis à niveau vers la version 7.0, vous pouvez mettre à niveau la plateforme d'inspection de Firewall Threat Defense vers la version Snort 3. Firewall Management Center 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 Firewall Threat Defense à la version 7.0, ils doivent être synchronisés manuellement.
- 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.
- Groupes de règles : Firewall Management Center regroupe toutes les règles de Snort 3 en groupes de règles. Les groupes de règles sont des groupes logiques de règles qui fournissent une interface de gestion simple pour améliorer l'accessibilité des règles, la navigation dans les règles et un meilleur contrôle sur le niveau de sécurité des groupes de règles.

À partir de Firewall Management Center 7.3.0, la navigation par les règles est prise en charge pour plusieurs niveaux de groupes de règles, ce qui offre plus de flexibilité et un ensemble logique des règles. Le cadre MITRE est ajouté et vous permet de naviguer dans les règles à l'aide du cadre MITRE. MITRE n'est qu'une autre catégorie de groupes de règles et fait partie des groupes de règles Talos.



Remarque

Consultez <https://attack.mitre.org> pour obtenir des renseignements sur MITRE.

Une règle peut faire partie de plusieurs groupes de règles, p. ex., plusieurs groupes de règles MITRE ATT&CK, un groupe de règles de catégorie de règles, plusieurs groupes de règles de « type de ressource », une campagne contre des programmes malveillants, etc. Les groupes de règles disponibles sont répertoriés dans l'éditeur de politiques de prévention des intrusions et peuvent être sélectionnés pour améliorer les politiques.

Grâce à cette structure hiérarchique à plusieurs niveaux, vous pouvez parcourir jusqu'au dernier élément, qui est le « groupe de règles descendant ». Ces groupes de règles contiennent des ensembles de règles liées les unes aux autres, comme un type de vulnérabilité spécifique, un système cible similaire ou une catégorie de menace similaire. Les groupes de règles sont associés à quatre niveaux de sécurité. Vous pouvez modifier le niveau de sécurité, ajouter ou supprimer des groupes de règles, et vous pouvez modifier l'action découlant d'une règle pour les règles qui correspondent au trafic observé sur le réseau. Cela est fait pour apporter un équilibre satisfaisant entre la sécurité, les performances et la résistance aux faux positifs.

Prise en charge de plusieurs processus Snort 3

Prise en charge de plusieurs processus Snort 3

- Sur les périphériques Secure Firewall 6160 et 6170 exécutant la version 10.0 de Secure Firewall, par défaut, Snort 3 associe plusieurs threads à deux instances de Snort.
- Lors du déploiement, chaque instance Snort 3 est automatiquement configurée avec les fils requis.
- Il en résulte une charge de mémoire réduite, un conflit de verrouillage réduit et des temps de génération de cœur plus courts pour améliorer la résilience, les performances et l'évolutivité.

Architecture multiprocessus Snort 3

Les instances Snort 3 individuelles offrent plusieurs avantages. Toute défaillance d'instance Snort entraîne un impact minimal sur le trafic et vous pouvez également redémarrer un seul processus Snort, le cas échéant.

Les fils Snort sont distribués sur les nœuds NUMA où chaque nœud est considéré comme un processeur indépendant. Cela garantit que les limites de mémoire sont respectées. Par exemple, l'instance Snort 0 utilise la mémoire du nœud 0 et l'instance 1 utilise la mémoire du nœud 1.

Les sorties CLI de commandes telles que **show coredump** et **show perfstats** ont été améliorées pour afficher des informations sur les deux instances Snort. Dans le centre de gestion, accédez à **Résolution de problèmes> Surveiller> Périphériques** pour afficher les sections **Aperçu> Processus critiques** et **Mémoire** pour obtenir des renseignements sur les deux instances Snort. S'il y a des erreurs de profilage de règle, le numéro d'instance Snort s'affiche avec l'erreur.

Désactiver la prise en charge multiprocessus de Snort 3

Cette tâche désactive la prise en charge de plusieurs processus Snort 3.

La désactivation de la prise en charge de processus multiples est destinée à des fins de débogage uniquement et nécessite un déploiement manuel pour prendre effet.

Procédure

Étape 1 Utilisez la commande **configure snort multi-process disable** pour désactiver la prise en charge de plusieurs processus Snort 3.

Exemple :

```
> configure snort multi-process disable
```

```
Caution: this command is intended for debugging purposes only.
A deployment is required after enabling/disabling multi-process and will cause a Snort
restart and temporary traffic interruption.
```

```
-----
Do you still want to continue?
Please enter 'YES' or 'NO': YES
Please perform a manual deployment to disable multi-process.
```

**Remarque**

Cette commande entraîne le redémarrage du moteur Snort et entraînera également une interruption du trafic lors du prochain déploiement, lorsque Snort passera de l'état multi-processus à un état de processus unique.

Étape 2

Redéployez la configuration pour vous assurer que la prise en charge multiprocessus de Snort 3 est désactivée.

Inspection multicouche

La fonctionnalité d'inspection multicouche dans Snort 3 vous permet d'inspecter le trafic sur plusieurs couches de protocole au cours d'une même session.

Snort 3 peut inspecter simultanément les couches suivantes :

- Couche réseau (L3) : adresses IP, fragmentation
- Couche de transport (L4) : ports TCP ou UDP, indicateurs, suivi de session
- Couche d'application (L7) : HTTP, DNS, SMTP, TLS, SIP et autres.
- Couche des fichiers et de charge utile : extraction des fichiers, signatures des programmes malveillants, contenu intégré

Snort 3 prend en charge le décodage pour un large éventail de protocoles. Il inspecte les protocoles encapsulés et évalue les en-têtes de paquets pour déterminer les actions des politiques lors de l'inspection avancée des menaces.

Inspection d'en-tête

Sur les versions antérieures à 7.6.4

Pour les protocoles d'encapsulation non pris en charge par Lina, le système fait correspondre initialement le trafic en fonction de l'en-tête IP externe. L'évaluation ultérieure dépend des critères de la règle :

- Règles sans critères de couche 7 (L7) : si la règle en correspondance n'inclut pas de critères L7 (comme l'URL, l'ID d'application ou l'identité de l'utilisateur), le système applique la règle en fonction de l'en-tête IP externe.
- Règles avec critères de couche 7 (L7) : si la règle comprend des critères L7, le système utilise la correspondance d'en-tête IP externe comme point de départ, puis effectue une évaluation supplémentaire à l'aide de l'en-tête le plus interne.

Ce comportement peut entraîner des résultats inattendus, comme une règle non L7 correspondant à l'en-tête de l'IP externe prenant le pas sur une règle correspondant à l'en-tête de l'IP interne situé plus bas dans l'ensemble de règles.

Sur la version 7.6.4 et les versions ultérieures

- Snort 3 inspecte toujours l'en-tête le plus à l'intérieur pour détecter les protocoles non pris en charge par Lina, quelle que soit la présence de règles de couche 7.
- Les règles basées sur l'en-tête externe ne sont pas suffisantes pour l'application des politiques pour des protocoles tels que VXLAN. Snort 3 ne tient pas compte des détails de la connexion pour l'action dans de tels cas, en utilisant plutôt le contenu réel du paquet.
- Pour les protocoles pris en charge par Lina, l'action de la politique continue d'être basée sur l'en-tête le plus à l'intérieur.
- Si vous gérez actuellement le trafic encapsulé pour des protocoles non pris en charge par Lina (comme VXLAN) en utilisant uniquement des règles d'IP externe, sachez que dans la version 7.6.4 ou une version ultérieure, ce trafic sera géré par la règle de contrôle d'accès par défaut. Dans un tel scénario, si votre action de politique par défaut est définie sur « Bloquer », cela peut entraîner l'abandon du trafic. Nous vous recommandons de passer en revue et de mettre à jour les politiques de contrôle d'accès pour qu'elles correspondent à l'en-tête IP interne pour ces protocoles, en plus de toute configuration d'en-tête IP externe existante.

Fonctionnalités de la couche 7

Pour le trafic encapsulé dans les fonctionnalités de couche 7, seul l'en-tête IP le plus à l'intérieur doit correspondre dans les règles. Les règles d'en-tête externe uniquement ne s'appliqueront pas.

Exemples de scénarios :

Le tableau suivant répertorie des exemples basés sur différents paramètres.

Protocole	Version	Règle IP externe	Règle IP interne	Règle L7 requise	Résultat
VXLAN (non pris en charge par LINA)	7.6.2	Oui	Non	Non	Trafic autorisé si l'en-tête externe correspond
VXLAN (non pris en charge par LINA)	7.6.4	Non	Oui	Non	Trafic autorisé si l'en-tête interne correspond
GRE (pris en charge par LINA)	7.6.2 et 7.6.4	Non	Oui	Non	Trafic autorisé si l'en-tête interne correspond
Fonctionnalité VXLAN + L7	7.6.2 et 7.6.4	Non	Oui	Oui	Règle d'en-tête interne requise

**Remarque**

Une règle d'IP externe fait correspondre le trafic en fonction des points d'extrémité du tunnel. Elle évalue :

- L'adresse IP source du périphérique d'encapsulation
- L'adresse IP de destination du périphérique d'encapsulation

Une règle d'IP interne fait correspondre le trafic en fonction du paquet IP d'origine dans le tunnel. Elle évalue :

- L'adresse IP réelle du client
- L'adresse IP réelle du serveur de destination

Limites de la couche d'encapsulation et comportement de l'inspection

Lors de la gestion du trafic encapsulé, il est important de comprendre les limites de traitement des deux principaux moteurs d'inspection du système, Lina et Snort.

- LINA : prend en charge le décodage jusqu'à 2 couches d'encapsulation.
- Snort : prend en charge le décodage jusqu'à 255 couches d'encapsulation (avec une limite par défaut de 40).

Protocoles pris en charge et capacités d'inspection de LINA et Snort 3

LINA

LINA prend en charge le décodage pour les protocoles suivants sur les couches de liaison de données (L2), de réseau (L3) et de transport (L4).

Couche	Protocoles et en-têtes pris en charge
couche 2	Cisco MetaData (CMD), IEEE 802.1Q, IEEE 802.1ad (DOT1AD) et Q-in-Q (EtherTypes 0x9100 et 0x9200). Prend en charge jusqu'à trois niveaux d'en-têtes de VLAN.
Couche 3	IPv4, IPv6
Couche 4	ICMP (v4/v6), ESP, VXLAN, Geneve, GRE, IP-en-IP et IPv6-en-IPv6. Prend en charge jusqu'à 1 niveau d'encapsulation.

Prise en charge spécifique de GRE

Pour le trafic GRE, le système prend en charge le décodage pour les types de protocoles suivants :

- protocole PPTP (Point-to-Point Tunneling Protocol)

- Protocole WCCP (Web Cache Communication Protocol)

Traitement ERSPAN

Le système décode GRE et ERSPAN (types 1, 2 et 3). Pour faciliter l'équilibrage de la charge de la couche de répartition, le système ignore en interne les en-têtes internes. Par conséquent, les autres modules ne peuvent pas inspecter les en-têtes ERSPAN.

Snort 3

Alors que Snort 3 prend en charge un vaste ensemble de protocoles, la liste suivante met en évidence les protocoles d'encapsulation et de tunnellation courants pris en charge pour l'inspection :

- VXLAN
- GRE
- Teredo
- GTP
- MPLS
- Geneve
- IP dans IP
 - IPv4-dans-IPv4
 - IPv6-dans-IPv4
 - IPv4-dans-IPv6
 - IPv6-dans-IPv6



Remarque

Cette liste n'est pas exhaustive. Snort 3 est conçu pour décoder un large éventail de protocoles standard de l'industrie.

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

Limites de la fonctionnalité Snort 3 pour Firewall Threat Defense géré par Firewall Management Center

Le tableau répertorie les fonctions prises en charge sur Snort 2 mais non sur Snort 3 pour les périphériques Firewall Management Center gérés Firewall Threat Defense.

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 de prévention des intrusions	• 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	Nom de domaine complet (FQDN).

Conditions préalables pour l'analyse de réseau et les politiques 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 Firewall 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 les politiques examinent le trafic à la recherche d'intrusions

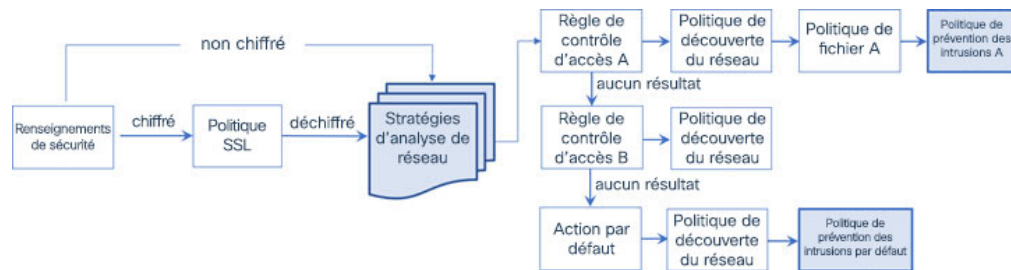
Lorsque le système analyse le trafic dans le cadre de votre déploiement de contrôle d'accès, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (règles de prévention des intrusions et paramètres avancés).

process_summary

Les composants clés concernés dans l'examen du trafic pour détecter les intrusions sont les suivants :

- Security Intelligence : effectue le filtrage et le blocage initiaux du trafic
- Politique SSL : gère l'inspection et le déchiffrement du trafic chiffré
- Politiques d'analyse du réseau : effectuer le décodage et le prétraitement du trafic
- Règles de contrôle d'accès : déterminez les politiques à appliquer au trafic

- ## process_workflow



12

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 échappent 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.
- 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 incidents 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

La sélection de la politique de prévention des intrusions est un processus d'évaluation du trafic qui :

- évalue le trafic après le prétraitement initial
- applique la règle de contrôle d'accès correspondante pour gérer le trafic par le biais des actions de supervision, de confiance, de blocage ou d'autorisation,
- inspecte le trafic autorisé pour les données de découverte, les programmes malveillants, les fichiers interdits et les intrusions dans cet ordre, et
- gère le trafic non correspondant à l'aide de l'action par défaut de la stratégie de contrôle d'accès.

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.

Processus d'évaluation du trafic

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 stratégie de contrôle d'accès, qui peut également inspecter les données de découverte et les intrusions.

**Remarque**

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

Le diagramme [Comment les politiques examinent le trafic à la recherche d'intrusions, à la page 11](#) montre le flux du trafic à travers un périphérique dans un déploiement en ligne de prévention des intrusions et AMP for Networks :

- 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 dont 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 stratégie de contrôle d'accès autorise le trafic correspondant. 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

L'inspection de prévention des intrusions est un mécanisme de sécurité qui

- utilise des politiques d'intrusion pour régir la manière dont le système inspecte le trafic à la recherche de violations de la sécurité et, dans les déploiements en ligne, peut bloquer ou modifier le trafic malveillant.
- emploie des règles de prévention des intrusions et de préprocesseur pour analyser le trafic réseau en fonction de critères spécifiés et détecter les tentatives d'exploit des vulnérabilités, et
- utilise des ensembles de variables pour définir des valeurs couramment utilisées dans les règles d'intrusion pour identifier les adresses IP et les ports source et destination.

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 Firewall Threat Defense sur Firewall Management Center.

Génération d'incidents de prévention des intrusions

La génération d'incidents d'intrusion est un mécanisme de sécurité qui :

- détecte les intrusions possibles grâce au décodage des paquets, au prétraitement et à l'analyse du moteur de règles,
- génère *des incidents d'intrusion ou de préprocesseur* (parfois appelés collectivement *incidents d'intrusion*) lorsque des menaces sont détectées, et
- transmet les incidents des périphériques gérés à Firewall Management Center pour une analyse agrégée et une protection des ressources réseau.

Création d'incidents et collecte de données

Chaque incident d'intrusion dans la base de données comprend un en-tête d'incidents et contient des informations sur le nom et la classification de l'incident; les adresses IP de source et de destination; les ports; le processus qui a généré l'incident; et la date et l'heure de l'incident, 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.

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.

Scénarios de génération d'incidents

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.

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

L'analyse du réseau et les politiques de prévention des intrusions sont des mécanismes de sécurité qui

- examinent le trafic à travers les étapes de prétraitement et de prévention des intrusions,
- fournissent des configurations par défaut fournies par le système pour un déploiement immédiat, et
- permettent la création de politiques personnalisées pour les exigences de sécurité adaptées.

Comportement de la politique par défaut dans les déploiements de contrôle d'accès

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.

Ce diagramme montre comment une nouvelle stratégie de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic :



Le flux du trafic présente ces caractéristiques :

- 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

Les politiques d'analyse de réseau et de prévention des intrusions fournies par le système sont des configurations de sécurité qui

- tirent parti de l'expérience de Cisco Talos Intelligence Group (Talos) pour les états de règles de prévention des intrusions et d'inspection et les paramètres avancés,
- fournissent des points de départ pour des politiques de défense bien réglées couvrant les configurations réseau courantes, et
- reçoivent des mises à jour automatiques par le biais des versions du paquet de sécurité allégé (LSP) pour les nouvelles vulnérabilités.

Caractéristiques clés et utilisation

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 redéployent 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, ce qui déploie également tout SSL associé, ainsi que les politiques d'analyse de réseau et de fichiers différentes de celles en cours d'exécution, et peut 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 du système :

- Politiques d'analyse de réseau et de prévention des intrusions 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 d'analyse de réseau et de prévention des intrusions pour la connectivité et la sécurité : ces politiques sont destinées aux entreprises où la connectivité (la possibilité d'accéder à toutes les ressources) prévaut sur la sécurité de l'infrastructure du 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 d'analyse de réseau et de prévention des intrusions Security Over Connectivity (sécurité au-dessus de la connectivité) : ces politiques sont conçues pour les entreprises où la sécurité de l'infrastructure réseau prévaut sur la commodité de 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 Détection maximale : ces politiques sont destinées aux organisations qui accordent à la sécurité de l'infrastructure du réseau une importance encore plus grande que celle accordée à la politique de sécurité sur la connectivité, avec un potentiel de répercussions opérationnelles encore plus important. 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 troupes 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 **Edit** (Modifier) à côté de la politique, puis cliquez sur la liste déroulante **Manage Base Policy** (Gestion de la politique de base).

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

Les politiques d'analyse de réseau personnalisées et de prévention des intrusions sont des configurations de sécurité qui :

- améliorent les performances du système dans votre environnement spécifique,
- fournissent une vue axée sur le trafic malveillant et les violations des politiques qui se produisent sur votre réseau, et
- permettent une configuration granulaire de la façon dont le système traite et inspecte le trafic réseau pour détecter les intrusions.

Structure de la politique personnalisée

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.

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

Politiques d'analyse de réseau personnalisées :

- permettre le prétraitement de réglage pour correspondre à des caractéristiques de trafic spécifiques et aux exigences de surveillance,
- réduire le surdébit du traitement du système en désactivant les inspecteurs inutiles, et
- permettre un prétraitement personnalisé pour différentes zones de sécurité, réseaux ou VLAN dans les déploiements complexes.

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, les sessions SSL chiffrées, ou des ports sur lesquels vous décidez le trafic Telnet, HTTP et RPC.

Si vous êtes un utilisateur avancé avec un déploiement complexe, vous pouvez créer plusieurs politiques d'analyse de 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

Les politiques de prévention des intrusions personnalisées sont des configurations de sécurité qui

- permettent une inspection sur mesure du trafic au moyen de plusieurs politiques de prévention des intrusions spécialisées
- gèrent les règles de prévention des intrusions et d'inspection qui sont activées et la manière dont elles sont configurées, et
- permettent aux règles de contrôle d'accès de préciser quelle politique inspecte quel trafic en fonction de plusieurs critères.

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

ajoutez des règles de contrôle d'accès ou changez 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 recommandations Cisco 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. Pour chaque 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 soit 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. Ce diagramme montre comment une nouvelle stratégie 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.

Vous pouvez régler le prétraitement en créant et en utilisant une politique d'analyse de réseau personnalisée comme politique 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.



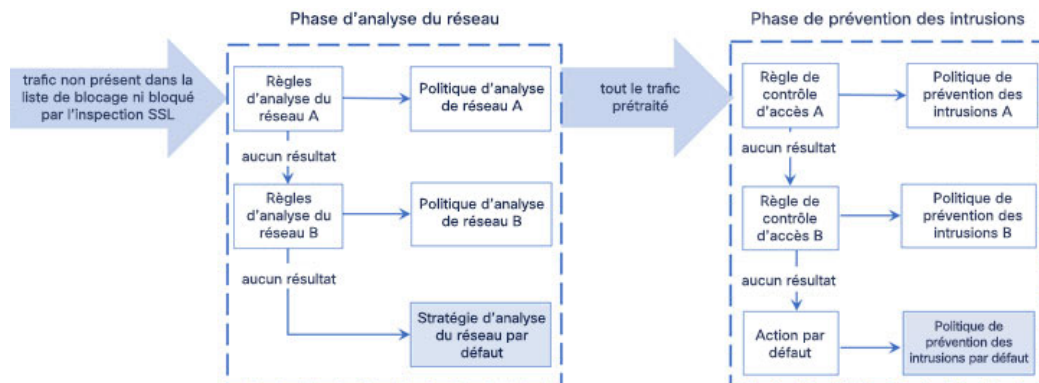
Astuces

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 elles.

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**.

Veillez 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.



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 Firewall Threat Defense avec Firewall Management Center. Snort 3 est requis dans la version 7.7 ou ultérieure. 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 Firewall 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. La mise à niveau de Firewall Threat Defense vers la version 7.7 ou ultérieure est bloquée pour les périphériques Snort 2.

- [Plateforme d'inspection Snort 3, à la page 27](#)
- [Snort 2 par rapport à Snort 3, à la page 28](#)
- [Migration de Snort 2 vers Snort 3, à la page 28](#)
- [Afficher le mappage de politique de base Snort 2 et Snort 3, à la page 33](#)
- [Synchroniser les règles de Snort 2 avec celles de Snort 3, à la page 34](#)
- [Déploiement des modifications de configuration, à la page 36](#)
- [Exemples de migration, à la page 38](#)

Plateforme d'inspection Snort 3

Snort 3 est un moteur d'inspection de réseau qui

- sert de moteur d'inspection par défaut pour les périphériques Firewall Threat Defense nouvellement enregistrés sur la version 7.0 ou ultérieure,
- nécessite une activation explicite après la mise à niveau des périphériques Firewall Threat Defense vers la version 7.0 ou une version ultérieure, et
- active la version Snort 3 de la politique de prévention des intrusions, qui est appliquée par le biais des politiques de contrôle d'accès, pour tout le trafic passant par le périphérique.

Pour les périphériques Firewall Threat Defense sur la version 6.x ou toute version antérieure, Snort 2 est le moteur d'inspection par défaut.

Commutation de version et mappage de règles

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 34.

Snort 2 par rapport à Snort 3

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.

Le tableau ci-dessous répertorie les différences entre les versions Snort 2 et Snort 3 en termes de capacités du moteur d'inspection.

Fonctionnalités	Snort 2	Snort 3
Fils de paquets	Un par processus	N'importe quel nombre par processus
Utilisation de la mémoire de configuration	Nombre de processus * x Go	x Go au total; plus de mémoire disponible pour les paquets
Rechargement de la configuration	Plus lent	Plus rapide; un fil peut être épinglé à des cœurs distincts
Syntaxe des règles	Incohérent et nécessite des échappements de ligne	Système uniforme avec espaces aléatoires
Commentaire sur la règle	Commentaires seulement	les marques #, #begin et #end; Le style de langage C

Référence supplémentaire : [Différences entre Snort 2 et Snort 3 dans Firepower](#)

Migration de Snort 2 vers Snort 3

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

process_summary

Selon vos besoins, passez par les étapes énumérées dans le flux de travail pour terminer la migration de votre périphérique de Snort 2 vers Snort 3.

process_workflow

Voici les étapes de la migration de Snort 2 vers Snort 3 :

1. Activez Snort 3 sur le périphérique.
 - [Activer Snort 3 sur un périphérique individuel](#), à la page 29
 - [Activer Snort 3 sur plusieurs périphériques](#), à la page 30
2. Convertissez 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 31
 - [Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3](#), à la page 32
3. Synchronisez les règles de Snort 2 avec celles de Snort 3.
 - [Synchroniser les règles de Snort 2 avec celles de Snort 3](#), à la page 34

Conditions préalables à la migration de Snort 2 vers Snort 3

Tenez compte des conditions préalables recommandées avant de migrer votre appareil de Snort 2 à 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

Activez Snort 3 sur un périphérique individuel pour profiter de fonctionnalités de sécurité renforcées.

Utilisez cette procédure lorsque vous devez mettre à niveau un périphérique spécifique du moteur d'inspection Snort 2 à Snort 3. Le système convertit vos configurations de politiques au cours du processus de déploiement pour les rendre compatibles avec la version sélectionnée de Snort.



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 [Déploiement des modifications de configuration, à la page 36](#).

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

Cette tâche permet à Snort 3 sur plusieurs périphériques de fournir des capacités de détection d'intrusion améliorées.

Pour activer Snort 3 sur plusieurs périphériques, assurez-vous que tous les périphériques Firewall 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).
- Étape 4** Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez [Déploiement des modifications de configuration, à la page 36](#).

Convertir les règles IPS personnalisées de Snort 2 en Snort 3

La conversion des règles IPS personnalisées Snort 2 au format Snort 3 est un processus de migration qui modifie les règles du système de prévention des intrusions personnalisées du format Snort 2 au format Snort 3.

Exigences de conversion et ressources

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 31](#)
- [Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 32](#)



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.

Convertissez les règles personnalisées Snort 2 existantes au format Snort 3 mis à jour pour assurer la compatibilité avec les systèmes de détection d'intrusion actuels.

Cette tâche migre les règles personnalisées Snort 2 existantes vers le format Snort 3, vous permettant de conserver vos configurations de règles personnalisées lors de la mise à niveau vers le dernier moteur de détection d'intrusion. Vous pouvez soit importer les règles converties directement, soit les télécharger pour les consulter avant de les importer.

Procédure

-
- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (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 Firewall Management Center 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 81](#).

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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration, à la page 36](#).

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

Convertissez les règles personnalisées Snort 2 dans une politique de prévention des intrusions au format Snort 3 pour maintenir la compatibilité avec les environnements Snort 3.

Lors de la migration vers Snort 3, les règles personnalisées Snort 2 existantes doivent être converties pour conserver leurs fonctionnalités. Cette tâche vous permet de convertir des règles personnalisées pour une politique de prévention des intrusions spécifique.

Procédure

- Étape 1** Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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 bleue **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 **Custom Rules** (Règles personnalisées).

Étape 5 Choisissez :

- **Import converted rules to this policy** (Importer les règles converties dans cette politique) : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans Firewall Management Center en tant que règles personnalisées Snort 3.
- **Download converted rules** (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration, à la page 36](#).

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

Cette tâche vous permet d'afficher le mappage entre les politiques de prévention des intrusions Snort 3 et Snort 2.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Procédure

-
- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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

Cette tâche permet de s'assurer que les paramètres de remplacement de règles Snort 2 et les règles personnalisées sont répliqués sur Snort 3, vous permettant de commencer avec une couverture similaire lors de la transition entre les versions.

Pour s'assurer que les paramètres et les règles personnalisées de la version Snort 2 sont conservés et transférés dans Snort 3, Firewall Management Center 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.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Si Firewall Management Center 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 Firewall Management Center. 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

Lorsque vous passez à Snort 3, gérez la version Snort 3 de la politique de manière indépendante. N'utilisez pas cet utilitaire comme une opération normale.

**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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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 bleue **Versions Snort synchronisées** (→).

- Étape 6** Lisez le résumé. Téléchargez une copie du résumé, au besoin.
- 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 Custom Rules (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 32.

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Déploiement des modifications de configuration

Déployez les modifications de configuration pour vous assurer que les modifications apportées aux configurations des périphériques prennent effet sur les périphériques concernés.

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 vous reporter à la rubrique sur le *déploiement des modifications de configuration* dans la dernière version du [Guide de configuration des appareils du système de gestion de Cisco Secure Firewall](#) pour comprendre les conditions préalables et les conséquences du déploiement des modifications avant de procéder aux étapes.



Mise en garde

Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon d'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 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.

- Recherche : recherchez par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Développer : cliquez sur **Flèche Développer** (►) pour afficher les modifications de configuration propres au périphérique à déployer.

Si vous cochez une case à côté d'un périphérique, toutes les modifications apportées à ce périphérique et répertoriées pour le périphérique sont incluses dans le 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 Firewall 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 Firewall Management Center. 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 Firewall Management Center.

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 :

- Déployer : continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Fermer : quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Les modifications de configuration sont déployées sur les périphériques sélectionnés et prennent effet en fonction des paramètres de déploiement.

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 Déployer les modifications de configuration dans la dernière version du [Guide de configuration des appareils du système de gestion de Cisco Secure Firewall](#).

Exemples de migration

Migrer de Snort 2 vers Snort 3

Migration de Snort 2 vers Snort 3

- implique la conversion et l'adaptation des règles Snort 2 à la syntaxe de la règle Snort 3,
- optimise les règles pour améliorer la détection et les performances, et
- permet aux entreprises de tirer parti des fonctionnalités et des capacités améliorées de Snort 3.

Les entreprises dont les périphériques de protection contre les menaces sont gérés par le centre de gestion de pare-feu Cisco Secure Firewall Management Center peuvent choisir une approche de déploiement hybride lors de la migration de Snort 2 à Snort 3. Cette approche permet une transition graduelle et réduit les perturbations potentielles, le cas échéant.

Avantages de la migration vers Snort 3

Snort 3 fournit

- **Enhanced protocol support** (Prise en charge améliorée des protocoles) : Snort 3 offre une prise en charge améliorée des protocoles, vous permettant de détecter et de superviser les menaces sur un large éventail de protocoles modernes, y compris le trafic chiffré.
- **Streamlined rule management** (Gestion simplifiée des règles) : Snort 3 offre un langage de règles et un système de gestion de règles plus convivial, ce qui permet de créer, de modifier et de gérer efficacement les règles.
- **Improved performance** (Performances améliorées) : Snort 3 a été optimisé pour gérer des volumes de trafic plus élevés plus efficacement, ce qui garantit une détection rapide des menaces et réduit le risque de goulot d'étranglement des performances.

Exemple de scénario d'entreprise

Cet exemple de scénario d'entreprise est une situation illustrative qui

- montre comment les entreprises évaluent les migrations des moteurs d'inspection de sécurité des réseaux,
- affiche les rôles et les motivations des analystes de sécurité et des administrateurs réseau dans les décisions en matière de technologie, et
- met en évidence les avantages de la mise à niveau des solutions de surveillance de sécurité existantes vers les solutions de surveillance de sécurité modernes.

Scénario de migration organisationnelle

Alice travaille en tant qu'analyste en sécurité dans une grande organisation qui s'appuie fortement sur le moteur d'inspection Snort pour superviser et protéger son infrastructure réseau. L'organisation utilise Snort version 2 depuis plusieurs années, mais elle a rencontré des limites et des défis.

Bob, l'administrateur réseau, envisage de migrer de Snort 2 à Snort 3 pour résoudre ces problèmes et améliorer les capacités de sécurité du réseau de son organisation.

Cette migration améliorera également la supervision de la sécurité du réseau, améliorera les performances et simplifiera la gestion des règles.

Bonnes pratiques pour la migration de Snort 2 à Snort 3

Suivez ces bonnes pratiques lors de la migration de Snort 2 vers Snort 3 pour assurer l'intégrité des données et maintenir la couverture de sécurité.

- Sauvegardez votre politique de prévention des intrusions avant d'effectuer la migration. Consultez la tâche Exporter les configurations dans le [Guide d'administration de Cisco Secure Firewall Management Center de Cisco Secure Firewall Management Center](#).
- Avant de mettre à niveau un périphérique vers Snort 3, si des modifications sont apportées dans Snort 2, utilisez l'utilitaire de synchronisation pour inclure la dernière synchronisation de Snort 2 à Snort 3 afin de pouvoir commencer avec une couverture similaire. Consultez [Synchroniser les règles de Snort 2 avec celles de Snort 3](#), à la page 34.
- Les règles personnalisées Snort 2 ne sont pas automatiquement converties en Snort 3 et doivent être migrées manuellement. Consultez [Convertir les règles IPS personnalisées de Snort 2 en Snort 3](#), à la page 31.
- La synchronisation ne migre pas les règles Snort 2 avec des seuils ou des suppressions. Ces règles doivent être créées à nouveau dans Snort 3.

Préalables pour la migration

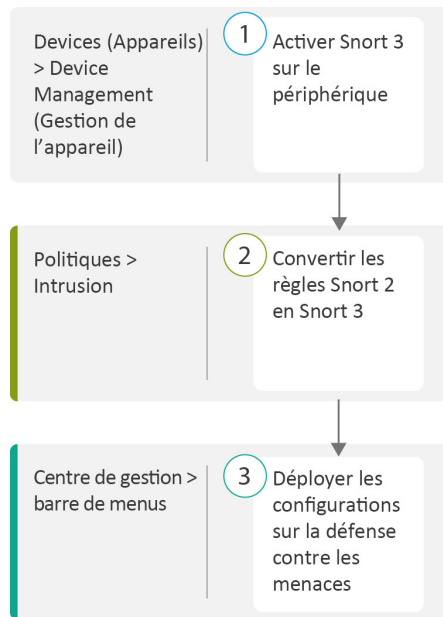
Remplissez ces conditions préalables avant de commencer le processus de migration pour assurer l'état de préparation du système et la protection des données.

- 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](#).

Flux de travail de migration de bout en bout

process_summary

Selon vos besoins, passez par les étapes énumérées dans le flux de travail pour terminer la migration de votre périphérique de Snort 2 vers Snort 3.

process_workflow

Voici les étapes de la migration de Snort 2 vers Snort 3 :

1. Activez Snort 3 sur le périphérique. Consultez [Activer Snort 3 sur le périphérique de protection contre les menaces, à la page 40](#).
2. Convertir les règles Snort 2 en Snort 3. Consultez [Convertir les règles Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 41](#).
3. Déployez la configuration. Consultez [Déploiement des modifications de configuration, à la page 36](#).

Activer Snort 3 sur le périphérique de protection contre les menaces

Activez Snort 3 sur votre périphérique de protection contre les menaces pour améliorer les capacités de sécurité.

Utilisez cette procédure pour effectuer une mise à niveau de Snort 2 à Snort 3 sur votre périphérique de protection contre les menaces.

**Attention**

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. |
| Étape 3 | Cliquez sur l'onglet Device (appareil). |
| Étape 4 | Dans la section Inspection Engine (Moteur d'inspection), cliquez sur Inspection Engine (Mise à niveau). |

Inspection Engine

Inspection Engine:

Snort 2

Before you upgrade, read and understand the Snort 3 configuration guide for your version: <https://www.cisco.com/go/fmc-snort3>. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed for minimal impact, features do not map exactly. Custom intrusion rules are not automatically migrated during upgrade but **options** are available to migrate. Careful planning and preparation can help you make sure that traffic is handled as expected.

Upgrading to Snort 3 also deploys configuration changes to affected devices. This briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. For details, see the [Snort Restart Traffic Behavior](#) section in the online help.

Upgrade to Snort3 should be done during a maintenance window.

Étape 5

Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez [Déploiement des modifications de configuration, à la page 36](#).

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 Snort 2 d'une politique de prévention des intrusions unique en Snort 3

Cette tâche synchronise et convertit les règles de politique de prévention des intrusions Snort 2 au format Snort 3, en veillant à ce que les règles personnalisées, les seuils et les suppressions soient correctement migrés pour maintenir l'efficacité de la politique de sécurité lors de l'utilisation des moteurs Snort 3.

Lorsque les politiques de prévention des intrusions affichent un indicateur de flèche orange, les versions Snort 2 et Snort 3 ne sont pas synchronisées. Le processus de synchronisation utilise l'outil snort2Lua pour convertir les règles et peut nécessiter une intervention manuelle pour les règles, les seuils et les suppressions personnalisés qui ne peuvent pas être migrés automatiquement.

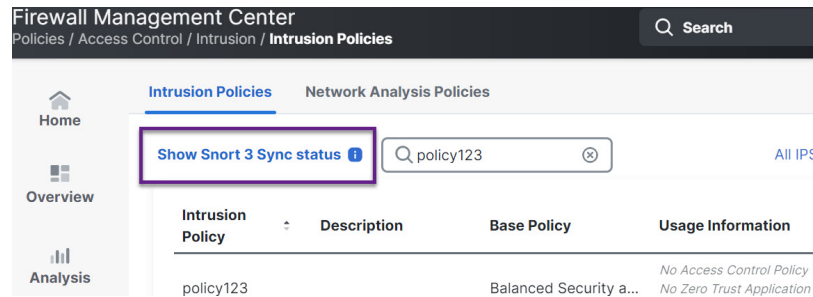
Before you begin

Suivez ces étapes pour convertir les règles Snort 2 d'une politique de prévention des intrusions unique en Snort 3 :

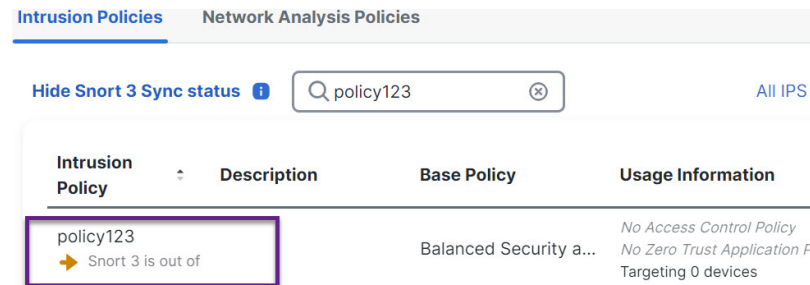
Procédure

Étape 1 Choisissez **Politiques (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Intrusion** > **Intrusion Policies (Politiques de prévention des intrusions)**.

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



Si votre politique affiche une flèche orange, cela indique que les versions Snort 2 et Snort 3 de la politique de prévention des intrusions ne sont pas synchronisées.



- b) Cliquez sur la flèche orange.

La page **Snort 2 to Snort 3 Sync Summary** (Résumé de la synchronisation Snort 2 to Snort 3) montre que la synchronisation de Snort 2 à Snort 3 est en attente.

Snort 2 to Snort 3 Sync Summary ?

This is a utility to synchronize Snort 2 policy configuration with Snort 3 version to start with a similar coverage.

- Snort 3 policy configuration is synced from Snort 2 version by the system when Firewall Management Center is upgraded from pre-7.0 version.
- Before upgrading a device to Snort 3, if changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with similar coverage.

Note: After moving to Snort 3, it is recommended that you manage the Snort 3 version of the policy independently and do not use this utility as a regular operation.

[Click here](#) to learn more.

Policy Name: policy123

➔ Snort 3 and Snort 2 Sync Pending 2025-01-10 03:49:25 EST

Used by: No Access Control Policy | No Device

Re-Sync

Close

- c) Cliquez sur **Re-Sync** (Resynchroniser) pour lancer la synchronisation.



Remarque

Lorsque vous cliquez sur **Re-Sync** (Resynchroniser), l'outil snort2Lua convertit les règles de Snort 2 en Snort 3.

La section **Summary Details** (Détails du résumé) répertorie les règles qui ont été migrées ou ignorées. Dans notre cas d'utilisation, il y a 76 règles Snort 2 personnalisées, 17 règles avec seuils et 15 règles avec suppression qui ont été ignorées pendant le processus de synchronisation. Pour migrer les règles personnalisées, passez à l'étape suivante.

Policy Name: _Intrusion_Policy_1

➔ Snort 3 is partially in sync with Snort 2. 2023-08-01 05:42:52 EDT

Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details

Rule Overrides

● Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.

▲ Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.

▲ Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

[Download Summary Details](#)

Overridden

Advanced

Custom Rules

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

Pour migrer des règles avec des seuils et des suppressions, passez à l'étape 6.

Policy Name: **_Intrusion_Policy_1**

➔ **Snort 3 is partially in sync with Snort 2.** 2023-08-01 05:42:52 EDT

Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details

Rule Overrides

● Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.

▲ Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.

▲ Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

[Download Summary Details](#)

Overridden

Advanced

Custom Rules

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

Étape 2

Pour migrer les 76 règles personnalisées, effectuez l'une des étapes suivantes :

- Dans l'onglet **Custom Rules** (Règles personnalisées), cliquez sur l'icône **Import** (Importer) pour convertir et charger automatiquement les règles locales dans la version Snort 3 de la politique.

Overridden

Advanced

Custom Rules

Convert the rules and auto-import them to the Snort 3 version of the policy 

OR

Download converted rules  You can upload the file after you have reviewed the converted rules 

Un message de confirmation s'affiche une fois les règles importées.

- Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)** et cliquez sur **Snort 3 All Rules** (Toutes les règles).
 1. Cliquez sur **Local Rules** (Règles locales) dans le volet de gauche pour vérifier si des règles ont été migrées. Remarquez qu'aucune règle personnalisée de Snort 2 n'a été migrée.
 2. Dans la liste déroulante **Tasks** (Tâches), choisissez **Convert Snort 2 rules and import** (Convertir les règles Snort 2 et les importer).

< Intrusion Policy

All Rules

> Local Rules(1 group)
> MITRE(1 group)
> Rule Categories(9 groups)

All Rules

All rules assigned to current intrusion policy

Rule Actions

1 ☒ | 51,056 rules

☐ **GID:SID**
☐ **Info**

> ☐ 133:3 (dce_smb)...

3. Cliquez sur **OK**.

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

All Rules

Local Rules (2 groups)
All Snort 2 Converted Global
_Intrusion_Policy_1_custom_rules

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions
Search by CVE, SID, Reference Info, or Rule Message
Tasks

49,218 rules

☐ **GID:SID**
☐ **Info**
☐ **Rule Action**
☐ **Assigned Groups**
☐ **Alert Configuration**

> ☐ 112:1 (arp_spoof) unicast ARP request Protocol/Builtins None

> ☐ 105:3 (back_office) Back Office server traffic detec... Protocol/Builtins None

The custom rules were successfully imported

Un groupe de règles nommé **All Snort 2 Converted Global** (Tous les éléments Snort 2 convertis - Global) est maintenant créé sous **Local Rules** (Règles locales) dans le volet de gauche.

Remarquez que les 76 règles personnalisées ont été migrées, comme le montre la figure suivante.

< Intrusion Policy

All Rules

Local Rules (2 groups)
All Snort 2 Converted Global
_Intrusion_Policy_1_custom_rules

Local Rules / _Intrusion_Policy_1_custom_rules

Description
Group created for custom rules enabled in snort 2 version

Rule Actions
Search by CVE, SID, Reference Info, or Rule Message
Tasks

76 rules

☐ **GID:SID**
☐ **Info**
☐ **Rule Action**
☐ **Assigned Groups**
☐ **Alert Configuration**

> ☐ 2000:1000143 http://mischa5xix2mrhd.onion/MZ2MMJ_2 All Snort 2 Converted... None

> ☐ 2000:1000139 CERT-In MALWARE THREAT EXCHANGE (CM... All Snort 2 Converted... None

The custom rules were successfully imported

Vous pouvez également sélectionner **Convert Snort 2 rules and download** (Convertir les règles Snort 2 et les télécharger) à l'étape précédente pour enregistrer le fichier de règles localement. Vous pouvez consulter les règles converties dans le fichier téléchargé, puis les charger ultérieurement à l'aide de l'option **Upload Snort 3 rules** (Charger les règles Snort 3).

Étape 3

Cliquez sur le lien **Download Summary Details** (Télécharger les détails du résumé) pour télécharger les règles au format .txt.

Il s'agit d'un exemple du résumé qui s'affiche.

Exemple :

```
"id": "00505691-15DC-0ed3-0000-004294988561",
"name": "_Intrusion_Policy_1",
"type": "IntrusionPolicy",
"syncStatus": {
  "source": {
    "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
    "type": "IntrusionPolicy"
  },
  "status": "WARN",
  "description": "Migration is partially successful. Some of the rules are not copied to
Snort3.",
  "timestamp": 1690883954814,
  "lastUser": {
    "name": "admin"
  },
  "details": [
    {
      "type": "Summary",
      "status": "INFO",
      "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides
migrated to 18635 Snort 3 rules."
    },
    {
      "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,

1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,

1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,

1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,

1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,

1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,

1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,

1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
      "type": "PolicyInfo",
      "description": "Corresponding Snort 2 policy overridden custom (local) rules."
    },
    {

```

```

    "type": "AssignedDevices",
    "status": "INFO",
    "description": "Snort3:0 , Snort2:0"
  },
  {
    "id": "122:6",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
  },
  {
    "id": "122:15",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_IP_PORTSWEEP_FILTERED"
  },
  {
    "id": "122:1",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_TCP_PORTSCAN"
  },
},

```

- Étape 4** Cliquez sur **Close** (Fermer) pour fermer la boîte de dialogue **Sync Summary** (Résumé de la synchronisation).
- Étape 5** Pour vérifier les règles ayant l'état : ERREUR, choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion** et cliquez sur la version **Snort 2** de la politique de prévention des intrusions.
- Étape 6** Sous **Policy Information** (Informations sur la politique), cliquez sur **Rules** (Règles) et filtrez la règle. Par exemple, saisissez **PSNG_TCP_PORTSCAN** dans le champ **Filter** (Filtre) pour trouver la règle.
- Étape 7** Cliquez sur **Show Details** (Afficher les détails) pour afficher la version détaillée de la règle.
- Étape 8** Créez à nouveau la règle dans Snort 3 en utilisant les directives de règle Snort 3 et enregistrez le fichier en tant que fichier .txt ou .rules. Pour en savoir plus, consultez www.snort3.org.
- Étape 9** Chargez la règle personnalisée que vous venez de créer localement dans la liste de toutes les règles Snort 3. Voir [Ajouter des règles personnalisées aux groupes de règles](#).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.



CHAPITRE 3

Stratégies de prévention des intrusions

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.

- [Politique de prévention des intrusions](#), à la page 49
- [Création d'une politique de prévention des intrusions Snort 3 personnalisée](#), à la page 51
- [Modification des politiques de prévention des intrusions Snort 3](#), à la page 52
- [Modifier la politique de base d'une politique de prévention des intrusions](#), à la page 58
- [Afficher le mappage de politique de base Snort 2 et Snort 3](#), à la page 59
- [Synchroniser les règles de Snort 2 avec celles de Snort 3](#), à la page 59
- [Gérer les politiques de prévention des intrusions](#), à la page 61
- [Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions](#), à la page 62
- [Régler les politiques de prévention des intrusions à l'aide de règles](#), à la page 64
- [Règles recommandées](#), à la page 85
- [Atténuer les menaces à l'aide du cadre MITRE dans les politiques de prévention des intrusions Snort 3](#), à la page 91

Politique de prévention des intrusions

Une *politique de prévention des intrusions* est un ensemble défini de configurations de détection et de prévention des intrusions qui

- inspecte le trafic pour détecter les violations de sécurité,
- peut bloquer ou modifier le trafic malveillant dans les déploiements en ligne, et
- sert de dernière ligne de défense du système avant que le trafic ne soit autorisé à se rendre à 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 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 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.

Par défaut, le système désactive l'inspection des charges utiles chiffrées. Cette valeur par défaut réduit les faux positifs et améliore les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès avec l'inspection de prévention des intrusions activée.

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](#).

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

Créez une politique de prévention des intrusions Snort 3 personnalisée pour adapter les paramètres de détection et de prévention des intrusions aux exigences de sécurité de votre réseau.

Les politiques de prévention des intrusions Snort 3 définissent la façon dont le système inspecte le trafic et répond aux menaces potentielles. Vous pouvez créer des politiques personnalisées en fonction des politiques existantes fournies par le système ou d'autres politiques personnalisées pour répondre à des besoins de sécurité spécifiques.

Before you begin

Suivez les étapes suivantes pour créer une politique de prévention des intrusions Snort 3 personnalisée :

Procédure

Étape 1 Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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 52.

Modification des politiques de prévention des intrusions Snort 3

Utilisez cette tâche pour comprendre comment accéder, modifier et gérer les politiques de prévention des intrusions Snort 3 dans le centre de gestion de pare-feu, y compris la modification des paramètres de politique, la gestion des groupes de règles et l'application de recommandations pour protéger votre réseau.

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

Before you begin

-

Procédure

- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.
- Étape 3** Cliquez sur **Versión Snort 3** à côté de la politique de prévention des intrusions que vous souhaitez configurer.
- Étape 4** Modifier votre politique
 - Change the mode (modifier le mode) : Cliquez sur le menu déroulant **Mode** pour modifier le mode d'inspection.



Mise en garde

Le mode d'inspection est modifié uniquement pour la version Snort 3 de la politique. Le mode d'inspection existant est conservé dans la version Snort 2 tel quel, ce qui signifie que vos versions Snort 2 et Snort 3 de la politique auront des modes d'inspection différents. Nous vous recommandons d'utiliser cette option avec prudence.

- **Prevention** (Prévention) : les règles de blocage déclenchées créent un événement (alerte) et abandonnent la connexion.
- **Detection** (Détection) : les règles de blocage déclenchées créent une alerte.

Vous pouvez choisir le mode de détection avant de choisir la prévention. Par exemple, avant de choisir le mode de prévention, vous pouvez souhaiter que les règles de blocage envoient uniquement des alertes, afin de vous permettre d'identifier les règles qui provoquent de nombreux faux positifs.

- Étape 5** Cliquez sur la couche **Politique de base** qui définit les paramètres par défaut de la politique de prévention des intrusions.
 - Search Rules (règles de recherche) : utilisez le champ de recherche pour filtrer l'affichage. Vous pouvez saisir le GID, la SID, le message de règle ou des informations de référence. Par exemple, GID:1; SID:9621 (pour afficher uniquement la règle 1:962, SID:9621,9622,9623) pour afficher plusieurs règles avec différents SID. Vous pouvez également cliquer dans la zone de texte Rechercher pour choisir l'une des options suivantes :
 - appliquez les filtres **Action = Alerte** ou **Actio : Block (Blocage)**.

- appliquer le filtre **Règles désactivées**
- afficher **les règles personnalisées/définies par l'utilisateur**
- filtrer par GID, SID ou GID:SIDf
- filtrer par CVE
- filtrer par commentaire
- View filtered Rules (afficher les règles filtrées) : cliquez sur l'un des paramètres **prédéfinis** pour afficher les règles qui sont définies pour alerter, bloquer, désactiver, etc.

Les règles remplacées indiquent les règles dans lesquelles l'action de règle a été remplacée par une action différente de l'action par défaut. Notez qu'une fois modifié, l'état de l'action découlant de la règle est Overridden même si vous lui rétablissez son action par défaut d'origine. Cependant, si vous sélectionnez **Revert to Default** (Revenir aux valeurs par défaut) dans la liste déroulante **Rule Action** (Actions de règles), l'état Overridden (Remplacé) est supprimé.

Les filtres avancés fournissent des options de filtre en fonction des versions du paquet de sécurité allégé (LSP), des classifications des intrusions et des vulnérabilités Microsoft.

- Afficher la documentation de la règle : cliquez sur l'ID de règle ou sur l'icône **Rule Documentation** (documentation de la règle) pour afficher la documentation Talos sur la règle.
- Afficher les détails d'une règle : cliquez sur l'icône **Flèche Développer** (➤) dans une ligne de règle pour afficher les détails de la règle.
- Ajouter des commentaires sur une règle : cliquez sur **Commentaires** (📝) dans la colonne Commentaires pour ajouter des commentaires concernant une règle.

Étape 6

Group Overrides (Remplacement de groupes) : cliquez sur la couche **Group Overrides** (Remplacement de groupes) qui répertorie toutes les catégories de groupes de règles. Le groupe de règles parent de niveau supérieur avec la description, les remplacements, les groupes activés et d'autres détails s'affiche. Les groupes de règles parents ne peuvent pas être mis à jour et sont en lecture seule. Seuls les groupes de règles feuille peuvent être mis à jour. Dans chaque groupe de règles, vous pouvez traverser jusqu'au dernier groupe feuille. Dans chaque groupe, vous pouvez remplacer, inclure et exclure des groupes de règles. Dans les groupes de règles feuille, vous pouvez :

- Search Rule Groups (rechercher des groupes de règles) : utilisez le champ de recherche pour saisir des mots-clés et rechercher des groupes de règles.
- Dans le panneau de gauche, vous pouvez choisir l'une des options de filtre prédéfinies pour rechercher des groupes de règles :
 - All (tout) : pour afficher tous les groupes de règles.
 - Excluded (Exclus) : pour les groupes exclus.
 - Included (Inclus) : pour les groupes inclus.
 - Overridden (Remplacé) : pour la configuration de groupe de règles qui est remplacée.
- Définir le niveau de sécurité d'un groupe de règles : accédez au groupe de règles requis dans le volet de gauche et cliquez dessus. Cliquez sur **Modifier** à côté du **niveau de sécurité** du groupe de règles pour augmenter ou diminuer le niveau de sécurité en fonction des paramètres de règle définis par le système.

Dans la boîte de dialogue **Edit Security Level** (Modifier le niveau de sécurité), vous avez la possibilité de cliquer sur **Revert to Default** (Revenir au niveau par défaut) pour rétablir les modifications que vous avez effectuées.

Firewall Management Center modifie automatiquement l'action pour les règles du groupe de règles en fonction du niveau de sécurité configuré. Dans la couche **Rule Overrides** (Remplacements de règles), notez le nombre de règles Block (blocage) et de règles Disabled (désactivées) dans les **présélections** chaque fois que vous modifiez le niveau de sécurité.

- Vous pouvez apporter des modifications en bloc au niveau de sécurité pour modifier le niveau de sécurité de tous les groupes de règles d'une catégorie de règles particulière. Le niveau de sécurité en bloc s'applique aux groupes de règles qui ont plusieurs groupes de règles. Après une mise à jour en bloc de groupes de règles, vous pouvez toujours mettre à jour le niveau de sécurité de n'importe quel groupe de règles qui y est associé.

Il peut y avoir des niveaux de sécurité **mixtes** au sein des groupes de règles; **mixte** indique que les groupes enfants contiennent un mélange de niveaux de sécurité au sein du groupe de règles parent.

- Inclure ou exclure des groupes de règles : les groupes de règles affichés sont les groupes de règles par défaut associés à la politique de base de prévention des intrusions fournie par le système. Vous pouvez inclure et exclure des groupes de règles de la politique de prévention des intrusions. Un groupe de règles exclu est supprimé de la politique de prévention des intrusions et ses règles ne sont pas appliquées au trafic. Pour en savoir plus sur le chargement de règles personnalisées dans Firewall Management Center, consultez [Ajouter des règles personnalisées aux groupes de règles, à la page 81](#).

Pour exclure un groupe de règles :

1. Naviguez dans le volet Rule Groups (Groupes de règles) et choisissez le groupe de règles que vous souhaitez exclure.
2. Cliquez sur le lien hypertexte **Exclude** dans le volet droit.
3. Cliquez sur **Exclude** (Exclure).

Pour inclure un nouveau groupe de règles ou plusieurs groupes de règles avec les règles personnalisées chargées ou un groupe de règles précédemment exclus :

1. Cliquez sur **Ajouter** (+) à côté de la liste déroulante du filtre de groupes de règles.
 2. Choisissez tous les groupes de règles que vous souhaitez ajouter en cochant la case à côté de ceux-ci.
 3. Cliquez sur **Save** (Enregistrer).
- Pour un groupe de règles enfant, cliquez sur l'icône sous l'en-tête de colonne **Override** (Remplacer) pour voir le journal d'actions de la règle, qui décrit la séquence d'actions de remplacement de règle qui peuvent être affectées en raison de remplacements de politique et de groupe de base pour une règle de prévention des intrusions. Les actions liées aux règles peuvent être obtenues à partir des configurations de politiques de base ou du remplacement de groupe d'utilisateurs. Le remplacement de groupe d'utilisateurs a la priorité entre les deux; La priorité fait référence à l'action finale remplacée qui est affectée au groupe de règles.
 - Cliquez sur le nombre de règles (nombre) sous l'en-tête de colonne **Nombre de règles** pour afficher un résumé des règles qui font partie du groupe de règles.

Étape 7 **Recommendations** (Recommandations) : cliquez sur la couche **Recommendations** (Recommandations) si vous souhaitez générer et appliquer les règles recommandées par Cisco. Les recommandations utilisent la base de données hôte pour activer ou désactiver les règles, en fonction des vulnérabilités connues.

Étape 8 **Rule Overrides** (Remplacements de règles) : cliquez sur la couche **Rule Overrides** (Remplacements de règles) pour choisir l'un des préréglages afin d'afficher les règles, qui sont définies comme suit : alerter, bloquer, désactiver, remplacer, réécrire, transmettre, abandonner ou rejeter.

- La colonne **Définir par** indique l'état défini par défaut (politique de base) ou l'état de règle modifié par les remplacements de groupe, les remplacements de règles ou les recommandations. La colonne **Set By** dans **All Rules** (Définir par dans Toutes les règles) (dans le volet gauche) affiche le suivi des actions de remplacement des règles en fonction de l'ordre de priorité. L'ordre de priorité des actions liées aux règles est Remplacement de la règle > Recommendations > Remplacement de groupe > Politique de base.
- Modifier **Rule Action** (Action de règle) : pour modifier des actions de règles, choisissez l'une des options suivantes :
 - Modification en bloc : choisissez une ou plusieurs règles, puis choisissez l'action requise dans la liste déroulante **Rule Action** (Action de règle); puis cliquez sur **Save** (Enregistrer).



Remarque

Les modifications en bloc d'actions de règle sont prises en charge uniquement pour les 500 premières règles.

- Single Rule Edit (modification d'une règle unique) : choisissez l'action pour la règle dans la liste déroulante de la colonne **Rule Action** (Actions de règle).

Les actions découlant d'une règle sont :

- **Block** (Blocage) : génère un événement, bloque le paquet correspondant actuel et tous les paquets suivants dans cette connexion.
- **Alert** (Alerte) : génère uniquement un événement pour le paquet correspondant, sans abandonner le paquet ni la connexion.
- **Disable** (Désactiver) : ne correspond pas au trafic avec cette règle. Aucun événement n'est généré.
- **Revert to default** (Revenir aux valeurs par défaut) : restaure l'action par défaut du système.
- **Pass** (Réussite) : aucun événement généré, ce qui permet au paquet de passer sans évaluation supplémentaire par les règles Snort suivantes.



Remarque

L'action Pass est disponible uniquement pour les règles personnalisées et non pour les règles fournies par le système.

- **Drop** (Abandonner) : génère un événement, abandonne le paquet correspondant et ne bloque pas le trafic additionnel dans cette connexion.
- **Reject** : génère un événement, abandonne le paquet correspondant, bloque le trafic additionnel dans cette connexion et envoie les messages réinitialisation TCP ou port ICMP inaccessible aux hôtes source et de destination.

Behavior of reject in different firewall modes and IP address or source or destination in relation to Client or Server (Comportement de rejet dans différents modes de pare-feu et adresse IP, ou source ou destination par rapport au client ou au serveur) : Snort envoie des paquets RST au client et au serveur dans le cas d'interfaces routées, en ligne et pontées. Snort envoie deux paquets RST. Le paquet RST dans la direction du client aura la source définie sur l'adresse IP du serveur et la destination définie sur l'adresse IP du client. Le paquet RST dans la direction du serveur aura la source définie sur l'adresse IP du client et la destination définie sur l'adresse IP du serveur.

- **Rewrite** (Réécrire) : génère des événements et remplace le contenu des paquets en fonction de l'option de remplacement dans la règle.

Pour la journalisation des actions liées aux règles IPS, consultez [Journalisation des actions liées aux règles, à la page 57](#).

S'il y a une règle **React** (Réagir), elle est convertie en action d'alerte.

Étape 9

Cliquez sur la couche **Summary** (résumé) pour obtenir une vue globale des modifications actuelles apportées à la politique. La page de résumé de la politique contient les informations suivantes :

- Répartition des règles de la politique, c'est-à-dire les règles actives, les règles désactivées, etc.
- Option d'exportation de la politique et de génération d'un rapport sur la politique de prévention des intrusions.
- Renseignements sur la politique de base.
- Générer des recommandations
- Les remplacements de groupe répertorient les groupes que vous avez remplacés.
- Remplacements de règles qui affiche la liste des règles que vous avez remplacées.
- Dans la couche **Summary** (Résumé), cliquez sur l'icône ? pour ouvrir une fenêtre contextuelle qui explique les concepts de superposition de Snort.

Pour modifier la politique de base, consultez [Modifier la politique de base d'une politique de prévention des intrusions, à la page 58](#).



Remarque

Vous pouvez accéder à **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**, puis cliquer sur l'onglet **Snort 3 Toutes les règles** et parcourir tous les groupes de règles d'intrusion. Le groupe de règles parent répertorie les groupes enfants associés et le nombre de règles.

Prochaine étape

Déployer les modifications de configuration. Voir [Déploiement des modifications de configuration, à la page 36](#).

Rapport de groupe de règles

Le rapport de groupe de règles est une fonction d'analyse de sécurité qui

- reflète les groupes de règles dans les incidents d'intrusion générés,
- comprend l'identification des tactiques et techniques MITRE, et
- fournit des colonnes dédiées pour les groupes de règles MITRE et non-MITRE dans les affichages des incidents d'intrusion.

Accès au rapport de groupe de règles et champs

Pour accéder aux incidents d'intrusion, dans Firewall Management Center, rendez-vous à **Analysis (Analyse) > Intrusions > Events (Événements)**, et cliquez sur l'onglet **Table View of Events** (Tableau des événements). Vous pouvez également afficher les champs d'incident d'intrusion dans la visionneuse d'**événements unifiés**. Dans l'onglet **Analysis** (analyse), cliquez sur **Unified Events** (événements unifiés).

Dans la page **Intrusion Events** (Incidents d'intrusion), les champs suivants sont ajoutés pour les rapports sur les groupes de règles. Notez que vous devez activer explicitement les colonnes mentionnées.

- MITRE ATT&CK
- Groupe de règles

Pour en savoir plus sur ces champs, consultez la section *Champs d'incidents d'intrusion* dans le *Guide d'administration de Cisco Secure Firewall Management Center, version 7.3*.

Journalisation des actions liées aux règles

À partir de la version Firewall Management Center 7.2.0, sur la page **Intrusion Events** (Incidents 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, les tableaux présentent les événements affichés dans la colonne **Inline Result** (Résultat en ligne) de la fenêtre **Intrusion Events** (Événements d'intrusion) et dans la colonne **Action** pour **Intrusion Event Type** (Type d'incident d'intrusion) dans la fenêtre **Unified Events** (Événements unifiés).

Action IPS pour Snort 3	Résultat en ligne : Firewall Management Center 7.1.0 ou versions antérieures	Résultat en ligne : Firewall Management Center 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 « **Would Rewrite** » (Réécrivait).
- L'action **Rewrite** (Réécriture) est également affichée comme **Would Rewrite** (Réécrivait) si l'option Replace (Remplacer) est spécifiée, mais que la politique IPS est en mode Detection (Détection) ou que le périphérique est en mode Inline-TAP (TAP en ligne) ou Passive (Passif).

**Remarque**

En cas de compatibilité ascendante (Firewall Management Center 7.2.0 assurant la gestion d'un périphérique Firewall 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 Firewall Management Center 7.1.0 s'appliquent.

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

Modifiez la politique de base pour utiliser une autre politique fournie par le système ou personnalisée comme base pour la configuration de votre 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 **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#), à la page 36.

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

Cette tâche vous permet d'afficher le mappage entre les politiques de prévention des intrusions Snort 3 et Snort 2.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Procédure

- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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

Cette tâche permet de s'assurer que les paramètres de remplacement de règles Snort 2 et les règles personnalisées sont répliqués sur Snort 3, vous permettant de commencer avec une couverture similaire lors de la transition entre les versions.

Pour s'assurer que les paramètres et les règles personnalisées de la version Snort 2 sont conservés et transférés dans Snort 3, Firewall Management Center 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.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Si Firewall Management Center 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 Firewall Management Center. 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**

Lorsque vous passez à Snort 3, gérez la version Snort 3 de la politique de manière indépendante. N'utilisez pas cet utilitaire comme une opération normale.

**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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Assurez-vous que l'onglet **Intrusion Politiques** (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 bleue **Versions Snort synchronisées** (→).

- Étape 6** Lisez le résumé. Téléchargez une copie du résumé, au besoin.
- 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 Custom Rules (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 32.

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Gérer les politiques de prévention des intrusions

Cette tâche vous permet d'effectuer des opérations de gestion complètes sur vos politiques de prévention des intrusions, notamment la création, la modification, la suppression, l'exportation, le déploiement et la création de rapports.

Sur la page Intrusion Policy (politique de prévention des intrusions) (**Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**), vous pouvez afficher vos politiques de prévention des intrusions personnalisées actuelles, ainsi que les informations suivantes :

- le nombre de stratégies de contrôle d'accès et de périphériques utilisant la politique de prévention des intrusions pour inspecter le trafic.
- Indique le domaine dans lequel la politique a été créée.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

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 **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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 51](#).
- **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 52](#).
- **Exporter** : si vous souhaitez exporter une politique de prévention des intrusions pour l'importer sur un autre Firewall Management Center, 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 [Déploiement des modifications de configuration, à la page 36](#).
- **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 configuration de règles de contrôle d'accès pour effectuer la prévention des intrusions est un mécanisme de sécurité qui

- permet à plusieurs règles de contrôle d'accès dans une stratégie de contrôle d'accès d'être associées aux politiques de prévention des intrusions,
- permet l'inspection de prévention des intrusions pour les règles de contrôle d'accès Allow (autoriser) ou Interactive (bloquer interactif) afin de faire correspondre différents profils d'inspection de prévention des intrusions à différents types de trafic, et
- évalue le trafic avant qu'il n'atteigne sa destination finale sur le réseau.

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.

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

Configurez une règle de contrôle d'accès pour activer l'inspection de prévention des intrusions sur le trafic réseau, afin de détecter et de prévenir les activités malveillantes en fonction des signatures et des politiques de prévention des intrusions.

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

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

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

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#), à la page 36.

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

Cette section 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.

Réglage des règles de prévention des intrusions

Le réglage des règles de prévention des intrusions est un processus de configuration qui

- active la modification de l'état des règles pour les règles d'objets partagés, les règles de texte standard et les règles d'inspection,
- contrôle la génération d'incidents et le traitement du trafic en fonction de la configuration des règles, et
- permet le filtrage des règles afin d'afficher des sous-ensembles précis pour les modifications de configuration ciblées.

Configuration de l'état des règles

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 argument 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.

Types de 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.

- *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.

Attributs et caractéristiques du type de règle

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

Tableau 2 : Types de 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 1,000,000	Cisco Talos Intelligence Group (Talos)	oui	limité
Règle de texte standard	1 (Domaine global ou GID existant)	inférieur à 1,000,000	Talos	oui	limité
	1 000-2 000 (domaine descendant)	1,000,000 ou plus	Créé ou importé par l'utilisateur	Oui	oui
règle de préprocesseur	propre au décodeur ou au préprocesseur	inférieur à 1,000,000	Talos	Non	Non
		1,000,000 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.

Règles personnalisées dans Snort 3

Une règle personnalisée dans Snort 3 est une règle de détection d'intrusion qui

- permet aux utilisateurs de créer une détection personnalisée des menaces en important des fichiers de règles locaux avec les extensions `.txt` ou `.rules`,
- appartient à des groupes de règles et peut être inclus dans plusieurs groupes simultanément, et
- reçoit un numéro de règle unique au format `GID:SID:Rev` avec des identifiants générés par le système.

Format du numéro de règle

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 1,000,000 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.
- Le *classtype* dans une règle Snort attribue une classification à la règle indiquant le type d'attaque associé à un événement. Un niveau de priorité de 1 à 4 est également associé à chaque *classtype*. Cependant, le niveau de priorité de certains *classtypes* sur l'appareil de protection contre les menaces ne correspond pas aux niveaux de priorité de *classtypes* Snort à code source libre qui sont mentionnés dans la [documentation](#) Snort. Par exemple, *tcp-connection* a une priorité de 4 dans Snort à code source libre, tandis qu'une priorité de 3 lui est attribuée sur l'appareil de protection contre les menaces.

Détection de données sensibles

Des données sensibles telles que les numéros de sécurité sociale, les numéros de carte de crédit, les courriels, etc. peuvent être divulgués sur Internet, intentionnellement ou accidentellement. La détection des données sensibles est utilisée pour détecter et générer des événements relatifs à d'éventuelles fuites de données sensibles. Les incidents sont générés uniquement en cas de transfert d'une quantité importante de renseignements personnels identifiables. La détection des données sensibles peut masquer les renseignements nominatifs dans la sortie des événements.

Utilisez l'option d'IPS `sd_pattern` pour détecter et filtrer les renseignements nominatifs. Ces renseignements comprennent les numéros de cartes de crédit, les numéros de sécurité sociale aux États-Unis, les numéros de téléphone et les adresses de courriel. La syntaxe d'une expression régulière (regex) est disponible pour définir vos propres renseignements nominatifs.

L'option `sd_pattern` a les paramètres suivants :

- **Modèle** : paramètre implicite obligatoire qui spécifie l'expression régulière à rechercher dans la PDU. L'expression régulière doit être écrite en syntaxe PCRE.
- **Seuil** : paramètre explicite et facultatif qui spécifie le nombre de correspondances dans la PDU requises pour générer un événement.

L'option de règle `sd_pattern` comme IPS est disponible dans Snort sans exigence pour des inspecteurs supplémentaires. La syntaxe de l'option de règle est la suivante :

```
sd_pattern: "<pattern>"[, threshold <count>];
```

Par exemple :

```
sd_pattern:"credit_card", threshold 2;
```

Il existe cinq modèles intégrés pour les données sensibles. Pour utiliser les schémas intégrés dans le paramètre « pattern », vous devez préciser le nom du type de renseignements nominatifs qui doivent être mis en correspondance, et l'expression régulière nécessaire lui est remplacée. Le nom des renseignements nominatifs et les mappages ou modèles d'expression régulière sont décrits comme suit :

Tableau 3 : Schémas intégrés

Nom des renseignements nominatifs	Schéma
credit_card	<code>\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}</code>
us_social	<code>[0-8]\d{2}-\d{2}-\d{4}</code>
us_social_nodashes	<code>[0-8]\d{8}</code>
Courriel	<code>[a-zA-Z0-9!#\$%&'*/=\?^_`{ }~]+(?:\. [a-zA-Z0-9!#\$%&'*/=\?^_`{ }~]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?</code>
us_phone	<code>(?:\+?1[-.\s]?)?(?:([2-9][0-8]\d)\s?[-.\s]([2-9]\d{2})[-.\s]\d{4})</code>

Le masquage pour les données correspondant à ces schémas ne fonctionne qu'avec les règles fournies par le système ou les schémas intégrés pour les cartes de crédit, les numéros de sécurité sociale américains, les adresses courriel et les numéros de téléphone aux États-Unis. Le masquage ne fonctionne pas pour les règles personnalisées ou les schémas de renseignements nominatifs définis par l'utilisateur. Les règles sont disponibles dans le paquet de sécurité allégé (LSP) pour les données sensibles, gid:13. Par défaut, ils ne sont activés dans aucune politique fournie par le système.

Les règles de données sensibles dans LSP couvrent tous les modèles intégrés et ont les valeurs de seuil suivantes :

- credit_card: 2
- us_social: 2
- us_social_nodashes: 20
- email: 20
- us_phone: 20

Vous pouvez utiliser l'option `sd_pattern` pour créer des règles personnalisées et modifier les règles existantes. Pour ce faire, utilisez l'interface de politique de prévention des intrusions Snort 3.

Exemple de règle avec `sd_pattern` avec un modèle et un seuil personnalisés :

```
alert tcp (sid: 1000000001; sd_pattern:"[lw-]+@[lw-]+\.[lw-]{2,4}",threshold 4; msg: "email, threshold 4")
```

Exemples

Exemple de règles personnalisées utilisant la détection des données sensibles :

Règle avec modèle intégré

```
alert tcp (
  msg:"SENSITIVE-DATA Email";
  flow:only_stream;
  pkt_data;
  sd_pattern:"email", threshold 5;
  service:http, smtp, ftp-data, imap, pop3;
  gid:2000;
  sid:1000001;
)
```

Règle avec modèle personnalisé

```

alert tcp (
  msg:"SENSITIVE-DATA US phone numbers";
  flow:only_stream;
  file_data;
  sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
2;

  service:http, smtp, ftp-data, imap, pop3;
  gid:2000;
  sid:1000002;
)

```

Voici quelques autres exemples de règles IPS Snort complètes avec des schémas de données sensibles intégrés :

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"crédit_card", seuil 2;)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2;)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2;)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2;)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email", threshold 2;)

La désactivation du masquage des données n'est pas prise en charge dans Cisco Secure Firewall Management Center et Cisco Secure Firewall Device Manager.

Pour en savoir plus sur l'ajout de règles personnalisées aux groupes de règles, consultez [Ajouter des règles personnalisées aux groupes de règles, à la page 81](#).

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

Cette tâche vous permet d'afficher et d'interagir avec les règles de prévention des intrusions Snort 3 dans une politique de prévention des intrusions, vous permettant de gérer les paramètres d'affichage des règles et d'accéder aux informations détaillées sur les règles.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion . |
| Étape 2 | Cliquez sur Version Snort 3 à côté de la politique. |
| Étape 3 | Lors de l'affichage des règles, vous pouvez : <ul style="list-style-type: none"> • 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 52 pour en savoir plus sur l'exécution de ces tâches.

Actions des règles de prévention des intrusions

Une action de règle de prévention des intrusions est un mécanisme de configuration de politiques qui

- active ou désactive les règles dans les politiques de prévention des intrusions individuelles,
- spécifie l'action entreprise par le système si les conditions surveillées déclenchent la règle, et
- hérite des actions par défaut de la politique de base utilisée lors de la création de la politique de prévention des intrusions.

Comportement de l'action par défaut

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 à des valeurs spécifiques qui déterminent la manière dont le système répond au trafic correspondant.

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

Définissez des actions de règles de prévention des intrusions pour contrôler la façon dont le système répond aux menaces détectées, vous permettant de configurer des règles pour alerter ou bloquer des tentatives d'intrusion spécifiques.

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

Procédure

Étape 1 Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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 52](#) pour plus d'informations sur les différentes actions de règle.

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

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration, à la page 36](#).

Filtres de notification d'incident d'intrusion dans une politique de prévention des intrusions

Un filtre de notification d'incident d'intrusion dans une politique de prévention des intrusions est un mécanisme de sécurité qui

- détermine l'importance d'un événement en fonction de la fréquence d'occurrence ou des adresses IP source et de destination,
- permet aux administrateurs de préciser des seuils pour le moment où les événements nécessitent votre attention, et
- empêche le système de se submerger en limitant les notifications pour les attaques généralisées.

Scénarios de filtrage des notifications d'événement

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. Votre système est dépassé lorsqu'il reçoit des centaines du même événement.

Seuils d'incidents d'intrusion

Le seuil d'incident d'intrusion est un paramètre de configuration qui

- limite 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,
- vous évite d'être submergé par un grand nombre d'événements identiques.
- peut être défini 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 4 : 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.

Option	Description
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 Typesur Both (Les deux), Count (Nombre) sur deux et Seconds (Secondes) sur 10, vous obtenez le nombre d'événements suivant : • 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 5 : 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 6 : 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.

Vous pouvez utiliser le seuillage des incidents d'intrusion seul ou le combiner avec la prévention des attaques basée sur le débit, le mot-clé `detection_filter` ou 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

Définissez un seuil pour qu'une règle de prévention des intrusions contrôle le moment et la fréquence de génération des alertes en fonction des instances d'événement au cours d'une période spécifiée.

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. Vous pourriez voir plus d'alertes sur différents flux de réseau, mais vous ne verrez pas moins d'alertes que le nombre configuré.

Procédure

-
- | | |
|-----------------|--|
| Étape 1 | Choisissez Objects (Objets) > Intrusion Rules (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 : <ul style="list-style-type: none"> • 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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#).

Afficher et supprimer les seuils d'incidents d'intrusion

Cette tâche vous permet d'afficher les paramètres de seuil existants pour les règles de prévention des intrusions et de les supprimer lorsqu'ils ne sont plus appropriés pour la configuration de votre système.

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 Objects (Objets) > Intrusion Rules (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Configuration de la suppression des politiques de prévention des intrusions

La configuration de suppression des politiques de prévention des intrusions est un mécanisme de sécurité qui

- supprime la notification d'incidents d'intrusion lorsqu'une adresse IP spécifique ou une plage d'adresses IP déclenche une règle ou un préprocesseur spécifique,
- élimine les faux positifs en permettant aux règles de se déclencher pour tous les paquets tout en n'affichant que les incidents pour les attaques légitimes, et
- est utile dans des scénarios tels que les serveurs de messagerie qui transmettent des paquets simulant des exploits spécifiques.

Exemple de suppression de serveur de messagerie

Si vous avez un serveur de messagerie qui transmet des paquets qui semblent être une exploitation spécifique, vous pouvez supprimer la notification d'incident pour cet incident 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 **Configuration d'alerte** de la page de l'éditeur de règles de prévention des intrusions **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)**, cliquez sur **Snort 3 toutes les règles**.

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

Cette tâche vous permet de configurer une ou plusieurs suppressions pour une règle de votre politique de prévention des intrusions afin de réduire les faux positifs et de vous concentrer sur les incidents de sécurité pertinents.

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

Before you begin

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

Suivez ces étapes pour définir la suppression pour une règle de prévention des intrusions dans Snort 3

Procédure

- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (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 **None** (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**, cliquez sur l'icône **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 étapes 5, 6 et 7, si nécessaire.

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

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Afficher et supprimer les conditions de suppression

Affichez ou supprimez les conditions de suppression existantes pour gérer les notifications d'événement pour des conditions de réseau spécifiques.

Vous souhaitez 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 **Objects (Objets) > Intrusion Rules (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Ajouter des commentaires sur les règles de prévention des intrusions

Ajoutez des commentaires aux règles de votre politique de prévention des intrusions à des fins de documentation et de gestion.

Vous pouvez ajouter des commentaires aux règles de votre politique de prévention des intrusions. Les commentaires ajoutés de cette manière sont spécifiques à la politique. 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 **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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).

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

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Préparer des règles personnalisées pour la conversion de SNORT 3

Avant de passer de Snort 2 à Snort 3, assurez-vous que vous êtes prêt à gérer votre ensemble de règles personnalisées pour 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.

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.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

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

Convertissez les règles personnalisées Snort 2 existantes au format Snort 3 mis à jour pour assurer la compatibilité avec les systèmes de détection d'intrusion actuels.

Cette tâche migre les règles personnalisées Snort 2 existantes vers le format Snort 3, vous permettant de conserver vos configurations de règles personnalisées lors de la mise à niveau vers le dernier moteur de détection d'intrusion. Vous pouvez soit importer les règles converties directement, soit les télécharger pour les consulter avant de les importer.

Procédure

- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (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 Firewall Management Center 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 81](#).

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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

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

Convertissez les règles personnalisées Snort 2 dans une politique de prévention des intrusions au format Snort 3 pour maintenir la compatibilité avec les environnements Snort 3.

Lors de la migration vers Snort 3, les règles personnalisées Snort 2 existantes doivent être converties pour conserver leurs fonctionnalités. Cette tâche vous permet de convertir des règles personnalisées pour une politique de prévention des intrusions spécifique.

Procédure

- Étape 1** Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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 bleue **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 **Custom Rules** (Règles personnalisées).
- Étape 5** Choisissez :
- **Import converted rules to this policy** (Importer les règles converties dans cette politique) : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans Firewall Management Center en tant que règles personnalisées Snort 3.
 - **Download converted rules** (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Ajouter des règles personnalisées aux groupes de règles

Chargez des règles personnalisées pour ajouter des règles Snort 3 créées localement à la liste de toutes les règles disponibles dans le système.

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

Procédure

- | | |
|----------------|--|
| Étape 1 | Choisissez Objects (Objets) > Intrusion Rules (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 <code>.txt</code> ou <code>.rules</code> 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** Choisissez l'une des options 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**

Toutes les règles chargées sont désactivées par défaut. Modifiez leur état au besoin pour vous assurer que les règles sont actives.

Prochaine étape

- Le téléversement de règles personnalisées dans le Firewall Management Center 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 82](#). Pour en savoir plus sur l'activation des règles personnalisées, consultez [Gérer les règles personnalisées dans Snort 3, à la page 83](#).
- Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration, à la page 36](#).

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

Activez les règles personnalisées dans une politique de prévention des intrusions pour appliquer ces règles au trafic réseau.

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 Firewall Management Center, ajoutez le groupe de règles avec les nouvelles règles personnalisées dans la politique de prévention des intrusions.

Procédure**Étape 1**

Choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#), à la page 36.

Gérer les règles personnalisées dans Snort 3

Cette tâche permet aux règles personnalisées chargées dans les politiques de prévention des intrusions d'appliquer la surveillance des règles au trafic réseau.

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.

Before you begin

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

Procédure

- Étape 1** Choisissez **Objects (Objets) > Intrusion Rules (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

Déployer les modifications de configuration Consultez [Déploiement des modifications de configuration](#), à la page 36.

Supprimer des règles personnalisées

Supprimez les règles personnalisées qui ne sont plus nécessaires de votre configuration de règles de prévention des intrusions pour maintenir un ensemble de règles ordonné et efficace.

Utilisez cette procédure lorsque vous devez supprimer des règles personnalisées de la section Local Rules (règles locales) dans l'interface Snort 3 All Rules. Avant la suppression, toutes les règles doivent être désactivées pour éviter les conflits de configuration.

Procédure

Étape 1 Choisissez **Objects (Objets) > Intrusion Rules (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 ces étapes pour désactiver l'action de règle pour plusieurs règles sélectionnées :

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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Supprimer les groupes de règles

Supprimez des groupes de règles pour supprimer les règles de détection d'intrusion indésirables ou obsolètes de la configuration de votre système et maintenir une structure de règles ordonnée.

Avant de supprimer un groupe de règles, vous devez l'exclure de toutes les politiques de prévention des intrusions et désactiver toutes les règles du groupe pour éviter les conflits de système.

Before you begin

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 52](#).

Suivez les étapes suivantes pour supprimer les groupes de règles :

Procédure

-
- | | |
|----------------|---|
| Étape 1 | Choisissez Objects (Objets) > Intrusion Rules (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 :
<ul style="list-style-type: none"> 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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration, à la page 36](#).

Règles recommandées

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

Les modifications de règles Snort 3 dans les mises à jour de LSP sont des modifications des règles de prévention des intrusions définies par le système qui

- remplacent les règles existantes par de nouvelles règles pour améliorer les capacités de détection,
- combinent plusieurs règles en une seule règle ou développent une seule règle en plusieurs règles lorsqu'une meilleure détection est possible, et
- suppriment les règles existantes définies par le système pour une meilleure gestion 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 **Conservez les dérogations s'appliquant aux utilisateurs pour les règles supprimées dans Snort 3**, cliquez sur **Système** (⚙️) > **Configuration** > **Intrusion Policy Preferences** (**Préférences pour les politiques de prévention des intrusions**).

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** (⚙️).

Règles conseillées pour Secure Firewall

Les règles recommandées pour Secure Firewall sont des recommandations de règles d'intrusion qui

- ciblent les vulnérabilités associées aux ressources hôtes détectées dans le réseau, telles que les systèmes d'exploitation, les serveurs et les protocoles d'application client,
- vous permettent d'adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé, et
- fournissent des recommandations individuelles pour chaque politique de prévention des intrusions. Elles s'appliquent généralement aux règles de texte standard et aux règles d'objet partagé, mais les recommandations peuvent également inclure des règles d'inspection et de décodeur.

Options de configuration de la recommandation de règle

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 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.

Générer de nouvelles recommandations Secure Firewall dans Snort 3

Générez les recommandations Secure Firewall pour créer de nouveaux paramètres de règle recommandés 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 **security levels** (niveaux de sécurité) basés sur les politiques de seuil que vous avez sélectionnées dans Snort 3. L'action conseillée dépend du niveau de sécurité sélectionné. S'il est supérieur à la politique de base, la recommandation comprend des actions au-delà de la génération d'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 immédiatement supérieur et désélectionnez l'option permettant de désactiver les règles.
- Définissez les recommandations au niveau de sécurité immédiatement supérieur et sélectionnez l'option permettant de désactiver les règles.
- Définissez les recommandations au niveau de sécurité actuel et sélectionnez l'option permettant de désactiver les règles.

Before you begin

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

Suivez ces étapes pour générer de nouvelles recommandations Secure Firewall dans Snort 3

Procédure

Étape 1 Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > 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. Cliquez sur **Start (Démarrer)**.

Dans la fenêtre Recommandations de règles de 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 de 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 et choisir de les appliquer.

- **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 Recommandations, 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, Firewall Management Center 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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Atténuer les menaces à l'aide du cadre MITRE dans les politiques de prévention des intrusions Snort 3

Cette section décrit comment utiliser le cadre MITRE ATT&CK dans les politiques de prévention des intrusions Snort 3 pour identifier les stratégies et les techniques d'attaque, passer en revue la couverture des règles et améliorer la réduction des menaces.

cadre MITRE

Le cadre MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) est une base de connaissance complète qui

- fournit des observations sur les tactiques, les techniques et les procédures (TTP) distribuées par les groupes de menaces ciblant les systèmes,
- intègre des groupes pour faire référence à des groupes de menaces, des groupes d'activités ou des actions de menace en fonction de l'ensemble de stratégies et de techniques qu'ils utilisent, et
- est compilé sous forme de matrices, chaque matrice représentant un système d'exploitation ou une plateforme particulière.

Chaque technique comprend des renseignements sur l'exécution, les procédures, les défenses, les détections et des exemples du monde réel.



Remarque

Consultez le site <https://attack.MITRE.org> pour obtenir des renseignements supplémentaires sur MITRE ATT&CK.

Le centre de gestion utilise le cadre MITRE ATT&CK pour améliorer la détection et la réponse aux menaces, en incorporant les fonctionnalités suivantes :

- Les incidents d'intrusion comprennent des TTP, ce qui permet aux administrateurs de gérer le trafic avec une plus grande granularité en regroupant les règles en fonction du type de vulnérabilité, du système cible ou de la catégorie de menace.
- Certains événements de programmes malveillants utilisent des TTP, ce qui améliore la capacité à détecter les menaces et à y répondre.
- Les visionneuses d'événements unifiés et classiques affichent les tactiques, les techniques, les graphiques de cycle de vie des attaques et les enrichissements contextuels à partir de la classification Talos. Ces enrichissements comprennent des balises MITRE et une vue hiérarchique des tactiques, techniques et sous-techniques associées. Vous pouvez également filtrer les événements à l'aide des identifiants MITRE.

Avantages du cadre MITRE

Le cadre MITRE offre des avantages de sécurité qui

- permettent aux administrateurs d'agir sur le trafic en fonction des Tactiques, Techniques et Procédures (TTP) MITRE ajoutées aux incidents d'intrusion,

- permettent l'affichage et le traitement du trafic avec plus de granularité grâce à des règles de regroupement par type de vulnérabilité, système cible ou catégorie de menace, et
- offrent la possibilité d'organiser les règles de prévention des intrusions selon le cadre MITRE ATT&CK pour des politiques personnalisées en fonction de tactiques et de techniques d'attaques spécifiques.

Exemple de scénario d'entreprise pour le réseau MITER

Un exemple de scénario d'entreprise pour le réseau MITER est un exemple d'implémentation de la sécurité qui

- utilise Snort 3 comme système principal de détection et de prévention des intrusions pour un grand réseau d'entreprise,
- répond au besoin de mesures de sécurité réseau robustes dans un paysage des menaces en pleine évolution, et
- permet aux administrateurs réseau de déterminer si les politiques configurées trouvent le trafic d'intérêt et font le suivi des groupes d'attaques connus.

Questions de sécurité réseau

Les administrateurs réseau doivent savoir si les attaquants tentent de profiter des faiblesses de leurs systèmes ou applications pour provoquer un comportement imprévu. La faiblesse du système peut être un bogue, un problème ou une vulnérabilité de conception. Les applications peuvent être des sites Web, des bases de données, des services standard, tels que Server Message Block (SMB) ou Secure Shell (SSH), des protocoles d'administration et de gestion des périphériques réseau ou des applications, telles que les serveurs Web et les services associés.

Les observations fournies par le cadre MITRE offrent aux administrateurs une possibilité plus précise de préciser la protection pour des ressources spécifiques et de protéger leur réseau contre des groupes de menaces spécifiques.

Préalables pour le cadre MITRE

Assurez-vous que votre système répond à ces exigences avant de mettre en œuvre le cadre MITRE :

- Vous devez exécuter Secure Firewall Management Center et Secure Firewall Threat Defense version 7.3.0 ou ultérieure avec Snort 3.
- Vous devez avoir au moins une politique de prévention des intrusions. Consultez [Création d'une politique de prévention des intrusions Snort 3 personnalisée](#), à la page 51.

Afficher et modifier votre politique de prévention des intrusions Snort 3

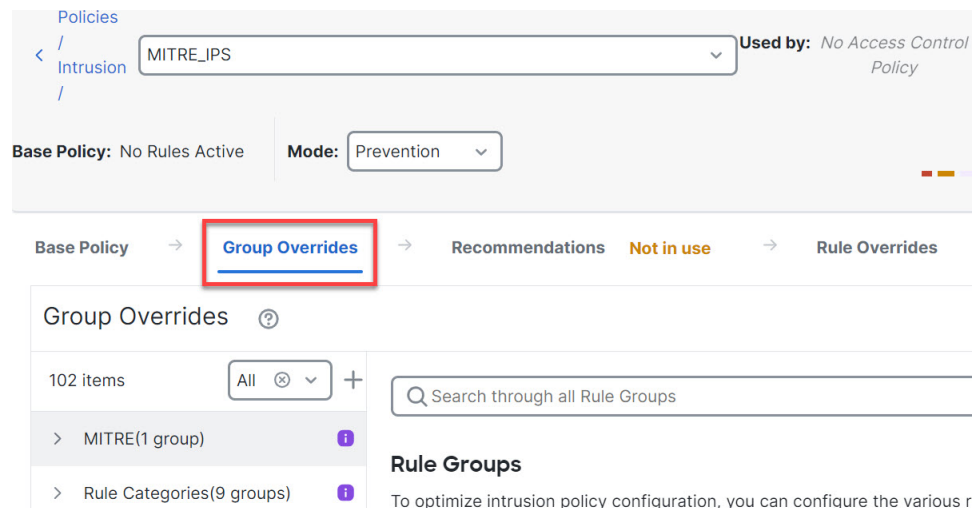
Cette tâche vous permet de personnaliser votre politique de prévention des intrusions Snort 3 en modifiant les groupes de règles, les niveaux de sécurité et d'accéder aux règles recommandées par Cisco pour améliorer les capacités de détection des menaces.

Les politiques de prévention des intrusions Snort 3 utilisent une structure de groupes de règles hiérarchique planifiée par le cadre MITRE. Vous pouvez accéder à des catégories de règles spécifiques et modifier les niveaux de sécurité pour les modifications en bloc ou les actions de règles individuelles. L'éditeur de politiques

fournit plusieurs couches, notamment les remplacements de groupe, les remplacements de règles, les recommandations et les affichages résumés.

Procédure

- Étape 1** Choisissez **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**.
- Étape 2** Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.
- Cliquez sur **Snort 3 Version** (Version Snort 3) à côté de la politique de prévention des intrusions que vous souhaitez afficher ou modifier.
 - Fermez le guide de l'assistant Snort qui s'affiche.
- Étape 3** Cliquez sur la couche **Group Overrides** (Remplacements de groupe).
- Cette couche répertorie toutes les catégories de groupes de règles dans une structure hiérarchique. Vous pouvez accéder au groupe de règles descendant sous chaque groupe de règles.



- Sous **Group Overrides** (Remplacements de groupe), assurez-vous que **All** (Tout) est choisi dans la liste déroulante, de sorte que tous les groupes de règles de la politique de prévention des intrusions correspondante soient visibles dans le volet gauche.

Étape 4 Cliquez sur **MITRE** dans le volet de gauche.



Remarque

Selon vos besoins spécifiques, vous pouvez choisir le groupe de règles **Rule Categories** (Catégories de règles) ou tout autre groupe de règles et ses groupes de sous-règles. Tous les groupes de règles utilisent le cadre MITRE.

a) Sous **MITRE**, cliquez sur **ATT&CK Framework** (Cadre ATT&CK) pour accéder aux détails.

The screenshot shows the 'Group Overrides' section of the Snort 3 web interface. The breadcrumb navigation is 'Policies > / Intrusion > /'. The 'MITRE_IPS' policy is selected. The 'Base Policy' is 'No Rules Active' and the 'Mode' is 'Prevention'. The 'Group Overrides' section shows 102 items. The 'MITRE' group is expanded, and the 'ATT&CK Framework' group is highlighted with a red box. The 'Security Level' is set to 1. The table below shows the 'MITRE' group with 1 group.

Group Name	Security Level	Override	Rule Count
MITRE	1		1

b) Sous **ATT&CK Framework**, (Cadre ATT&CK), cliquez sur **Enterprise** (Entreprise) pour le développer.

The screenshot shows the 'Group Overrides' section of the Snort 3 web interface. The breadcrumb navigation is 'Policies > / Intrusion > /'. The 'MITRE_IPS' policy is selected. The 'Base Policy' is 'No Rules Active' and the 'Mode' is 'Prevention'. The 'Group Overrides' section shows 102 items. The 'MITRE' group is expanded, and the 'ATT&CK Framework' group is expanded. The 'Enterprise' group is highlighted with a red box. The 'Security Level' is set to 1. The table below shows the 'MITRE / ATT&CK Framework' group with 1 group.

Group Name	Security Level	Override
MITRE / ATT&CK Framework	1	

c) Cliquez sur l'icône **Modifier** (✎) à côté du **niveau de sécurité** du groupe de règles pour apporter des modifications en bloc à tous les niveaux de sécurité de groupe de règles associés dans la catégorie du groupe de règles **Enterprise**.

Group Overrides ?

102 items All ⊗ +

Search through all Rule Groups

MITRE / ATT&CK Framework
1 Groups

Security Level  

Group Name	Security Level	Override	Rule Count
------------	----------------	----------	------------

- d) Dans la fenêtre **Edit Security Level** (Modifier le niveau de sécurité), choisissez un **Security Level** (Niveau de sécurité) (dans cet exemple, **3**), puis cliquez sur **Save** (Enregistrer).

Edit Security Level ?

Bulk Group Security Level

Impacts 34 groups. This action will change the security level of all leaf groups within this group category.

Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks

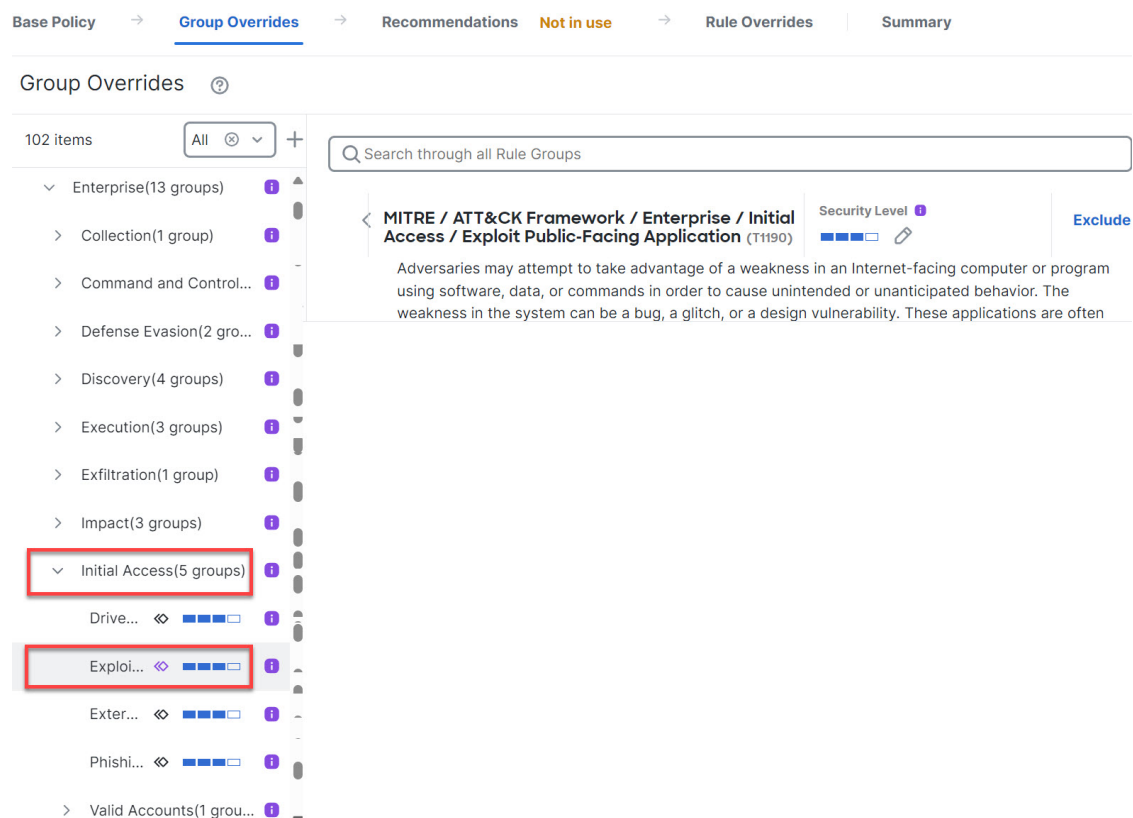
← Revert to default

Cancel

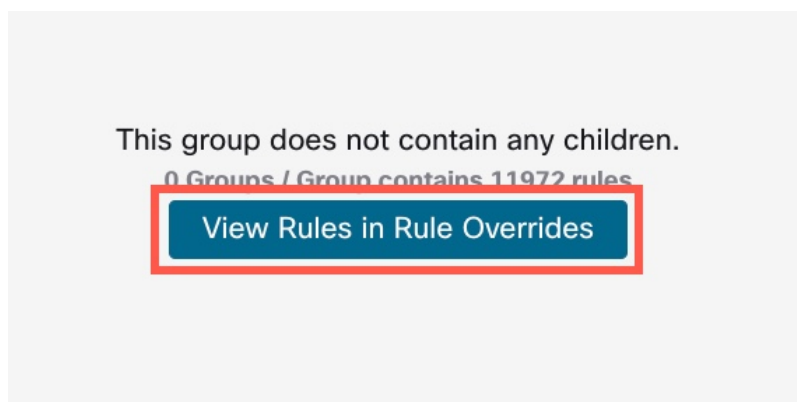
Save

Étape 5 Sous **Enterprise** (Entreprise), cliquez sur **Initial Access** (Accès initial) pour le développer.

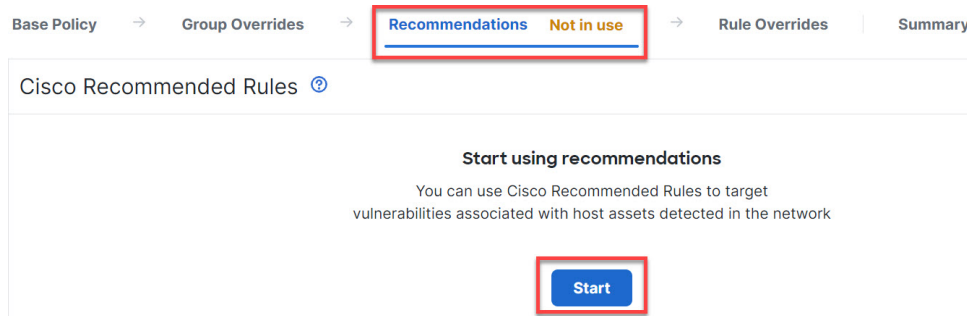
Étape 6 Sous **Initial Access** (Accès initial), cliquez sur **Exploit Public-Facing Application** (Exploiter une application accessible au public), qui est le dernier groupe de règles enfant.

**Étape 7**

Cliquez sur **View Rules** (Afficher les règles) dans Rule Overrides (Remplacements de règles) pour afficher les règles disponibles, leurs détails et leurs actions. Vous pouvez modifier les actions découlant d'une ou de plusieurs règles dans la couche **Rule Overrides** (Remplacements de règles).

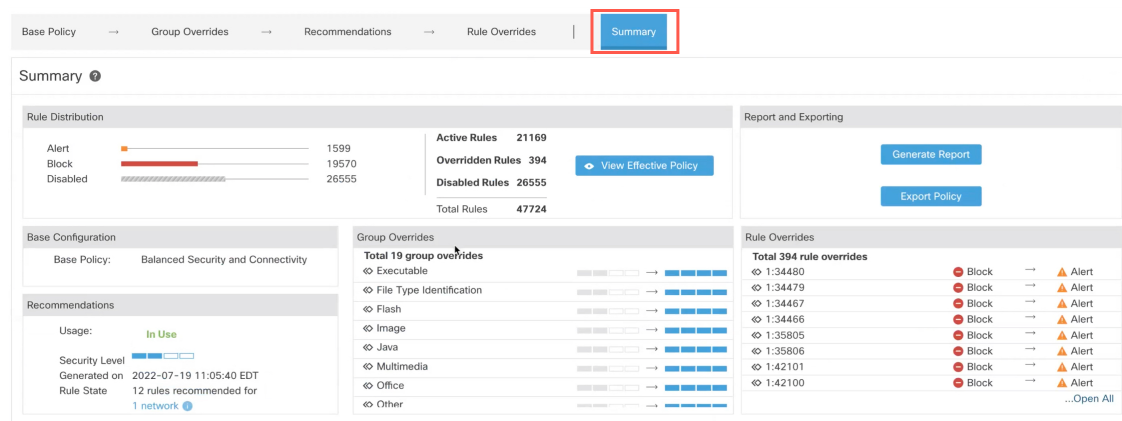
**Étape 8**

Cliquez sur la couche **Recommendations** (Recommandations), puis sur **Start** (Démarrer) pour commencer à utiliser les règles recommandées par Cisco. Vous pouvez utiliser les règles de prévention des intrusions recommandées par Cisco pour cibler les vulnérabilités associées aux ressources hôtes détectées dans le réseau. Pour en savoir plus, consultez [Générer de nouvelles recommandations Secure Firewall dans Snort 3](#), à la page 87.



Étape 9

Cliquez sur la couche **Summary** (résumé) pour obtenir une vue globale des modifications actuelles apportées à la politique. En fonction des remplacements de règles, des modifications de niveau de sécurité et de la génération de règles recommandées par Cisco, vous pouvez afficher la répartition des règles de la politique, les remplacements de groupe, les remplacements de règles, les recommandations de règles et des détails supplémentaires pour vérifier vos modifications.



Prochaine étape

Déployez votre politique de prévention des intrusions pour détecter et consigner les incidents déclenchés par les règles Snort. Consultez [Déploiement des modifications de configuration](#), à la page 36.

Afficher les incidents d'intrusion

Cette tâche vous permet d'afficher les techniques MITRE ATT&CK et les groupes de règles associés aux incidents d'intrusion, en fournissant un contexte de sécurité et un mappage des modèles d'attaque pour une meilleure analyse des menaces.

Vous pouvez afficher les techniques MITRE ATT&CK et les groupes de règles dans les incidents d'intrusion sur les pages **Classic Event Viewer** (Visionneuse d'événements classique) et **Unified Event Viewer** (Visionneuse d'événements unifiés). Talos fournit des mappages à partir des règles Snort (GID:SID) vers les techniques et les groupes de règles MITRE ATT&CK. Ces mappages sont installés dans le cadre du paquet de sécurité allégé (LSP).

Procédure

Étape 1 Cliquez sur **Analysis** (Analyse) et sélectionnez **Events** (Événements) sous **Intrusions**.

Étape 2 Cliquez sur l'onglet **Table View of Events** (Vue de tableau des événements).

Events By Priority and Classification [\(switch workflow\)](#)

2025-01-12 13:30:29 - 2025-01-12 14:45:19
Expanding

No Search Constraints [\(Edit Search\)](#)

Drilldown of Event, Priority, and Classification **Table View of Events** Packets

Jump to...

☐	Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP
☐	2025-01-12 14:43:19	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1
☐	2025-01-12 14:43:19	low	Unknown Target	Alert		0.0.0.0		224.0.0.1
☐	2025-01-12 14:43:19	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1
☐	2025-01-12 14:41:14	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1

Étape 3 Sous **MITRE ATT&CK**, vous pouvez voir les techniques utilisées pour un incident d'intrusion. Cliquez sur **1 Technique** pour afficher les techniques MITRE ATT&CK.

Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

Dans cet exemple, **Exploit Public-Facing Application** (Exploiter une application publique) est la technique.

MITRE ATT&CK Techniques

- Enterprise
 - Initial Access
 - Exploit Public-Facing Application

[Close](#)

Access Control Rule	Network Analysis Policy	MITRE ATT&CK
TestRuleFile	Simple NAP Policy	1 Technique
TestRuleFile	Simple NAP Policy	
TestRuleFile	Simple NAP Policy	
TestRuleFile	Simple NAP Policy	
TestRuleFile	Simple NAP Policy	

Étape 4 Cliquez sur **Close** (Fermer).

Étape 5 Cliquez sur **Analysis** (Analyse) et sélectionnez **Unified Events** (Événements unifiés).

Étape 6 Si elle n'est pas activée, cliquez sur l'icône du sélecteur de colonne pour activer les colonnes **MITRE ATT&CK** et **Rule Group** (Groupe de règles).

Search...

70 103 0 0 173 events

2025-01-12 13:56:29 EST 1h Go Live

Time	Event Type	Rule	Access Control Policy	Device	MITRE ATT&CK
2025-01-12 14:55:49	Connection	AC_with_security_intelligen..			
2025-01-12 14:55:49	Intrusion	AC_with_security_intelligen..			
2025-01-12 14:55:49	Intrusion	AC_with_security_intelligen..			
2025-01-12 14:55:49	Connection	AC_with_security_intelligen..			
2025-01-12 14:55:49	Intrusion	AC_with_security_intelligen..			
2025-01-12 14:53:44	Connection	AC_with_security_intelligen..			
2025-01-12 14:53:44	Intrusion	AC_with_security_intelligen..			

Column set

Q mitre

Deselect 1 filtered | Select default

☒ MITRE ATT&CK

Revert

12 selected Apply

Étape 7

Dans cet exemple, l'incident d'intrusion est déclenché par un événement mappé à un groupe de règles. Cliquez sur **1 Group** (1 groupe) sous la colonne **Rule Group** (Groupe de règles).

Views... Select...

Showing all 5,112 events (4,518 594)

2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT

Time	Event Type	Device	MITRE ATT&CK	Rule Group
2022-07-19 11:19:02	Intrusion	192.168.7.115		1 Group
2022-07-19 11:18:59	Connection	192.168.7.115		Click to view groups
2022-07-19 11:18:59	Connection	192.168.7.115		

Étape 8

Vous pouvez afficher **Protocol** (Protocole), qui est le groupe de règles parent, et le groupe de règles DNS en dessous. Choisissez **Protocol (Protocole) > DNS** pour rechercher tous les incidents d'intrusion qui ont au moins un groupe de règles.

Views... Select...

Showing all 5,112 events (4,518 594)

2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT

Time	Event Type	Device	MITRE ATT&CK	Rule Group
2022-07-19 11:19:02	Intrusion	192.168.7.115		1 Group
2022-07-19 11:18:59	Connection	192.168.7.115		Protocol
2022-07-19 11:18:59	Connection	192.168.7.115		DNS
2022-07-19 11:18:59	Connection	192.168.7.115		
2022-07-19 11:18:59	Connection	192.168.7.115		

Les résultats de la recherche sont affichés.

Views... Rule Group Protocol Select...

Showing all 501 events (501)

2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Snort ID
2022-07-19 11:19:08	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:07	Intrusion	192.168.7.115		Protocol	1:254:16
2022-07-19 11:19:03	Intrusion	192.168.7.115		DNS	1:254:16
2022-07-19 11:19:02	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:59	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:38	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:35	Intrusion	192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:31	Intrusion	192.168.7.115		1 Group	1:254:16

Références supplémentaires

Cette référence fournit des liens vers de la documentation et des ressources supplémentaires pour les politiques de prévention des intrusions dans Snort 3 et les informations de cadre MITRE pour la classification des incidents de programmes malveillants.

- [Politique de prévention des intrusions dans Snort 3](#)
- [Modification des politiques de prévention des intrusions Snort 3, à la page 52](#)
- [Informations MITRE dans les incidents de programmes malveillants](#)



CHAPITRE 4

Réglage du rendement de la prévention des intrusions

Ce chapitre explique comment affiner les performances de la prévention des intrusions.

- [Réglage du rendement de la prévention des intrusions, à la page 103](#)
- [Licence requise pour le réglage du rendement de la prévention des intrusions, à la page 104](#)
- [Exigences et conditions préalables pour le réglage du rendement de la prévention des intrusions, à la page 104](#)
- [Limitation de la mise en correspondance de modèles pour les intrusions, à la page 105](#)
- [Remplacements des limites de l'expression régulière pour les règles d'intrusion, à la page 106](#)
- [Remplacements des limites de l'expression régulière pour les règles de prévention des intrusions, à la page 107](#)
- [Limites de génération d'incidents d'intrusion par paquet, à la page 108](#)
- [Limitation des incidents de prévention des intrusions générés par paquet, à la page 109](#)
- [Configuration du seuil de latence des paquets et des règles d'intrusion, à la page 109](#)
- [Configuration de la journalisation des statistiques de rendement en cas d'intrusion, à la page 117](#)
- [Configuration de la journalisation des statistiques de rendement de la prévention des intrusions, à la page 118](#)

Réglage du rendement de la prévention des intrusions

Le réglage des performances de la prévention des intrusions est un mécanisme d'optimisation du système qui

- améliore les performances lors de l'analyse du trafic à la recherche de tentatives d'intrusions,
- applique les paramètres sur une base par politique de contrôle d'accès à toutes les politiques de prévention des intrusions invoquées par cette politique de contrôle d'accès parente, et
- équilibre la sécurité avec la nécessité de maintenir la latence de l'appareil à un niveau acceptable.

Fonctionnalités de réglage de la performance

Cisco fournit plusieurs fonctionnalités pour améliorer les performances de votre système lors de l'analyse du trafic à la recherche de tentatives d'intrusions. Vous pouvez réaliser les actions suivantes :

- Spécifiez le nombre de paquets à autoriser dans la file d'attente des événements. Vous pouvez également, avant et après le réassemblage des flux, activer ou désactiver l'inspection des paquets qui seront recréés en flux plus importants.
- Remplacez les limites de correspondance et de récursivité par défaut sur PCRE qui sont utilisées dans les règles de prévention des intrusions pour examiner le contenu de la charge utile des paquets.
- Choisissez que le moteur de règles journalise plus d'un événement par paquet ou flux de paquets lorsque plusieurs événements sont générés, ce qui vous permet de recueillir des informations au-delà de l'événement signalé.
- Trouvez un équilibre entre la sécurité et le besoin de maintenir la latence des périphériques à un niveau acceptable grâce à un seuil de latence des paquets et des règles.
- Configurez les paramètres de base sur la façon dont les périphériques surveillent et communiquent leurs propres performances. Cela vous permet de préciser les intervalles auxquels le système met à jour les statistiques de performance sur vos périphériques.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Licence requise pour le réglage du rendement de la prévention des intrusions

Cette référence fournit les renseignements de licence nécessaires pour mettre en œuvre le réglage de performance de prévention des intrusions sur les appareils Cisco Secure Firewall, pour la protection contre les menaces et les modèles de licence classique.

Licence de défense contre les menaces

IPS

Exigences et conditions préalables pour le réglage du rendement de la prévention des intrusions

Cette référence présente les exigences du système et les configurations préalables nécessaires avant de mettre en œuvre le réglage des performances de prévention des intrusions sur les périphériques Cisco Secure Firewall.

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles de l'utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Limitation de la mise en correspondance de modèles pour les intrusions

Limitez la mise en correspondance de modèles pour les intrusions afin d'optimiser les performances du système en contrôlant le nombre d'états de modèle analysés par paquet et en gérant l'inspection du contenu avant et après le réassemblage des flux.

Les limites de correspondance de modèles aident à équilibrer l'efficacité de la sécurité et les performances du système. Lors du traitement de volumes de trafic élevés, la limitation du nombre d'états de modèle analysés par paquet peut empêcher la dégradation des performances tout en maintenant les capacités essentielles de détection des intrusions.

Before you begin

Suivez ces étapes pour limiter la mise en correspondance de modèles pour les intrusions :

Procédure

- | | |
|----------------|--|
| Étape 1 | <p>Dans l'éditeur de stratégie de contrôle d'accès, cliquez sur Advanced (Avancés) (Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Access Control (Contrôle d'accès), cliquez sur Edit (Modifier) puis sur Advanced Settings (Paramètres avancés)).</p> <p>Dans la nouvelle interface utilisateur, sélectionnez Advanced Settings (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.</p> |
| Étape 2 | <p>Cliquez sur Modifier (🔗) à côté de Performance Settings (Paramètres de performance).</p> <p>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.</p> |
| Étape 3 | Cliquez sur Limites de correspondance de modèles dans la fenêtre contextuelle Paramètres de performance . |
| Étape 4 | Saisissez une valeur pour le nombre maximal d'événements à mettre en file d'attente dans le champ Nombre maximal d'états de signatures à analyser par paquet . |
| Étape 5 | Pour désactiver l'inspection des paquets qui seront recréés en flux de données plus volumineux avant et après le réassemblage des flux dans Snort 2, cochez la case Disable Content Checks on Traffic Subject to future Reassembly (Désactiver les vérifications de contenu sur le trafic sujet à un réassemblage futur). L'inspection |

avant et après le assemblage nécessite une surcharge de traitement plus importante et peut réduire les performances.



Important Dans Snort 3, les paramètres de la case à cocher **Désactiver les vérifications de contenu sur le trafic sujet à un réassemblage futur** sont :

- **Cochée** : indique la détection de la charge utile TCP avant le réassemblage. Cela comprend l'inspection des paquets avant et après le réassemblage du flux. Ce processus nécessite plus de trafic de traitement et peut réduire les performances.
- **Non cochée** : indique la détection de la charge utile TCP après le réassemblage.

Étape 6 Cliquez sur **OK**.

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

Prochaine étape

- Déployer les changements de configuration.

Remplacements des limites de l'expression régulière pour les règles d'intrusion

Les limites de l'expression régulière par défaut assurent un niveau de performance minimal. Le dépassement de ces limites peut accroître la sécurité, mais peut également avoir un impact considérable sur les performances en autorisant l'évaluation des paquets par rapport à des expressions régulières inefficaces.



Mise en garde N'outrepassiez pas les limites PCRE par défaut à moins d'être un rédacteur de règles de prévention des intrusions expérimenté et de connaître les incidences des modèles dégradés.

Tableau 7 : Options de contrainte d'expression régulière

Option	Description
Faire correspondre à l'état limite	Spécifie s'il faut remplacer la Match Limit (Limite de correspondance). Vous avez les options suivantes : • sélectionnez Default (par défaut) pour utiliser la valeur configurée pour la limite de correspondance. • sélectionnez Illimité pour autoriser un nombre illimité de tentatives. • sélectionnez Personnalisé pour spécifier une limite de 1 ou plus pour la Limite de correspondance ou spécifiez 0 pour désactiver complètement les évaluations de correspondance PCRE

Option	Description
Faire correspondre à la limite	Spécifie le nombre de tentatives de correspondre à un modèle défini dans une expression régulière PCRE.
Faire correspondre à l'état limite de récursivité	Spécifie s'il faut remplacer la Match Recursion Limit (Limite de récursivité de correspondance). Vous avez les options suivantes : • sélectionnez Default (par défaut) pour utiliser la valeur configurée pour la limite de récursivité de correspondance. • sélectionnez Illimité pour autoriser un nombre illimité de récursivités. • sélectionnez Personnalisé pour spécifier une limite égale ou supérieure à 1 pour la limite de récursivité de correspondance ou spécifiez 0 pour désactiver complètement les récursions PCRE Notez que pour que la limite de récursivité de correspondance soit significative, elle doit être inférieure à la limite de correspondance.
Faire correspondre à la limite de récursivité	Spécifie le nombre de récursions lors de l'évaluation d'une expression régulière PCRE par rapport à la charge utile du paquet.

Remplacements des limites de l'expression régulière pour les règles de prévention des intrusions

Remplacez les limites d'expression régulière par défaut pour personnaliser les paramètres de performance pour les règles de prévention des intrusions en fonction des exigences de votre réseau.

Les limites d'expression régulière contrôlent le traitement de la mise en correspondance de modèle dans les règles de prévention des intrusions. La modification de ces limites peut aider à optimiser les performances en fonction de votre environnement et de vos modèles de trafic spécifiques.

Procédure

-
- Étape 1** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé).
- Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.
- Étape 2** Cliquez sur **Modifier** (✎) à côté de **Performance Settings** (Paramètres de performance).
- 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.
- Étape 3** Cliquez sur **Normal Expression Limits** (Limites d'expression normale) dans la fenêtre contextuelle **Performance Settings** (Paramètres de performance).

- Étape 4** Vous pouvez modifier n'importe quelle option, comme décrit dans [Remplacements des limites de l'expression régulière pour les règles d'intrusion](#), à la page 106.
- Étape 5** Cliquez sur **OK**.
- Étape 6** Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Limites de génération d'incidents d'intrusion par paquet

Lorsque le moteur de règles de prévention des intrusions évalue le trafic en fonction des règles, il place les événements générés pour un paquet ou flux de paquets donné dans une file d'attente des événements, puis signale les principaux événements de la file d'attente à l'interface utilisateur. Lors de la configuration des limites de journalisation des incidents d'intrusion, vous pouvez préciser le nombre d'événements qui peuvent être placés dans la file d'attente et combien sont journalisés, et sélectionner les critères pour déterminer l'ordre des événements dans la file d'attente.

Tableau 8 : Options de limites de journalisation des incidents d'intrusion

Option	Description
Nombre maximal d'incidents stockés par paquet	Le nombre maximal d'événements qui peuvent être stockés pour un paquet ou flux de paquets donné.
Nombre maximal d'incidents journalisés par paquet	Le nombre d'événements enregistrés pour un paquet ou flux de paquets donné. Le nombre ne peut pas dépasser la valeur Nombre maximal d'événements stockés par paquet .
Prioriser la journalisation des incidents par	Valeur utilisée pour déterminer l'ordre des événements dans la file d'attente des événements. L'événement ordonné le plus élevé est signalé par l'intermédiaire de l'interface utilisateur. Vous avez le choix entre : • <code>priority</code> (priorité), qui classe les événements dans la file d'attente en fonction de leur priorité. • <code>content_length</code> (longueur du contenu), qui classe les événements en fonction de la correspondance de contenu identifié la plus longue. Lorsque les événements sont classés en fonction de la longueur du contenu, les événements liés aux règles ont toujours la priorité sur les événements liés au décodeur et au préprocesseur.

Limitation des incidents de prévention des intrusions générés par paquet

Cette tâche vous permet de contrôler le nombre d'incidents d'intrusion générés par paquet en configurant les limites de journalisation des événements d'intrusion dans les paramètres de performance de la stratégie de contrôle d'accès.

Utilisez cette tâche lorsque vous devez gérer les performances du système de détection d'intrusion en limitant le nombre d'événements générés pour chaque paquet traité par le pare-feu.

Procédure

-
- Étape 1** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé).
- Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.
- Étape 2** Cliquez sur **Modifier** (✎) à côté de **Performance Settings** (Paramètres de performance).
- 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.
- Étape 3** Cliquez sur **Intrusion Event Logging Limits** (Limites d'enregistrement des incidents d'intrusion) dans la fenêtre contextuelle **Performance Settings** (Paramètres de rendement).
- Étape 4** Vous pouvez modifier n'importe quelle option dans [Limites de génération d'incidents d'intrusion par paquet, à la page 108](#).
- Étape 5** Cliquez sur **OK**.
- Étape 6** Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.
-

Prochaine étape

- Déployer les changements de configuration.

Configuration du seuil de latence des paquets et des règles d'intrusion

La configuration du seuil de latence des paquets et des règles d'intrusion est un mécanisme de gestion des performances qui

- utilise un seuil pour gérer les performances de traitement des paquets et des règles dans les stratégies de contrôle d'accès,
- mesure le temps écoulé pour les opérations de traitement des paquets et des règles, et

- met en œuvre des actions de protection lorsque les seuils de temps configurables sont dépassés.

Mécanismes de traitement

Cette configuration comprend deux mécanismes de traitement distincts :

- **Packet latency thresholding** (Seuil de latence des paquets) : mesure le temps total écoulé pour traiter un paquet par les décodeurs, préprocesseurs et règles applicables, et interrompt l'inspection du paquet si le temps de traitement dépasse un seuil configurable.
- **Rule latency thresholding** (Seuil de latence des règles) : mesure le temps écoulé nécessaire à chaque règle pour traiter un paquet individuel, suspend la règle en question ainsi qu'un groupe de règles connexes pendant un temps donné si le temps de traitement dépasse le seuil de latence de la règle un nombre de fois consécutives configurables, et restaure les règles à l'expiration de la suspension.



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Paramètres de performance en fonction de la latence

Les paramètres de performance basés sur la latence sont un mécanisme de configuration système qui

- prend les paramètres de performance de la dernière mise à jour des règles de prévention des intrusions déployées sur le système,
- applique les paramètres en fonction du niveau de sécurité de la politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) associée à la politique de contrôle d'accès, et
- évalue la politique d'analyse de réseau la plus sécurisée parmi les règles personnalisées lorsque plusieurs politiques sont configurées.

Logique d'évaluation des politiques

Les paramètres de latence qui sont réellement appliqués dépendent du niveau de sécurité de la politique d'analyse de réseau (NAP) associée à la politique de contrôle d'accès. En général, il s'agit de la politique Politique d'analyse de réseau (NAP) par défaut. Toutefois, si des règles d'analyse de réseau personnalisées sont configurées et si l'une d'entre elles spécifie une politique d'analyse de réseau (NAP) plus sécurisée que la politique d'analyse de réseau (NAP) par défaut, les paramètres de latence sont basés sur la politique d'analyse de réseau (NAP) la plus sécurisée parmi les règles personnalisées. Si la politique d'analyse de réseau (NAP) par défaut ou des règles personnalisées font appel à une politique d'analyse de réseau (NAP) personnalisée, le niveau de sécurité utilisé dans l'évaluation est celui de la politique de base fournie par le système sur lequel chaque politique d'analyse de réseau (NAP) personnalisée est basée.

Cette logique d'évaluation de politique s'applique, que les configurations de seuil et d'analyse de réseau effectives soient héritées ou configurées directement dans la politique.

Seuil de latence des paquets

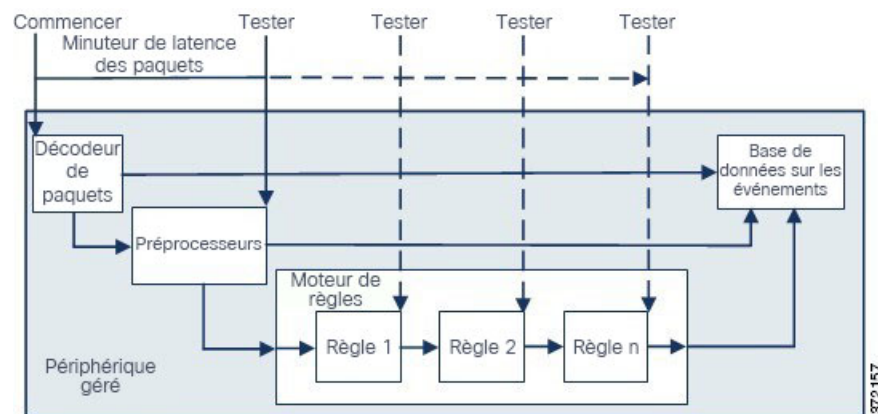
Le seuil de latence des paquets est une implémentation logicielle de la latence qui

- mesure le temps écoulé, pas seulement le temps de traitement, afin de refléter plus précisément le temps réel nécessaire à la règle pour traiter un paquet,
- n'impose pas de synchronisation stricte, et
- peut améliorer les performances du système en interrompant l'inspection des paquets qui nécessitent un temps de traitement excessif.

Fonctionnement du seuil de latence des paquets

Une minuterie démarre pour chaque paquet au début du traitement du décodeur. La synchronisation se poursuit jusqu'à la fin du traitement du paquet ou jusqu'à ce que la durée de traitement dépasse le seuil à un point de test de synchronisation.

Le compromis pour les avantages en matière de performance et de latence dérivés du seuil de latence est que les paquets non inspectés pourraient contenir des attaques.



La synchronisation de la latence des paquets est testée à ces points de test :

- après l'achèvement de tous les traitements du décodeur et du préprocesseur et avant le début du traitement des règles
- après le traitement par chaque règle

Si le temps de traitement dépasse le seuil à un point de test, l'inspection des paquets s'arrête.



Astuces

Le temps total de traitement des paquets ne comprend pas les heures de réassemblage des flux TCP de routine ou des fragments IP.

Le seuil de latence des paquets n'a aucun effet sur les événements déclenchés par un décodeur, un préprocesseur ou une règle qui traite le paquet. Tout décodeur, préprocesseur ou règle applicable se déclenche normalement jusqu'à ce qu'un paquet soit entièrement traité ou jusqu'à la fin du traitement des paquets parce que le seuil de latence est dépassé, selon la première de ces éventualités. Si une règle de suppression détecte une intrusion dans un déploiement en ligne, elle déclenche un événement et le paquet est abandonné.

**Remarque**

Aucun paquet n'est évalué par rapport aux règles une fois que le traitement de ce paquet a cessé en raison d'une violation du seuil de latence des paquets. Une règle qui aurait déclenché un événement ne peut pas déclencher cet événement et, pour les règles de suppression, ne peut pas abandonner le paquet.

Le seuil de latence des paquets peut améliorer les performances du système dans les déploiements passifs et en ligne et peut réduire la latence dans les déploiements en ligne, en arrêtant l'inspection des paquets qui nécessitent un temps de traitement excessif. Ces gains de performance peuvent se produire lorsque, par exemple :

- Pour les déploiements passifs et en ligne, l'inspection successive d'un paquet par plusieurs règles nécessite beaucoup de temps
- Pour les déploiements en ligne, une période de faible performance du réseau, par exemple lorsqu'un utilisateur télécharge un fichier extrêmement volumineux, ralentit le traitement des paquets

Dans un déploiement passif, l'arrêt du traitement des paquets peut ne pas contribuer à restaurer les performances du réseau, car le traitement passe simplement au paquet suivant.

Remarques sur le seuil de latence des paquets

Par défaut, les paramètres de performance basés sur la latence pour la gestion des paquets sont désactivés. Vous pouvez choisir de l'activer. Cependant, Cisco vous recommande de ne pas modifier la valeur par défaut du paramètre de seuil. Les informations de cette rubrique s'appliquent uniquement si vous choisissez de spécifier des valeurs personnalisées.

Activer le seuil de latence des paquets

Activez le seuil de latence des paquets pour superviser et gérer les retards de traitement des paquets, ce qui permet d'optimiser les performances du réseau et d'identifier les goulots d'étranglement potentiels.

Le seuil de latence des paquets vous permet de définir les paramètres de performance pour le traitement des paquets. Cette fonctionnalité est utile pour superviser les performances du réseau et assurer un flux de paquets optimal dans le système.

Procédure

- | | |
|----------------|--|
| Étape 1 | <p>Dans l'éditeur de politique de contrôle d'accès, cliquez sur Advanced (Avancé).</p> <p>Dans la nouvelle interface utilisateur, sélectionnez Advanced Settings (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.</p> |
| Étape 2 | <p>Cliquez sur Modifier (✎) à côté de Latency-Based Performance Settings (Paramètres de performance basés sur la latence).</p> <p>Si Afficher (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.</p> |
| Étape 3 | <p>Cliquez sur Packet Management (gestion des paquets) dans la fenêtre contextuelle Latency-Based Performance Settings (paramètres de performance basés sur la latence).</p> |
| Étape 4 | <p>Cochez la case Enabled (activer).</p> |

- Étape 5** Cliquez sur **OK**.
- Étape 6** Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configuration du seuil de latence des paquets

Cette tâche vous permet de configurer le seuil de latence des paquets pour les paramètres de performance basés sur la latence.

Par défaut, les paramètres de performance basés sur la latence pour la gestion des paquets sont désactivés. Vous pouvez choisir de l'activer. Cependant, Cisco vous recommande de ne pas modifier la valeur par défaut du paramètre de seuil.

Procédure

- Étape 1** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé).
- Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.
- Étape 2** Cliquez sur **Modifier** (✎) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).
- Système** (🔍) > **Monitoring (Supervision)** > **Statistics (Statistiques)**
- Étape 3** Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.
- Étape 4** Cliquez sur **Packet Management** (gestion des paquets) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).
- Par défaut, l'option **Installed Rule Update** (mise à jour des règles installée) est sélectionnée. Il est conseillé d'utiliser cette valeur par défaut.
- Les valeurs affichées ne reflètent pas les paramètres automatisés.
- Étape 5** Si vous choisissez d'indiquer des valeurs personnalisées :
- Cochez la case **Enabled** (activé) et consultez [Remarques sur le seuil de latence des paquets, à la page 112](#) pour connaître les paramètres de **seuil** minimaux recommandés.
 - Vous devez préciser des valeurs personnalisées dans les onglets de gestion des paquets et des règles.
- Étape 6** Cliquez sur **OK**.
- Étape 7** Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Seuil de latence des règles

Le seuil de latence des règles est une implémentation logicielle de la latence qui

- mesure le temps écoulé, pas seulement le temps de traitement, afin de refléter plus précisément le temps réel nécessaire à la règle pour traiter un paquet,
- n'impose pas de synchronisation stricte, et
- suspend temporairement les règles qui dépassent les seuils de temps de traitement précisés afin d'améliorer les performances du système.

Opérations de seuil de latence des règles

Une minuterie mesure le temps de traitement chaque fois qu'un paquet est traité selon un groupe de règles. Chaque fois que le temps de traitement de la règle dépasse un seuil de latence de règle spécifié, le système incrémente un compteur. Si le nombre de dépassements de seuil consécutifs atteint un nombre déterminé, le système effectue les actions suivantes :

- suspend les règles pendant la période spécifiée
- déclenche un événement indiquant que les règles ont été suspendues
- réactive les règles à l'expiration de la suspension.
- déclenche un événement indiquant que les règles ont été réactivées

Le système remet le compteur à zéro lorsque le groupe de règles a été suspendu ou lorsque les violations aux règles ne sont pas consécutives. Autoriser certaines violations consécutives avant de suspendre les règles vous permet d'ignorer des violations occasionnelles de règles qui pourraient avoir un impact négligeable sur les performances et de vous concentrer sur l'impact plus important des règles qui dépassent à plusieurs reprises le seuil de latence des règles.

Le compromis pour les avantages en matière de performance et de latence dérivés du seuil de latence est que les paquets non inspectés pourraient contenir des attaques.

Le seuil de latence des règles n'a aucun effet sur les incidents d'intrusion déclenchés par les règles qui traitent le paquet. Une règle déclenche un événement pour toute intrusion détectée dans le paquet, que le temps de traitement de la règle dépasse ou non le seuil. Si la règle qui détecte l'intrusion est une règle de suppression dans un déploiement en ligne, le paquet est abandonné. Lorsqu'une règle de suppression détecte une intrusion dans un paquet qui entraîne la suspension de la règle, la règle de suppression déclenche un incident d'intrusion, le paquet est abandonné et cette règle ainsi que toutes les règles connexes sont suspendues.

**Remarque**

Les paquets ne sont pas évalués par rapport aux règles suspendues. Une règle suspendue qui aurait déclenché un événement ne peut pas déclencher cet événement et, pour les règles de suppression, ne peut pas abandonner le paquet.

Le seuil de latence des règles peut améliorer les performances du système dans les déploiements passifs et en ligne, et peut réduire la latence dans les déploiements en ligne, en suspendant les règles qui prennent le plus de temps à traiter les paquets. Les paquets ne sont pas évalués à nouveau par rapport aux règles suspendues avant l'expiration d'un délai configurable, ce qui donne au périphérique surchargé le temps de récupérer. Ces gains de performance peuvent se produire lorsque :

- des règles écrites à la hâte et en grande partie non testées nécessitent un temps de traitement excessif
- une période de piètre performance du réseau, quand quelqu'un télécharge un fichier extrêmement volumineux, retarde l'inspection des paquets

Exemples de seuil de latence des règles

L'exemple suivant montre cinq temps de traitement de règle consécutifs qui n'entraînent pas la suspension de règle.

1	2	3	4	5	Paquet
1100	1100	1100	500	1100	Temps de traitement (microsecondes) (Seuil = 1 000)
1	2	3	0	1	Violations (Violations consécutives avant suspension = 5)

☐ = Aucune infraction ☒ = Violation du seuil

Dans cet exemple, le temps requis pour traiter chacun des trois premiers paquets dépasse le seuil de latence de la règle de 1000 microsecondes, et le compteur de violations augmente à chaque violation. Le traitement du quatrième paquet ne dépasse pas le seuil et le compteur des violations est réinitialisé à zéro. Le sixième paquet viole le seuil et le compteur de violations redémarre à un.

Cet exemple, montre cinq temps de traitement de règle consécutifs qui entraînent une suspension de règle.

1	2	3	4	5	6	...	n	Paquet
1100	1100	1100	1100	1100				Temps de traitement (microsecondes) (Seuil = 1 000)
1	2	3	4	5				Violations (Violations consécutives avant suspension = 5)

☐ = Aucune infraction ☒ = Violation du seuil ☐ = Non inspecté (règle suspendue)

Dans le deuxième exemple, le temps nécessaire pour traiter chacun des cinq paquets enfreint le seuil de latence de la règle de 1 000 microsecondes. Le groupe de règles est suspendu, car le temps de traitement de la règle de 1100 microsecondes pour chaque paquet dépasse le seuil de 1000 microsecondes pour les cinq violations consécutives spécifiées. Les paquets suivants, représentés dans la figure par les paquets 6 à n, ne sont pas examinés en fonction des règles de suspension avant l'expiration de la suspension. Si plus de paquets se produisent après la réactivation des règles, le compteur de violations recommence à zéro.

Remarques sur le seuil de latence des règles

Le seuil de latence des règles suspend les règles pendant la durée spécifiée par l'attribut **Suspension Time** (Temps de suspension) lorsque la durée nécessaire aux règles pour traiter un paquet dépasse le **Threshold** (Seuil) le nombre de fois consécutives précisé par **Consécutif Threshold Violations Before Suspending Rule** (Violations consécutives du seuil avant la suspension de la règle).

Par défaut, les paramètres de rendement basés sur la latence pour le traitement des paquets et des règles sont automatiquement remplis par la dernière mise à niveau des règles d'intrusion déployées, et il est conseillé de ne pas modifier la valeur par défaut.

Les informations de cette rubrique s'appliquent uniquement si vous choisissez de spécifier des valeurs personnalisées.

Vous pouvez activer la règle 134:1 pour générer un événement lorsque des règles sont suspendues et la règle 134:2 pour générer un événement lorsque des règles suspendues sont activées.

Tableau 9 : Options de seuil de latence des règles

Option	Description
Seuil	Spécifie la durée en microsecondes que les règles ne doivent pas dépasser lors de l'examen d'un paquet.
Quantité de violations consécutives du seuil avant la suspension de la règle	Spécifie le nombre de fois consécutives où les règles peuvent prendre plus de temps que le temps défini pour le Threshold (Seuil) pour inspecter les paquets avant que les règles ne soient suspendues.
Temps de la suspension	Spécifie la durée en secondes de suspension d'un groupe de règles.

Configurer le seuil de latence des règles

Configurez le seuil de latence des règles pour personnaliser la façon dont le système gère les règles lorsque des conditions de latence sont détectées, ce qui améliore les performances globales et la réactivité du système.

Par défaut, les paramètres de rendement basés sur la latence pour le traitement des paquets et des règles sont automatiquement remplis par la dernière mise à niveau des règles d'intrusion déployées, et il est conseillé de ne pas modifier la valeur par défaut.

Procédure

-
- Étape 1** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé).
- Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.
- Étape 2** Cliquez sur **Modifier** (✎) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).
- 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.

- Étape 3** Cliquez sur **Rule Management** (gestion des règles) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).
- Par défaut, l'option **Installed Rule Update** (mise à jour des règles installée) est sélectionnée. Il est conseillé d'utiliser cette valeur par défaut.
- Les valeurs affichées ne reflètent pas les paramètres automatisés.
- Étape 4** Si vous choisissez d'indiquer des valeurs personnalisées :
- Vous pouvez configurer n'importe quelle option dans [Remarques sur le seuil de latence des règles, à la page 116](#).
 - Vous devez préciser des valeurs personnalisées dans les onglets de gestion des paquets et des règles.
- Étape 5** Cliquez sur **OK**.
- Étape 6** Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Si vous souhaitez générer des événements, activez les règles de latence 134:1 et 134:2.
- Déployer les changements de configuration.

Configuration de la journalisation des statistiques de rendement en cas d'intrusion

Cette référence fournit des informations sur les options de configuration de la journalisation des statistiques de performance en cas d'intrusion, y compris les paramètres d'heure d'échantillonnage, les exigences minimales de paquets et les options de débogage pour les données de session de journalisation et de distribution de protocole.

Durée d'échantillonnage (secondes) et nombre minimal de paquets

Lorsque le nombre de secondes spécifié s'écoule entre les mises à jour des statistiques de performance, le système vérifie qu'il a analysé le nombre de paquets spécifié. Si tel est le cas, le système met à jour les statistiques de performance. Sinon, le système attend d'analyser le nombre de paquets spécifié.



Mise en garde

La configuration d'une valeur très faible, comme une seconde, pour le Sample time (Temps d'échantillonnage) peut avoir une incidence considérable sur le périphérique. Le périphérique peut rencontrer des problèmes d'espace disque et son fonctionnement peut être perturbé par le volume de statistiques de rendement enregistrées. Pour éviter ces problèmes, ne définissez pas une valeur très faible.

Options de débogage : journaliser la session/la distribution du protocole

Le service d'assistance peut vous demander lors d'un appel de débogage de journaliser la distribution du protocole, la longueur des paquets et les statistiques de port.

**Mise en garde**

N'activez pas la **journalisation de session/de la distribution du protocole**, sauf si le service d'assistance vous le demande. Notez que pour les périphériques classiques uniquement, l'activation ou la désactivation de la **journalisation de session/de la distribution du protocole** redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Selon la façon dont le périphérique attribué traite le trafic, celui-ci peut être abandonné durant l'interruption ou passer sans inspection supplémentaire.

Options de dépannage : récapitulatif

Lors d'un appel de dépannage, l'assistance peut vous demander de configurer le système pour qu'il calcule les statistiques de performance uniquement lorsque le processus Snort est arrêté ou redémarré. Pour activer cette option, vous devez également activer l'option de dépannage **session de journalisation/la distribution du protocole**.

**Mise en garde**

N'activez pas le **récapitulatif**, sauf si le service d'assistance vous le demande.

Configuration de la journalisation des statistiques de rendement de la prévention des intrusions

Configurez la journalisation des statistiques de performance en cas d'intrusion pour personnaliser la façon dont le système échantillonne et enregistre les statistiques de performance à des fins de supervision et de dépannage.

La journalisation des statistiques de performance vous permet de superviser les performances du périphérique en échantillonnant les statistiques à des intervalles définis. Une configuration adéquate garantit des performances optimales du périphérique tout en fournissant les données de supervision nécessaires.

Procédure**Étape 1**

Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Modifier** (✎) à côté de **Performance Settings** (paramètres de rendement).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

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.

Étape 2

Cliquez sur **PerformanceStatistics** dans la fenêtre contextuelle qui apparaît.

Étape 3

Modifiez la **durée d'échantillonnage** ou le **nombre minimal de paquets** comme décrit dans [Configuration de la journalisation des statistiques de rendement en cas d'intrusion](#), à la page 117.

**Mise en garde**

La configuration d'une valeur très faible, comme une seconde, pour le **Sample time** (Temps d'échantillonnage) peut avoir une incidence considérable sur le périphérique. Le périphérique peut rencontrer des problèmes d'espace disque et son fonctionnement peut être perturbé par le volume de statistiques de rendement enregistrées. Pour éviter ces problèmes, ne définissez pas une valeur très faible.

Étape 4

Vous pouvez également développer la section des **options de dépannage** et modifier ces options uniquement si le service d'assistance vous le demande.

Étape 5

Cliquez sur **OK**.

Prochaine étape

- Déployer les changements de configuration.



CHAPITRE 5

Stratégies 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.

- [Analyse du réseau, à la page 121](#)
- [Gérer les politiques d'analyse du réseau, à la page 122](#)
- [Définitions et terminologies pour les politiques d'analyse de réseau Snort 3, à la page 123](#)
- [Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 126](#)
- [Paramètres de politique d'analyse de réseau et modifications en cache, à la page 155](#)
- [Générer des recommandations Snort 3, à la page 156](#)

Analyse du réseau

Une *politique d'analyse de réseau* est une configuration de prétraitement du trafic qui

- régit de nombreuses options de prétraitement du trafic et est appelée par les paramètres avancés de votre stratégie de contrôle d'accès,
- effectue le prétraitement après la correspondance Security Intelligence et le déchiffrement SSL, et
- termine le traitement avant que ne commence l'inspection des intrusions ou des fichiers.

Politiques d'analyse du réseau par défaut et personnalisées

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 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

Cette tâche vous permet d'effectuer diverses opérations de gestion sur les politiques d'analyse de réseau, notamment la création, la modification, la suppression, la comparaison et la génération de rapports.

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.

**Remarque**

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour plus de renseignements sur les fonctionnalités de Snort 2 prises en charge dans les versions antérieures à la version 7.7, consultez le [guide du centre de gestion](#) correspondant à votre version de Threat Defense.

Procédure

Étape 1

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

- **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Access Control (Contrôle d'accès)**, puis cliquez sur **Politique d'analyse de réseau**
- **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion**, puis cliquez sur **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 **version Snort 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 126.

- **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 les politiques 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 10 : 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).

Terme	Description
Inspecteur de classeur	L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et en tenir compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur Binder, alors seulement les valeurs et configurations de cet inspecteur entrent en vigueur. Pour en savoir plus, consultez la section <i>Inspecteur de classeur</i> dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 126.
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 <i>Inspecteurs Singleton</i> dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 126.
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 <i>Inspecteurs Multiton</i> dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 126.
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 134.

Terme	Description
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 134.
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 134.
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 134.

Sujets connexes

[Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 126](#)

[Personnaliser la politique d'analyse de réseau, à la page 134](#)

[Mappage de la stratégie d'analyse du réseau, à la page 131](#)

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

La création d'une politique d'analyse de réseau personnalisée pour Snort 3 est un processus de configuration basé sur les données qui

- permet aux utilisateurs avancés de personnaliser la politique d'analyse de réseau par défaut pour des exigences de réseau spécifiques ou d'optimiser les performances, et
- utilise JSON et le schéma JSON en fonction de la spécification OpenAPI pour configurer les inspecteurs et les paramètres.

Aperçu de la personnalisation de la politique d'analyse du réseau

La politique d'analyse de réseau par défaut est réglée pour les exigences de réseau typiques et des performances optimales. Dans la plupart des situations, vous n'avez pas besoin de personnaliser la politique. 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.

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. Le nombre d'inspecteurs et de paramètres disponibles dans Firewall Management Center est un sous-ensemble de ceux 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 Firewall Management Center.



Remarque

- Lors de la mise à niveau de Firewall Management Center 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 **Inspectors** (Inspecteurs) dans la version **Snort 3** de votre politique d'analyse de réseau.

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 Binder, alors seulement les valeurs et 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.

a

Si ces conditions sont remplies, utilisez le type imap.

```

▼ binder
185 {
186   "when": {
187     "service": "imap",
188     "role": "any"
189   },
190   "use": {
191     "type": "imap"
192   }
193 },

```

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. Assurez-vous d'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"
        }
      }
    ]
  }
}

```

Sécurité du Protocole industriel commun (CIP)

La sécurité CIP (Common Industrial Protocol) est un ensemble d'extensions du protocole CIP qui

- permet le fonctionnement sécurisé des périphériques,
- fournit une communication à sécurité intégrée entre différents nœuds sur un réseau CIP, et
- comprend deux composants principaux pour l'échange des paramètres de sécurité et la transmission des informations de sécurité.

Composants du protocole de sécurité CIP

Le protocole sécurité CIP comprend deux composants principaux :

- Segments CIP Safety : utilisés dans les messages Forward Open pour échanger des paramètres de sécurité pour la session de sécurité suivante.
- Messages CIP Safety : utilisés pour échanger des informations de sécurité réelles.

L'inspecteur CIP détecte et identifie :

- CIP en tant que service et client
- Charges utiles, telles que la lecture CIP, l'administration CIP, l'infrastructure CIP et l'écriture CIP

L'inspecteur CIP peut analyser les segments CIP et détecter les segments CIP Safety dans les demandes Forward Open.

Pour tester la fonction CIP Safety, vous devez activer l'inspecteur CIP. Consultez [Détection et blocage des segments de sécurité dans les paquets CIP](#), à la page 130.

Détection et blocage des segments de sécurité dans les paquets CIP

Cette tâche permet la détection et le blocage des segments de sécurité CIP tout en permettant le passage d'autres paquets CIP.

Utilisez cette procédure pour détecter et bloquer les segments CIP Safety tout en autorisant d'autres paquets CIP :

- Créez une politique d'analyse de réseau personnalisée appelée **cip_safety**.
- Créez des règles de contrôle d'accès dans votre politique de contrôle d'accès pour bloquer la fonction CIP Safety et autoriser tous les autres paquets.

Pour tester la fonction CIP Safety, activez l'inspecteur CIP dans le centre de gestion et affectez-le à une stratégie de contrôle d'accès.

Procédure

- | | |
|----------------|--|
| Étape 1 | Accédez à Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Cliquez sur la version Snort 3 de la politique d'analyse de réseau cip_safety que vous avez créée. |
| Étape 3 | Sous Inspectors (Inspecteurs) , cliquez sur CIP pour le développer.

La configuration par défaut s'affiche dans la colonne de gauche et la configuration remplacée s'affiche 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) et modifiez le champ « enabled » dans le champ Sous Inspectors (Inspecteurs) , cliquez sur CIP pour le développer . de false (par défaut) à true. |
| Étape 5 | Cliquez sur OK , puis sur Save (Enregistrer). |
| Étape 6 | Pour affecter l'inspecteur CIP à la stratégie de contrôle d'accès, choisissez Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Access Control (Contrôle d'accès) , cliquez sur Edit (Modifier) et sélectionnez l'option Advanced Settings (Paramètres avancés) dans la liste déroulante More (Plus) à la fin de la ligne de flux de paquets. |

- Étape 7** Cliquez sur **Modifier** (✎) à côté de **Politiques d'analyse du réseau et de prévention des intrusions**.
- Étape 8** Dans la fenêtre **Network Analysis and Intrusion Policies** (Politiques d'analyse du réseau et de prévention des intrusions), choisissez la politique de contrôle d'accès **cip_safety** que vous avez créée dans la liste déroulante **Default Network Analysis Policy** (Politique d'analyse du réseau par défaut).
- L'inspecteur CIP est maintenant activé dans le centre de gestion. Vous pouvez créer les règles de contrôle d'accès personnalisées pour bloquer les paquets CIP Safety et autoriser tous les autres paquets CIP.
- Étape 9** Après avoir envoyé le trafic en direct contenant les flux de paquets CIP Safety, accédez à **Connection Events** (Incidents de connexion) pour vérifier que la charge utile est la charge utile attendue qui contient les journaux de paquets CIP Safety pour le scénario de détection et de blocage comme mentionné dans cette procédure.
- CIP** est détecté en tant que protocole d'application et client (consultez les champs **Application Protocol** (Protocole d'application) et **Client** (client) et **CIP Safety** (CIP Safety) est affiché sous le champ **Web Application** (Application Web).

Mappage de la stratégie d'analyse du réseau

Le mappage des politiques d'analyse du réseau est un mécanisme de corrélation qui

- fournit des informations de cartographie pour les politiques d'analyse du réseau,
- recherche la version des politiques Snort 2 correspondante pour la version Snort 3, et
- garantit que les politiques de la version Snort 3 ont leur équivalent dans la version Snort 2.

Afficher le mappage de la politique d'analyse des réseaux

Affichez les politiques d'analyse de réseau Snort 3 qui sont automatiquement mappées à leurs politiques équivalentes Snort 2 dans le système.

Le mappage des politiques d'analyse de réseau vous permet de voir la relation entre les politiques Snort 3 et Snort 2 lors de la transition entre les versions ou de la gestion des deux simultanément.

Procédure

- Étape 1** Accédez à **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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

Créez une nouvelle politique d'analyse de réseau qui fournit des versions Snort 2 et Snort 3 pour l'inspection et l'analyse du trafic réseau.

Toutes les politiques d'analyse de réseau existantes sont disponibles dans Firewall Management Center 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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Cliquez sur Créer une politique . |
| Étape 3 | Remplissez les champs Nom et Description . |
| Étape 4 | Sélectionnez une politique de base et cliquez sur Save (Enregistrer). |
-

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

Cette tâche vous permet de mettre à jour la configuration d'une politique d'analyse de réseau existante en modifiant ses propriétés telles que le nom, la description ou les paramètres de la politique de base.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Cliquez sur Edit (Modifier) pour changer le nom, la description, le mode d'inspection ou la politique de base. |

**Attention**

Obsolescence du mode de détection : à partir de la version 7.1.0 du centre de gestion, pour une politique d'analyse de réseau (NAP), le mode d'inspection de **détection** est obsolète et sera supprimé dans une prochaine version.

Le mode de **détection** était destiné à être utilisé comme mode de test afin que vous puissiez activer les inspections et voir comment elles se comportent dans votre réseau avant de le configurer pour abandonner le trafic, c'est-à-dire pour afficher le trafic qui serait abandonné.

Ce comportement est amélioré lorsque tous les abandons de l'inspecteur sont contrôlés par l'état de la règle et que vous pouvez définir chacun d'eux pour générer des événements. Ceci est fait pour les tester avant de configurer l'état de la règle pour abandonner le trafic. Comme nous avons maintenant un contrôle fin des pertes de trafic dans Snort 3, le mode de **détection** ne fait qu'ajouter plus de complexité au produit et n'est pas nécessaire, le mode de détection est donc obsolète.

Si vous modifiez une Politique d'analyse de réseau (NAP) de **détection** à **Prévention**, la Politique d'analyse de réseau (NAP) qui traite le trafic des incidents d'intrusion qui « sera abandonnée » est « abandonnée », et le trafic correspondant abandonnera le trafic de ces événements. Cela s'applique aux règles dont les GID ne sont pas 1 ou 3. Les GID 1 et 3 sont des règles de texte ou compilées (généralement fournies par Talos ou à partir de vos règles personnalisées ou importées), et tous les autres GID sont des inspections pour détecter des anomalies. Il s'agit de règles moins courantes à déclencher dans un réseau. Il est peu probable que le passage en mode de **prévention** ait un impact sur le trafic. Il vous suffit de désactiver la règle de prévention des intrusions qui s'applique au trafic abandonné et de la régler sur généré ou désactivé.

Nous vous recommandons de choisir **Prévention** comme mode d'inspection, mais si vous choisissez **Prévention**, vous ne pouvez pas revenir au mode **Détection**.

**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).

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

Cette tâche vous permet de localiser rapidement des inspecteurs dans l'interface de politique d'analyse de réseau en utilisant la fonctionnalité de recherche.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.

- 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 **Search** (Rechercher).
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.
-

Copier la configuration de l'inspecteur

Cette tâche décrit comment copier les configurations 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 **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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 **Copy to clipboard** (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 134

Personnaliser la politique d'analyse de réseau

Personnalisez la politique d'analyse de réseau pour adapter les configurations Snort 3 en fonction de vos exigences de sécurité.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.

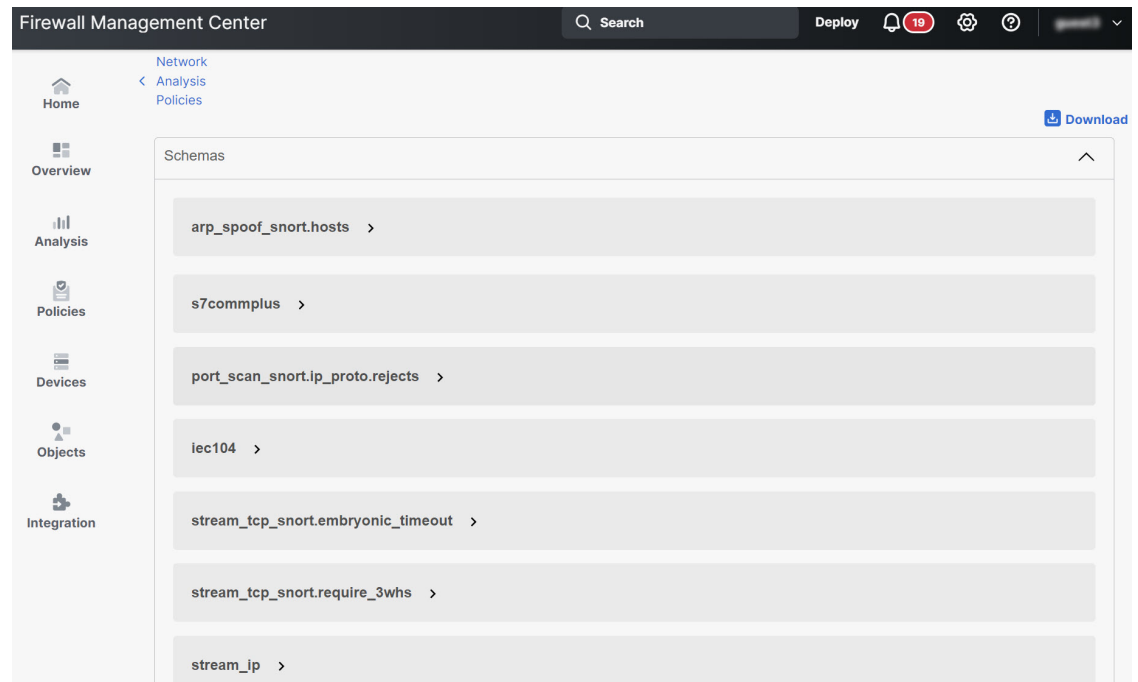
Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

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.

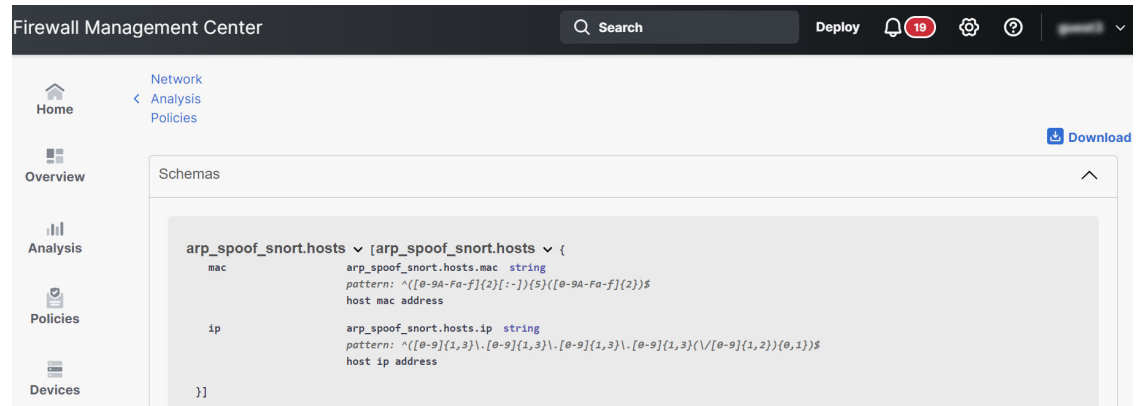
a) Cliquez sur **Télécharger le schéma** pour télécharger le fichier de schéma.

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. Ce fichier contient tous les renseignements sur la configuration de l'inspecteur.

- 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 Firewall Management Center. 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 charger le fichier de configuration remplacé.

Si vous avez choisi d'effectuer les modifications en ligne directement dans Firewall Management Center, 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 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 charger 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. Passez attentivement votre choix en revue avant d'utiliser cette option pour remplacer la configuration.

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 une sauvegarde de temps à autre lorsque vous remplacez la configuration de l'inspecteur.

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.

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 134](#) pour obtenir de plus amples renseignements.

Procédure

- Étape 1** Accédez à **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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, Firewall Management Center 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 134](#)
- [Annuler les modifications non enregistrées lors des modifications en ligne, à la page 140](#)
- [Rétablir la configuration remplacée à la configuration par défaut, à la page 141](#)
- [Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 144](#)

Annuler les modifications non enregistrées lors des modifications en ligne

Cette tâche vous permet de revenir sur toutes les modifications non enregistrées effectuées lors des modifications en ligne afin de remplacer la configuration d'un inspecteur, en revenant à la dernière valeur enregistrée.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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 X** 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 remplacée à la configuration par défaut](#), à la page 141

[Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 138

Afficher la liste des inspecteurs avec remplacements

Cette tâche vous permet d'identifier et de passer en revue tous les inspecteurs qui ont été remplacés dans la configuration de votre politique d'analyse de réseau.

Vous pouvez afficher une liste de tous les inspecteurs remplacés.

Procédure

-
- Étape 1** Accédez à **Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau)**.
- 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

[Rechercher un inspecteur dans la page des politiques d'analyse de réseau.](#), à la page 133

[Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 138

[Personnaliser la politique d'analyse de réseau](#), à la page 134

Rétablir la configuration remplacée à la configuration par défaut

Annulez les modifications que vous avez apportées pour remplacer la configuration par défaut d'un inspecteur, en restaurant les paramètres par défaut d'origine.

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 (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion > Network Analysis Policies (Politiques d'analyse de réseau) . |
| Étape 2 | Accédez à la version Snort 3 de la politique d'analyse de réseau. |
| Étape 3 | <p>Sous Inspecteurs, développez l'inspecteur requis pour lequel vous souhaitez rétablir la configuration remplacée.</p> <p>Les inspecteurs remplacés sont signalés par une icône jaune à côté de leur nom.</p> <p>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.</p> <p>Si vous n'avez apporté aucune modification à la configuration par défaut de l'inspecteur, cette option est désactivée.</p> |
| Étape 4 | Cliquez sur Revert (Rétablir) pour confirmer la décision. |
| Étape 5 | <p>Cliquez sur Enregistrer pour enregistrer vos modifications.</p> <p>Si vous ne souhaitez pas enregistrer les modifications, vous pouvez cliquer sur Annuler ou sur l'icône ✕ X.</p> |

Sujets connexes

[Annuler les modifications non enregistrées lors des modifications en ligne](#), à la page 140

[Personnaliser la politique d'analyse de réseau](#), à la page 134

[Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration](#), à la page 138

[Exemples de configuration de politique d'analyse de réseau personnalisée](#), à la page 144

Valider les politiques Snort 3

Cette tâche valide les politiques Snort 3 pour s'assurer qu'elles fonctionnent correctement avec les versions de périphérique actuelles et précédentes, en gérant les configurations spécifiques à la version et les paramètres d'inspection.

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

- La version actuelle de Firewall Management Center peut gérer plusieurs versions de Firewall Threat Defense.
- La version actuelle de Firewall Management Center prend en charge les configurations de politique d'analyse de réseau (NAP) qui ne sont pas applicables aux versions précédentes de Firewall 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 Firewall Threat Defense.
- Les modifications de configuration de la politique sont acceptées si elles sont valides pour la version actuelle et effectuées à l'aide du binaire Snort 3 et du schéma NAP actuels.
- Pour les versions précédentes de Firewall 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 la configuration non prise en charge sur la version donnée ne sera pas déployée, tandis 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.

- a) 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`. Cliquez sur **OK**.

- b) Cliquez sur **Enregistrer** pour enregistrer vos modifications.

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

- Étape 2** Cliquez sur le menu déroulant **Actions** dans la section **Snort 3 Version** (Version Snort 3) de la politique d'analyse de réseau.
- Étape 3** Sous **Upload** (Charger), vous pouvez cliquer sur **Overridden Configuration** (Configuration remplacée) pour charger le fichier JSON qui contient la configuration remplacée.

**Mise en garde**

Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas charger 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.

- **Merge inspector overrides (Fusionner les remplacements de l'inspecteur)** : le contenu du fichier chargé 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.
- **Replace inspector overrides (Remplacer les remplacements de l'inspecteur)** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier chargé.

**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 4** **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).
- 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.
 - Cliquez sur **OK** puis sur **Save** (Enregistrer) pour enregistrer la politique.
- Étape 5** 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).
- Cliquez sur **Add Rule** (ajouter une règle).
 - Configurez les conditions de la règle en cliquant sur les options que vous souhaitez ajouter.
 - 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.
 - Cliquez sur **Add** (ajouter).

- Étape 6** **Déploiement :** Dans la barre de menu Firewall Management Center, cliquez sur **Déployer**, puis sélectionnez **Déploiement**.
- Étape 7** Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.
- Recherche : Recherchez 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 cochant la case du périphérique, toutes les modifications pour ce périphérique qui y sont répertoriées sont transmises. Vous pouvez également utiliser **Policy Selection** (Sélection de politique) pour sélectionner des politiques ou des configurations individuelles à déployer tout en excluant les autres.
- Facultativement, utilisez **Afficher ou masquer la politique** pour afficher ou masquer sélectivement les politiques non modifiées connexes.
- Étape 8** Cliquez sur **Deploy** (déployer).
- Étape 9** 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 de réseau Snort 3 contient des inspecteurs ou des attributs non valides pour cette version Firewall Threat Defense. 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 Firewall Management Center. Consultez [Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 138](#).
- Utilisez le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez [Personnaliser la politique d'analyse de réseau, à la page 134](#).

Avant de choisir l'une de ces options, consultez tous les détails et exemples pour vous aider à définir les remplacements de politique d'analyse de réseau avec succès. Pour éviter les risques et les erreurs, lisez et comprenez les scénarios fournis ici.

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": []
  },
  "iecl04": {
    "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 Firewall 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**.

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.

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.

Générer des recommandations Snort 3

Recommandations de règles Snort 3

Les recommandations de règles Snort 3 sont une fonctionnalité de réglage de sécurité qui

- ajuste automatiquement votre politique de prévention des intrusions avec des règles spécifiques à l'environnement hôte,
- active des règles supplémentaires ou ajustent l'ensemble de règles actuel en désactivant les règles pour les vulnérabilités non présentes dans votre réseau, et
- utilise la base de données de l'hôte pour déterminer les règles qui s'appliquent à votre environnement.

Fonctionnement des recommandations de règles

Le centre de gestion crée une base de données d'hôtes sur votre réseau avec des détails tels que l'adresse IP, le nom de domaine, le système d'exploitation, les services, les utilisateurs et les applications client par découverte passive. En fonction de ces informations, le système fait correspondre les vulnérabilités à chaque hôte détecté. La fonctionnalité de recommandations utilise cette base de données d'hôte pour déterminer les règles qui s'appliquent à votre environnement.

Dans Snort 3, il existe quatre niveaux de sécurité, chacun correspondant à une politique Talos spécifique :

- Niveau 1 : connectivité sur la sécurité
- Niveau de sécurité 2 : équilibre entre sécurité et connectivité
- Niveau de sécurité 3 : la sécurité prime sur la connectivité
- Niveau de sécurité 4 : détection maximale

Cochez la case **Accept Recommendation to Disable Rules** (Accepter la recommandation pour désactiver les règles) pour désactiver les règles pour les vulnérabilités introuvables sur les hôtes de votre réseau. Utilisez cette option, uniquement si vous devez supprimer votre ensemble de règles en raison d'un nombre élevé d'alertes ou pour améliorer les performances de l'inspection.

Pour en savoir plus, consultez [Règles conseillées pour Secure Firewall](#), à la page 86.

Avantages

- En configurant les recommandations, vous pouvez adapter votre politique de prévention des intrusions pour détecter des types de menaces spécifiques à l'aide de règles spécifiques à l'environnement d'hôte.
- Les recommandations contribuent à un processus d'intervention plus efficace en réduisant les faux positifs et les fausses négations.

Exemple de scénario d'entreprise

Un exemple de scénario d'entreprise est une implémentation de la sécurité réseau qui montre comment un grand réseau d'entreprise utilise Snort 3 comme système principal de détection et de prévention des intrusions

pour améliorer les capacités de réponse aux incidents par le biais de la génération de règles basées sur les vulnérabilités et de l'optimisation des politiques de prévention des intrusions.

Détails du scénario d'exploitation

Dans ce scénario, un grand réseau d'entreprise adopte des mesures de sécurité réseau robustes dans un paysage des menaces en pleine évolution. L'équipe de sécurité souhaite améliorer ses capacités de réponse aux incidents en générant des recommandations ou des ensembles de règles en fonction des vulnérabilités détectées dans le réseau d'hôte. Cela les aide à optimiser leurs politiques de prévention des intrusions, veillant ainsi au réseau plus efficacement.

Bonnes pratiques

- Vous devez avoir des données d'hôte précises et de haute qualité.
En raison de la nature passive de la découverte du réseau, vos appareils de défense contre les menaces doivent être placés aussi près que possible de vos hôtes protégés. Cela permet aux appareils de défense contre les menaces de surveiller le trafic réseau à destination et en provenance de ces hôtes, ce qui vous fournit des données précises sur les applications, les services et les vulnérabilités de votre réseau.
- Les périphériques doivent avoir une visibilité sur les flux de trafic est-ouest ainsi que sur les flux de trafic nord-sud pour créer un profil d'hôte précis.
- Vous pouvez créer une tâche planifiée pour mettre à jour automatiquement les recommandations.

Conditions préalables à la génération de recommandations

- 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

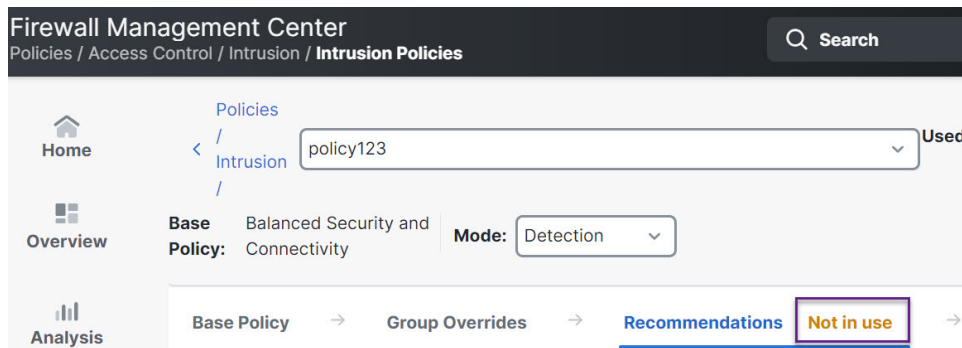
Générer des recommandations Snort 3

Générez et appliquez des recommandations de règles Snort 3 pour optimiser votre politique de prévention des intrusions en fonction de la configuration de votre réseau et des exigences de sécurité.

Les recommandations Snort 3 vous aident à configurer des politiques de prévention des intrusions avec des règles adaptées à votre environnement réseau. Le système analyse vos réseaux protégés et suggère les niveaux de sécurité et les configurations de règles appropriés.

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Choisissez Politiques (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion. |
| Étape 2 | Cliquer sur le bouton Snort 3 Version (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 **Cisco Recommended Rules** (Règles conseillées par Cisco), vous pouvez définir le niveau de sécurité.

Cisco Recommended Rules

Security Level (Click to select)



☐ Accept Recommendation to Disable Rules ⓘ

No Impact— No new rules will be enabled and no existing rules will be disabled.
To increase protections, please select a higher Security Level.

Protected Networks ⓘ

 Add +

Cancel

Generate

Generate and Apply

Étape 4 Cliquez pour sélectionner le niveau de sécurité.

Étape 5 (Facultatif) Cochez la case **Accept Recommendation to Disable Rules** (Accepter la recommandation pour désactiver les règles) pour désactiver les règles écrites pour les vulnérabilités introuvables sur les hôtes de votre réseau.

Utilisez cette option, uniquement si vous devez supprimer votre ensemble de règles en raison d'un nombre élevé d'alertes ou pour améliorer les performances de l'inspection.

Étape 6 Dans la liste déroulante **Protected Networks** (Réseaux protégés), choisissez les objets réseau qui doivent être inspectés par les recommandations. Par défaut, tous les réseaux IPv4 ou IPv6 sont sélectionnés si vous ne faites aucune sélection.

Cliquez sur **Add +** (Ajouter) pour créer un nouvel objet réseau de type **Host** (Hôte) ou **Network** (Réseau) et cliquez sur **Save** (Enregistrer).

Étape 7 Générer et appliquer les recommandations :

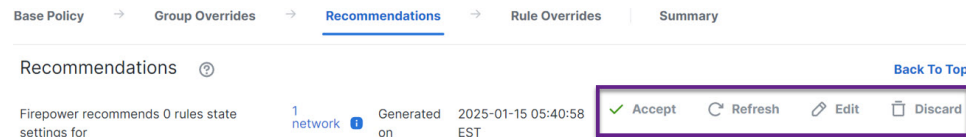
- **Generate** (Générer) : génère les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous **Recommended Rules (Not in use)** (Règles recommandées [non utilisées]).
- **Generate and Apply** (Générer et appliquer) : génère et applique les recommandations pour une politique de prévention des intrusions. Cette action répertorie les règles sous **Recommended Rules (Not in use)** (Règles recommandées [non utilisées]).

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.

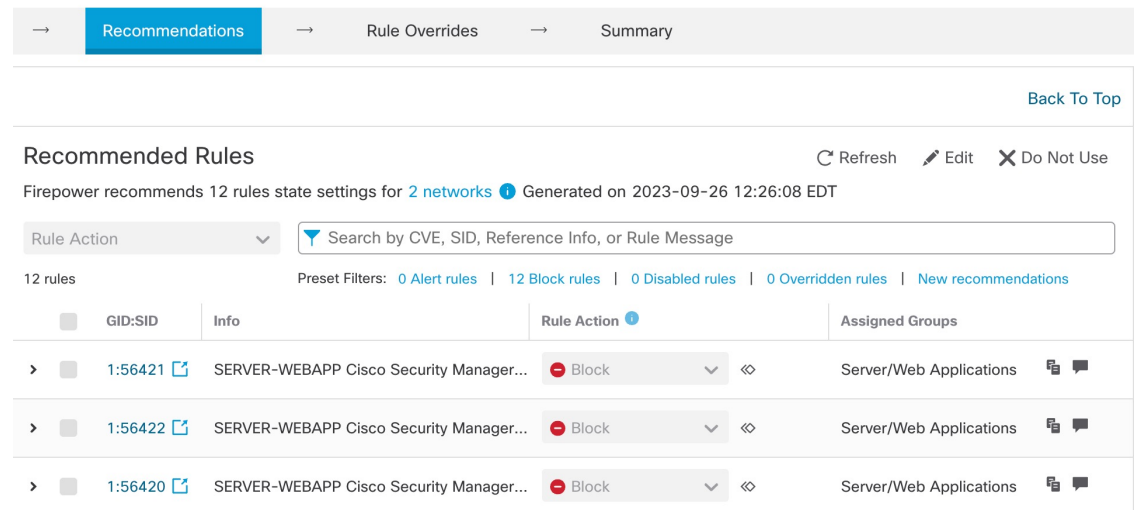
Étape 8

Vérifiez les recommandations, puis appliquez-les en conséquence :

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



Sous **All Rules** (Toutes les règles), la section Recommended Rules (Règles recommandées) affiche les règles recommandées.



Étape 9

Pour utiliser efficacement les recommandations, elles doivent être mises à jour périodiquement. Suivez ces étapes :

1. Choisissez **Système** (🔍) > **Tools (Outils)** > **Scheduling (Planification)**.
2. Cliquez sur **Add Task** (Ajouter une tâche).
3. Choisissez **Cisco Recommended Rules** (Règles conseillées par Cisco) dans la liste déroulante **Job Type** (Type de tâche).
4. Veuillez mettre à jour les champs obligatoires, au besoin.

New Task

Job Type Cisco Recommended Rules ▾

(Cisco Recommended Rules must first be configured in the selected [policies](#))Schedule task to run ☐ Once ☒ Recurring

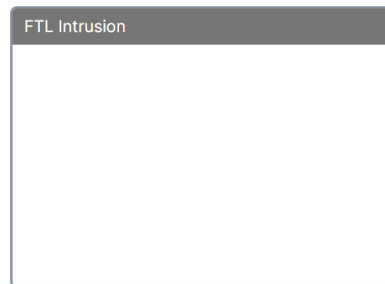
Start On January ▾ 15 ▾ 2025 ▾ America/New York

Repeat Every 1 ▾ ☐ Hours ☐ Days ☒ Weeks ☐ Months

Run At 10:00 ▾ Pm ▾

Repeat On ☒ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Job Name Update recommendations

Policies ☒ All Policies

5. Cliquez sur **Save** (Enregistrer).

Prochaine étape

Déployer les modifications de configuration Reportez-vous à [Déploiement des modifications de configuration, à la page 36](#)



CHAPITRE 6

Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

Ce chapitre décrit comment configurer les paramètres avancés pour l'analyse de réseau et les politiques de prévention des intrusions.

- Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion, à la page 161
- Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion, à la page 162
- Exigences et conditions préalables pour les paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion, à la page 162
- Inspection des paquets qui passent avant que le trafic ne soit identifié, à la page 163
- Paramètres avancés pour les politiques d'analyse de réseau, à la page 165

Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

Les paramètres de contrôle d'accès avancé sont des configurations de détection et de prévention des intrusions qui

- nécessitent une expertise spécifique pour la configuration,
- ne nécessitent généralement que peu ou aucune modification, et
- ne sont pas communes à tous les déploiements.

Compatibilité des versions



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

Les paramètres de contrôle d'accès avancé sont des configurations de détection et de prévention des intrusions qui

- nécessitent une expertise spécifique pour la configuration,
- ne nécessitent généralement que peu ou aucune modification, et
- ne sont pas communes à tous les déploiements.

Compatibilité des versions



Remarque

Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Exigences et conditions préalables pour les paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

Cette référence présente les exigences du système, les conditions préalables aux logiciels et les dépendances de configuration nécessaires pour mettre en œuvre les paramètres de contrôle d'accès avancé pour l'analyse du réseau et les politiques de détection d'intrusion dans les environnements Cisco Secure Firewall.

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles de l'utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Inspection des paquets qui passent avant que le trafic ne soit identifié

L'inspection des paquets qui passent avant que le trafic ne soit identifié est un processus de sécurité réseau qui

- permet à quelques paquets de passer initialement pour l'établissement de la connexion et l'identification du trafic,
- permet à des fonctionnalités telles que le filtrage d'URL, la détection des applications, la limitation de débit, et le contournement intelligent des applications de fonctionner correctement, et
- nécessite une configuration explicite dans les stratégies de contrôle d'accès pour inspecter et bloquer ces paquets initiaux et générer des incidents à leur sujet.

Exigences de configuration

Vous devez configurer explicitement votre politique de contrôle d'accès pour inspecter ces paquets, les empêcher d'atteindre leur destination et générer des événements.

Dès que le système identifie la règle de contrôle d'accès ou l'action par défaut qui doit gérer la connexion, les paquets restants de la connexion sont gérés et inspectés en conséquence.

Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic

L'action par défaut spécifiée pour une politique de contrôle d'accès N'EST PAS appliquée à ces paquets.

Utilisez plutôt les lignes directrices suivantes pour choisir une valeur pour la **politique de prévention des intrusions utilisée avant la détermination de la règle de contrôle d'accès** dans les paramètres avancés de la stratégie de contrôle d'accès.

- Vous pouvez choisir une politique de prévention des intrusions créée par le système ou personnalisée. Par exemple, vous pouvez sélectionner **Sécurité et connectivité équilibrées**.
- Pour des raisons de performance, sauf si vous avez une bonne raison de procéder autrement, ce paramètre doit correspondre aux actions par défaut définies pour votre politique de contrôle d'accès.
- Si votre système n'effectue pas d'inspection des intrusions (par exemple, dans un déploiement de découverte uniquement), sélectionnez **No Rules Active** (Aucune règle active). Le système n'inspectera pas ces paquets initiaux et ils seront autorisés à passer.
- Par défaut, ce paramètre utilise l'ensemble de variables par défaut. Assurez-vous qu'il convient à vos besoins. Pour en savoir plus, consultez [Ensembles de variables](#).
- La politique d'analyse de réseau associée à la première règle d'analyse de réseau correspondante prétraite le trafic pour la politique que vous sélectionnez. S'il n'y a aucune règle d'analyse de réseau ou qu'aucune règle ne correspond, la politique d'analyse de réseau par défaut est utilisée.

Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic

Cette tâche explique comment préciser le comportement du système pour le trafic réseau pendant la période précédant l'identification du trafic.



Remarque

Ce paramètre est parfois appelé *politique de prévention des intrusions par défaut*. (à ne pas confondre avec l'action par défaut pour une politique de contrôle d'accès.)



Mise en garde

Modification du nombre total de politiques de prévention des intrusions utilisées par une politique de contrôle d'accès redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Selon la façon dont le périphérique attribué traite le trafic, celui-ci peut être abandonné durant l'interruption ou passer sans inspection supplémentaire. Vous pouvez ajouter une politique de prévention des intrusions qui n'est pas actuellement utilisée ou supprimer la dernière instance d'une politique de prévention des intrusions. Les politiques de prévention des intrusions sont utilisées dans les règles de contrôle d'accès, comme action par défaut ou comme politique de prévention des intrusions par défaut.

Before you begin

Passez en revue les bonnes pratiques pour ces paramètres. Consultez [Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic](#), à la page 163.

Suivez ces étapes pour préciser une politique pour gérer les paquets qui passent avant l'identification du trafic

Procédure

- Étape 1** Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé), puis sur **Modifier** (✎) à côté de la section **Network Analysis** (Analyse du réseau) et **Intrusion Policies** (Politiques de prévention des intrusions).

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.
- Étape 2** Sélectionnez une politique de prévention des intrusions dans la liste déroulante **Politique de prévention des intrusions utilisée avant la détermination de la règle de contrôle d'accès**.

Si vous choisissez une politique créée par l'utilisateur, vous pouvez cliquer sur **Modifier** (✎) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.
- Étape 3** Vous pouvez également sélectionner un autre ensemble de variables dans la liste déroulante **Intrusion Policy Variable Set** (ensemble de variables de politique de prévention des intrusions). Vous pouvez également sélectionner **Modifier** (✎) à côté de l'ensemble de variables pour créer et modifier des ensembles de variables. Si vous ne modifiez pas l'ensemble de variables, le système utilise un ensemble par défaut.
- Étape 4** Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

[Ensembles de variables](#)

Paramètres avancés pour les politiques d'analyse de réseau

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

Concepts de configuration avancée

Ce prétraitement de trafic a lieu après la mise en correspondance Security Intelligence et le déchiffrement du trafic, mais avant que les politiques de prévention des intrusions n'inspectent les paquets en détail. Par défaut, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique d'analyse de réseau par défaut.



Astuces

La politique d'analyse du réseau de sécurité et de connectivité équilibrée fournie par le système et la politique d'intrusion de sécurité et de connectivité équilibrée fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles d'intrusion. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention des intrusions régit principalement les règles de prévention des intrusions.

Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut. Si vous êtes un utilisateur avancé avec un déploiement complexe, vous pouvez créer plusieurs politiques d'analyse de 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.

Pour ce faire, ajoutez des *règles d'analyse de réseau* personnalisées à votre politique de contrôle d'accès. Une règle d'analyse de réseau est simplement un ensemble de configurations et de conditions qui spécifient la manière dont vous traitez le trafic qui correspond à ces conditions. Vous pouvez créer et modifier les règles d'analyse de réseau dans les options avancées d'une politique de contrôle d'accès existante. Chaque règle n'appartient qu'à une seule politique.

Chaque règle comporte :

- un ensemble de conditions de règles qui identifient le trafic spécifique que vous souhaitez prétraiter
- une politique d'analyse de réseau associée que vous souhaitez utiliser pour prétraiter le trafic qui répond à toutes les conditions des règles.

Lorsque vient le temps pour le système de prétraiter le trafic, il fait correspondre les paquets aux règles d'analyse de réseau 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.

Définir la politique d'analyse du réseau par défaut

La définition d'une politique d'analyse de réseau par défaut établit le comportement de prétraitement de référence pour l'analyse du trafic réseau au sein de votre politique de contrôle d'accès.

Vous pouvez choisir une politique créée par le système ou par l'utilisateur.



Remarque

Si vous désactivez un préprocesseur, mais que le système doit évaluer les paquets prétraités par rapport à une règle de prévention des intrusions ou de préprocesseur activée, le système active et utilise automatiquement le préprocesseur, bien qu'il reste désactivé dans l'interface Web de la politique d'analyse de réseau. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**. Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** faire attention et autoriser les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet à se compléter.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Modifier** (✎) à côté de la section Network Analysis and Intrusion Policies (Analyse de réseau et politiques d'intrusion).

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.

Étape 2 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 **Modifier** (✎) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.



Mise en garde

Modification du nombre total de politiques d'analyse de réseau utilisées par une stratégie de contrôle d'accès redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Selon la façon dont le périphérique attribué traite le trafic, celui-ci peut être abandonné durant l'interruption ou passer sans inspection supplémentaire. Vous modifiez le nombre total de politiques d'analyse de réseau en ajoutant une politique qui n'est pas utilisée actuellement ou en supprimant la dernière instance d'une politique d'analyse de réseau. Vous pouvez utiliser une politique d'analyse de réseau avec des règles d'analyse de réseau ou comme politique d'analyse de réseau par défaut.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

[Limites des politiques personnalisées](#)

Règles d'analyse du réseau

Une règle d'analyse de réseau est un composant de configuration de prétraitement qui

- adapte les configurations de prétraitement au trafic réseau dans les paramètres avancés de la stratégie de contrôle d'accès,
- fait correspondre les paquets en ordre croissant par numéro de règle, en commençant par 1, et
- prétraite le trafic selon la première règle où toutes les conditions correspondent.

Conditions des règles d'analyse du réseau et mise en correspondance

Vous pouvez ajouter des conditions de zone, de réseau et de balise VLAN à une règle. Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère. Par exemple, une règle avec une condition de réseau, mais aucune condition de zone évalue le trafic en fonction de son adresse IP de source ou de destination, quelle que soit son interface d'entrée ou de sortie. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut.

Conditions des règles de politique d'analyse de réseau

Les conditions de règles de politique d'analyse de réseau sont des paramètres de configuration qui vous permettent d'affiner votre politique d'analyse de réseau pour cibler les utilisateurs et les réseaux que vous souhaitez contrôler.

Sujets connexes

[Conditions des règles de zone de sécurité](#), à la page 167

[Conditions des règles de réseau](#), à la page 168

[Conditions des règles des balises VLAN](#), à la page 168

Conditions des règles de zone de sécurité

Une condition de règle de zone de sécurité est un mécanisme de contrôle du trafic réseau qui

- segmente votre réseau pour vous aider à gérer, classer et déchiffrer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.
- contrôle ou déchiffre le trafic en fonction de ses zones de sécurité source et de destination, et
- exige que toutes les interfaces d'une zone soient du même type (toutes en ligne, passives, commutées ou routées).

Correspondance du trafic de condition de zone

Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, réduisez le nombre de critères de correspondance, en particulier pour les périmètres de sécurité, les objets réseau et les objets portuaires. Lorsque vous précisez plusieurs critères, le système doit être en *correspondance* avec l'ensemble des contenus du critères que vous précisez.



Astuces

Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions de zone de sécurité dans les environnements multidomaine

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Une condition de réseau est un critère de correspondance de trafic qui

- contrôle ou déchiffre le trafic en fonction des adresses IP source et de destination à l'aide d'en-têtes de paquets internes,
- permet aux administrateurs de spécifier des adresses IP exactes ou des blocs pour l'application des politiques granulaires, et
- peut être créée à l'aide d'objets réseau prédéfinis ou en saisissant manuellement des adresses IP ou des blocs d'adresses.

Restrictions des conditions des règles de réseau

Dans la mesure du possible, réduisez le nombre de critères de correspondance, en particulier pour les périmètres de sécurité, les objets réseau et les objets portuaires. Lorsque vous précisez plusieurs critères, le système doit être en *correspondance* avec l'ensemble des contenus du critères que vous précisez.



Remarque

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

Conditions des règles des balises VLAN

Les conditions de règle des balises VLAN sont des mécanismes de filtrage qui

- contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés)

- utilisent la balise VLAN la plus interne pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus externe, et
- s'appliquent uniquement aux ensembles en ligne et ne correspondent pas au trafic sur les interfaces de pare-feu.

Détails de la configuration des conditions de règle de balise VLAN



Remarque

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

Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez cette prise en charge de Q-in-Q :

- Firewall Threat Defense sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Firewall Threat Defense Pour tous les autres modèles :
 - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
 - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

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

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

Configuration des règles d'analyse du réseau

Les règles d'analyse de réseau vous permettent de préciser quelle politique d'analyse de réseau doit prétraiter le trafic qui correspond à des conditions spécifiques, fournissant un contrôle fin sur l'inspection du trafic avant la détection des intrusions.

Les règles d'analyse de réseau sont configurées dans les paramètres avancés d'une politique de contrôle d'accès. Vous pouvez créer des règles personnalisées pour appliquer différentes politiques d'analyse de réseau en fonction des conditions de trafic telles que la source, la destination, les ports ou les applications.

Before you begin

Suivez les étapes suivantes pour configurer les règles d'analyse du réseau :

Procédure

Étape 1

Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Modifier** (✎) à côté de la section Network Analysis and Intrusion Policies (Analyse de réseau et politiques d'intrusion).

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.

**Astuces**

Cliquez sur **Network Analysis Policy List** (Liste des politiques d'analyse de réseau) pour afficher et modifier les politiques d'analyse de réseau personnalisées existantes.

- Étape 2** À côté de **Network Analysis Rules** (règles d'analyse de réseau), cliquez sur l'énoncé qui indique combien de règles personnalisées vous avez.
- Étape 3** Cliquez sur **Add Rule** (ajouter une règle).
- Étape 4** Configurez les conditions de la règle en cliquant sur les conditions que vous souhaitez ajouter.
- Étape 5** 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.

Cliquez sur **Modifier** () pour modifier une politique personnalisée dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

**Mise en garde**

Modification du nombre total de politiques d'analyse de réseau utilisées par une politique de contrôle d'accès redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Selon la façon dont le périphérique attribué traite le trafic, celui-ci peut être abandonné durant l'interruption ou passer sans inspection supplémentaire. Vous modifiez le nombre total de politiques d'analyse de réseau en ajoutant une politique qui n'est pas utilisée actuellement ou en supprimant la dernière instance d'une politique d'analyse de réseau. Vous pouvez utiliser une politique d'analyse de réseau avec des règles d'analyse de réseau ou comme politique d'analyse de réseau par défaut.

- Étape 6** Cliquez sur **Add** (ajouter).

Prochaine étape

- Déployer les changements de configuration.

Gestion des règles d'analyse du réseau

Les règles d'analyse du réseau vous permettent de contrôler le prétraitement du trafic en définissant des conditions et des configurations spécifiques qui déterminent les méthodes de gestion du trafic.

Une règle d'analyse de réseau est simplement un ensemble de configurations et de conditions qui spécifient la manière dont vous traitez le trafic qui correspond à ces conditions. Vous pouvez créer et modifier les règles d'analyse de réseau dans les options avancées d'une politique de contrôle d'accès existante. Chaque règle n'appartient qu'à une seule politique.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé), puis sur **Modifier** () à côté de la section Politiques de prévention des intrusions et d'analyse de réseau.

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.

Étape 2 À côté de **Network Analysis Rules** (règles d'analyse de réseau), cliquez sur l'énoncé qui indique combien de règles personnalisées vous avez.

Étape 3 Modifier vos règles personnalisées. Vous avez les options suivantes :

- Pour modifier les conditions d'une règle ou la politique d'analyse de réseau appelée par la règle, cliquez sur **Modifier** () à côté de la règle.
- Pour modifier l'ordre d'évaluation d'une règle, cliquez sur la règle et faites-la glisser jusqu'à l'emplacement approprié. Pour sélectionner plusieurs règles, utilisez la touche Maj + Ctrl.
- Pour supprimer une règle, cliquez sur **Supprimer** () à côté de la règle.



Astuces

Cliquez avec le bouton droit sur une règle pour afficher un menu contextuel qui vous permet de couper, de copier, de coller, de modifier, de supprimer et d'ajouter de nouvelles règles d'analyse de réseau.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

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.