Les gens du pays faits sur commande reniflent des règles sur un système de Cisco FireSIGHT

Contenu

Introduction

Une règle locale faite sur commande sur un système de FireSIGHT est une norme faite sur commande reniflent la règle que vous importez dans un format de fichier texte ASCII d'un ordinateur local. Un système de FireSIGHT te permet pour importer des règles locales utilisant l'interface web. Les étapes pour importer des règles locales sont très simples. Cependant, pour écrire une règle locale optimale, un utilisateur exige la connaissance approfondie sur Snort et des protocoles de réseau.

Le but de ce document est de te fournir des conseils et de l'aide d'écrire une règle locale faite sur commande. Les instructions sur créer des règles locales sont disponibles dans le *manuel d'utilisation de renifler,* qui est disponible chez snort.org. Cisco recommande que vous téléchargiez et lisiez le manuel d'utilisation avant que vous écriviez une règle locale faite sur commande.

> Remarque: Les règles fournies dans un module de la mise à jour de règle de Sourcefire (SRU) sont créées et testées par les renseignements de sécurité et l'organisme de recherche de Cisco Talos, et prises en charge par le centre d'assistance technique Cisco (TAC). Cisco TAC ne fournit pas l'assistance sur l'écriture ou accorder une règle locale faite sur commande, cependant si vous éprouvez n'importe quelles questions avec la fonctionnalité d'importation de règle de votre système de FireSIGHT, contactez s'il vous plaît Cisco TAC.

> **Avertissement** : Une règle locale faite sur commande mal écrite peut affecter l'interprétation d'un système de FireSIGHT qui peut mener à la dégradation d'interprétation du tout le réseau. Si vous éprouvez n'importe quels problèmes de performance dans votre réseau, et il

y a quelques gens du pays faits sur commande reniflent des règles activées sur votre système de FireSIGHT, Cisco vous recommande pour désactiver ces règles locales.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur les règles Snort et le système de FireSIGHT.

Composants utilisés

Les informations sur ce document sont basées sur des ces matériel et versions de logiciel :

- Le centre de Gestion de FireSIGHT (également connu sous le nom de centre de la défense)
- Version de logiciel 5.2 ou plus tard

Fonctionner avec les règles locales faites sur commande

Règles de gens du pays d'importation

Avant que vous commenciez, vous devez s'assurer que les règles dans le fichier ne contiennent aucun caractère d'échappement. L'importation de règle a besoin de toutes les règles faites sur commande d'être importé utilisant encoder ASCII ou d'UTF-8.

La procédure suivante explique comment importer des règles standard locales des textes d'un ordinateur local :

1. Accédez à la page d'**éditeur de règle** en naviguant vers les **stratégies > l'éditeur d'intrusion > de règle**.

2. **Règles d'importation de** clic. La page de **mises à jour de règle** paraît.

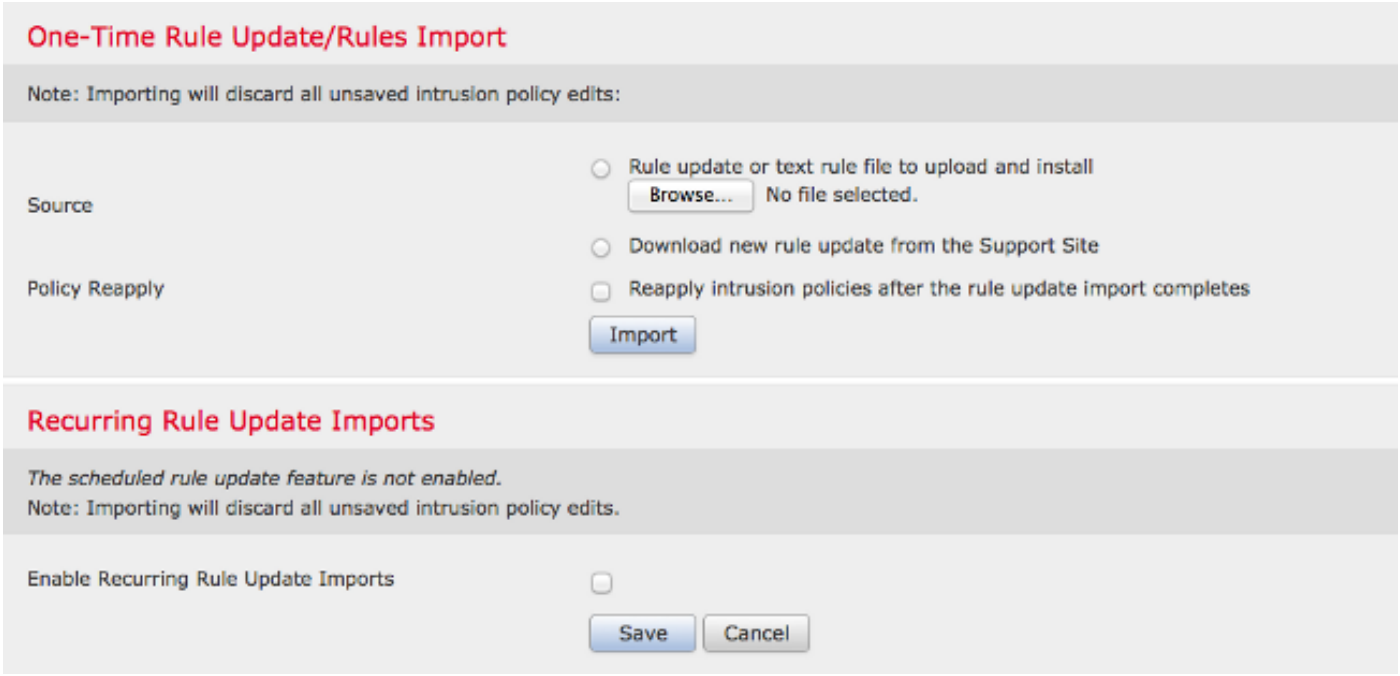


Figure : Un tir d'écran de la règle met à jour la page

3. Sélectionnez la **mise à jour de règle ou le fichier de règle des textes au télécharger et installer** et le clic **parcourent** pour sélectionner le fichier de règle.

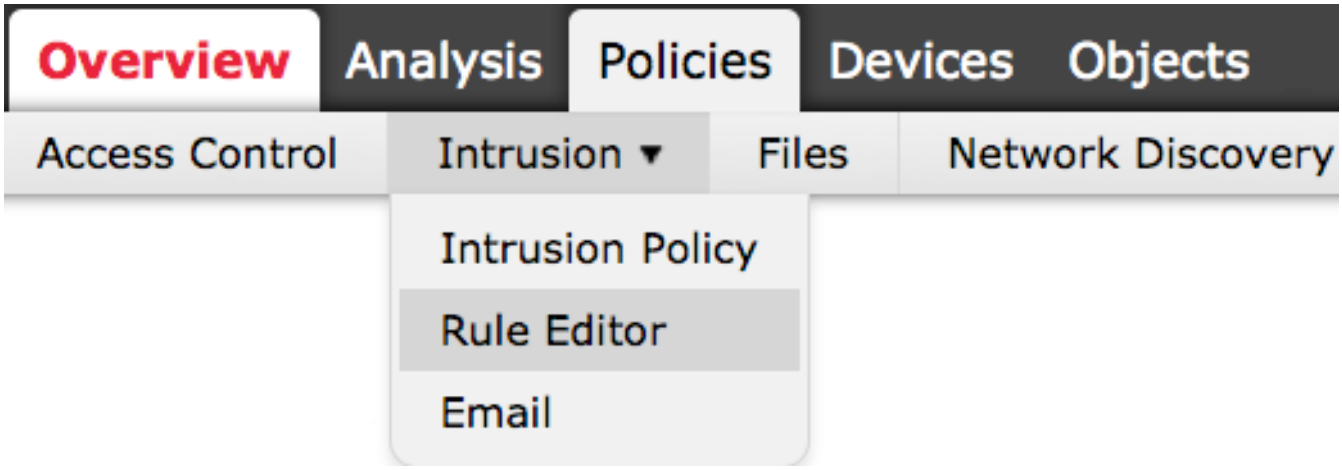
> Remarque: Toutes les règles téléchargées sont enregistrées dans la catégorie **locale de règle**.

4. Cliquez sur **Import**. Le fichier de règle est importé.

> **Attention** : Les systèmes de FireSIGHT n'utilisent pas le nouvel ensemble de règles pour l'inspection. Pour lancer une règle locale, vous devez l'activer dans la stratégie d'intrusion, et puis appliquez la stratégie.

Règles de gens du pays de vue

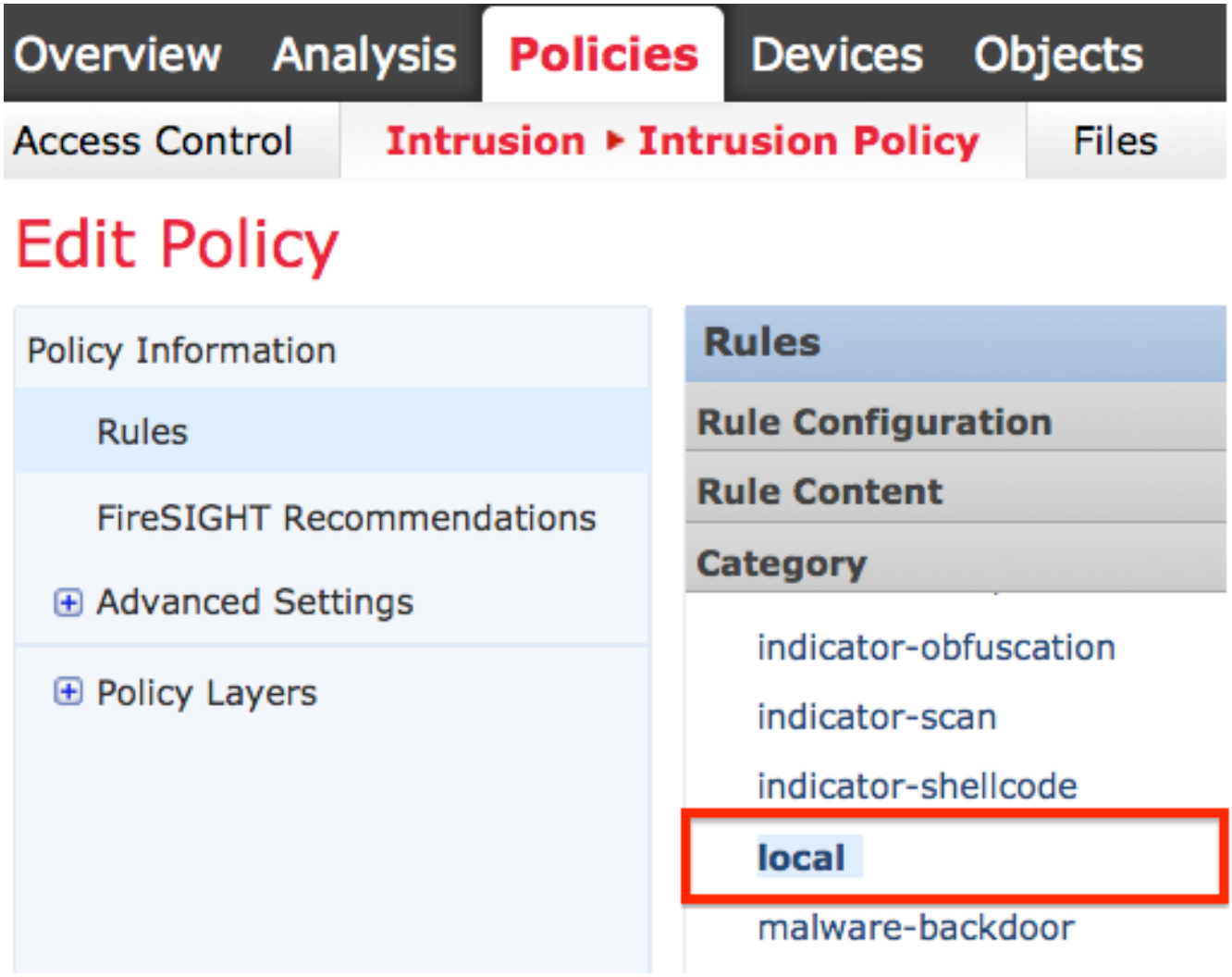
- Pour visualiser le nombre de révision pour une règle locale en cours, naviguez vers la page d'**éditeur de règle** (**stratégies > éditeur d'intrusion >** de **règle**).



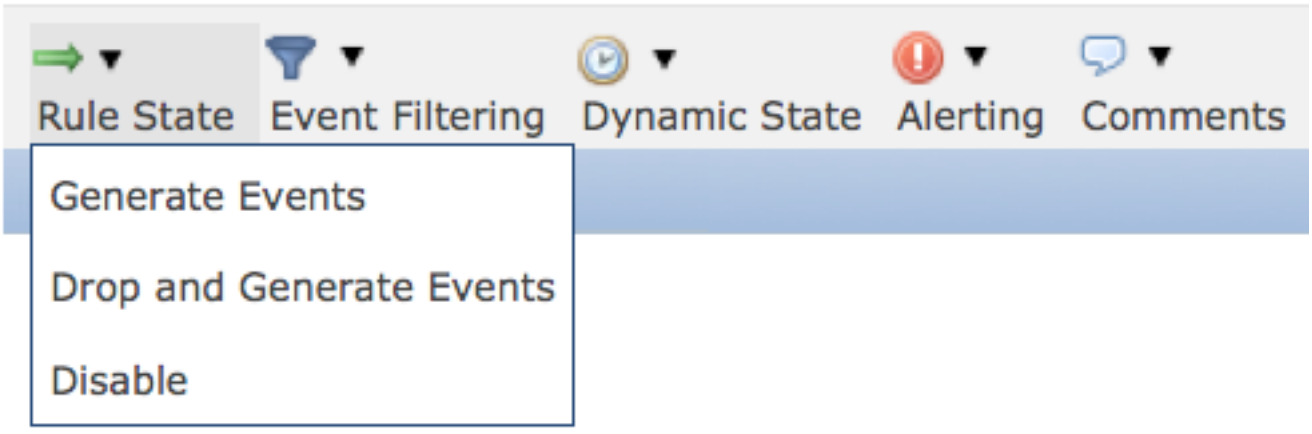
- Dans la page d'éditeur de règle, cliquez sur en fonction la catégorie **locale de règle** pour développer le répertoire, puis cliquez sur Edit à côté de la règle.
- Toutes les règles locales importées sont automatiquement enregistrées dans la catégorie **locale de règle**.

Règles de gens du pays d'enable

- Par défaut, le système de FireSIGHT place les règles locales dans un état handicapé. Vous devez manuellement placer l'état de règles locales avant que vous puissiez les utiliser dans votre stratégie d'intrusion.
- Afin d'activer une règle locale, naviguez vers la page d'éditeur de stratégie (**stratégies > intrusion > stratégie d'intrusion**). **Règles** choisies dans le panneau gauche. Sous la **catégorie**, **gens du pays** choisis. Toutes les règles locales devraient apparaître, si disponibles.



- Après avoir sélectionné les règles locales désirées, sélectionnez un état pour les règles.



- Une fois l'état de règle est sélectionné, clique sur en fonction l'option de l'**information de stratégie** sur le panneau gauche. Sélectionnez le bouton de **modifications de validation**. La stratégie d'intrusion est validée.

  Remarque: La validation de stratégie échoue si vous activez une règle locale importée qui utilise le mot clé désapprouvé de seuil en combination avec la caractéristique de seuillage d'événement d'intrusion dans une stratégie d'intrusion.

Visualisez les règles locales supprimées

- Toutes les règles locales supprimées sont déplacées de la catégorie locale de règle à la catégorie supprimée de règle.
- Pour visualiser le nombre de révision d'une règle locale supprimée, aller à la page d'**éditeur de règle**, cliquent sur en fonction la catégorie **supprimée** pour développer le répertoire, puis cliquent sur l'icône de *crayon* pour visualiser le détail de la règle dans la page d'**éditeur de règle**.

Numérotation des règles locales

- Vous ne devez pas spécifier un générateur (GID) ; si vous faites, vous pouvez spécifier seulement le 1par GID une règle standard des textes ou 138 pour des données sensibles ordonnent.
- Ne spécifiez pas un nombre de l'ID (SID) ou de révision de renifler en important une règle pour la première fois ; ceci évite des collisions avec des SID d'autres règles, y compris des règles supprimées.
- Le centre de Gestion de FireSIGHT assigne automatiquement la prochaine règle faite sur commande disponible SID de 1000000 ou plus grand, et un nombre de révision de 1.
- Si vous tentez d'importer une règle d'intrusion avec un SID plus grand que 2147483647, une erreur de validation se produira.
- Vous devez inclure le SID assigné par IPS et un nombre de révision plus grand que le nombre de révision en cours en important une version mise à jour d'une règle locale que vous avez précédemment importée.
- Vous pouvez rétablir une règle locale que vous avez supprimée en important la règle utilisant le SID assigné par IPS et un nombre de révision plus grand que le nombre de révision en cours. Notez que le centre de Gestion de FireSIGHT incrémente automatiquement le nombre de révision quand vous supprimez une règle locale ; c'est un périphérique qui te permet pour rétablir des règles locales.