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

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

Présentation du réglage des règles de prévention des intrusions

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

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

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

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

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

Règles de prévention des intrusions

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

Une politique de prévention des intrusions contient :

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

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

Tableau 1 : Règles de prévention des intrusions

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

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

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

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

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

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

Règles personnalisées dans Snort 3

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

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

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

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

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

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

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

Remarque

- Les règles personnalisées Snort 3 ne peuvent pas être modifiées. Assurez-vous que les règles personnalisées comportent un message de classification valide pour `classtype` dans le texte de la règle. Si vous importez une règle sans classification ou avec une mauvaise classification, supprimez et recréez la règle.
- Vous pouvez créer des règles de prévention des intrusions personnalisées dans Snort 3. Cependant, la prise en charge du réglage et de la résolution de problèmes liés à ces règles n'est pas disponible pour le moment.
- Le paramètre *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*. Toutefois, le niveau de priorité de certains *classtypes* sur l'appareil Threat Defense ne correspond pas aux niveaux de priorité des *classtypes* Snort en source ouverte mentionnés dans la documentation Snort. Par exemple, *tcp-connection* a une priorité de 4 dans Snort en source ouverte, tandis qu'une priorité de 3 lui est attribuée sur l'appareil Threat Defense.

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 14.

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

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

Procédure

Étape 1 Choisissez **Policies (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 :

- 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 pour en savoir plus sur l'exécution de ces tâches.

Action de règle de prévention des intrusions

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

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

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

Options d'actions liées aux règles de prévention des intrusions

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

Alerte

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

Bloquer

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

Désactiver

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

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

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

Définir une action de règle de prévention des intrusions

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

Procédure

Étape 1 Choisissez **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.

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 pour plus d'informations sur les différentes actions de règle.

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

Prochaine étape

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

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

L'importance d'un incident d'intrusion peut être fonction de sa fréquence ou de l'adresse IP source ou de destination. Dans certains cas, vous pouvez ne pas vous soucier d'un événement tant qu'il ne se produit pas un certain nombre de fois. Par exemple, vous pourriez ne pas être concerné si quelqu'un tente de se connecter

à un serveur avant d'échouer un certain nombre de fois. Dans d'autres cas, vous n'aurez peut-être besoin que de quelques occurrences pour savoir qu'il y a un problème généralisé. Par exemple, si une attaque DoS est lancée contre votre serveur Web, vous n'aurez peut-être besoin de voir que quelques occurrences d'un incident d'intrusion pour savoir que vous devez corriger la situation. Le fait de constater des centaines d'événements identiques ne fait que submerger votre système.

Seuils de incidents d'intrusion

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

Définir les seuils d'incidents d'intrusion

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

Tableau 2 : Options de seuil

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

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

Tableau 3 : 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 4 : Options de durée/instance de seuil

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

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

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

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

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

Procédure

Étape 1 Choisissez **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 :

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

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

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

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

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

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

Prochaine étape

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

Afficher et supprimer les seuils d'incidents d'intrusion

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

Procédure

Étape 1 Choisissez **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

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

Configuration de la suppression des politiques de prévention des intrusions

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

Types de suppression des politiques de prévention des intrusions

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

Astuces Vous pouvez ajouter des suppressions à partir de la vue de paquets d'un incident d'intrusion. Vous pouvez également accéder aux paramètres de suppression via la colonne **Configuration de l'alerte** de la page d'édition des règles d'intrusion (**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

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

Avant de commencer

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

Procédure

Étape 1 Choisissez **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 **Aucun** dans la colonne Alert Configuration (Configuration des alertes) de la règle de prévention des intrusions.

Étape 4 Cliquez sur **Modifier** ( ).

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

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

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

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

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

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

Prochaine étape

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

Afficher et supprimer les conditions de suppression

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

Procédure

Étape 1 Choisissez **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

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

Ajouter des commentaires sur la règle de prévention des intrusions

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

Procédure

Étape 1 Choisissez **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).

Astuces

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

Prochaine étape

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

Conversion des règles personnalisées de Snort 2 vers Snort 3

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

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

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

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

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

Procédure

Étape 1 Choisissez **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) (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 FMC en tant que règles personnalisées Snort 3.
- (Convertir et télécharger) (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 14.

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

Prochaine étape

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

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

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 verte**Versions Snort synchronisées** ( ). Cela indique qu'il n'y a aucune règle personnalisée à convertir.

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

Étape 5 Choisissez :

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

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

Prochaine étape

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

Ajouter des règles personnalisées aux groupes de règles

Le téléversement de règles personnalisées dans le FMC 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 Glissez et déposez le fichier `.txt` ou `.rules` qui contient les règles personnalisées de Snort 3 que vous avez créées.

Étape 5 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 6 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 7 Effectuez l'une des opérations suivantes :

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

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

Étape 8 Cliquez sur **Next** (suivant).

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

Étape 9 Cliquez sur **Finish** (terminer).

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

Prochaine étape

- Le téléversement de règles personnalisées dans le FMC 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 15. Pour en savoir plus sur l'activation des règles personnalisées, consultez Gérer les règles personnalisées dans Snort 3, à la page 16.
- Déployez les modifications de configuration; voir Déployer les modifications de configuration.

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

Les règles personnalisées qui sont téléversées dans le système doivent être activées dans une politique de prévention des intrusions pour appliquer ces règles au trafic. Après avoir téléversé les règles personnalisées sur FMC, 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

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

Gérer les règles personnalisées dans Snort 3

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

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

Procédure

Étape 1 Choisissez **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

Déployez les modifications sur le périphérique. Consultez, Déployer les modifications de configuration.

Supprimer des règles personnalisées

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

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

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

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

Prochaine étape

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

Supprimer le groupe de règles

Avant de commencer

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

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 :

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

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

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

Prochaine étape

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

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.