Règles Snort locales personnalisées sur un système Cisco FireSIGHT

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Utilisation des règles locales personnalisées](#)
[Importer les règles locales](#)
[Afficher les règles locales](#)
[Activer les règles locales](#)
[Afficher les règles locales supprimées](#)
[Numérotation des règles locales](#)

Introduction

Une règle locale personnalisée sur un système FireSIGHT est une règle Snort standard personnalisée que vous importez au format de fichier texte ASCII à partir d'un ordinateur local. Un système FireSIGHT vous permet d'importer des règles locales à l'aide de l'interface Web. La procédure d'importation des règles locales est très simple. Cependant, pour écrire une règle locale optimale, un utilisateur doit posséder des connaissances approfondies sur Snort et les protocoles réseau.

L'objectif de ce document est de vous fournir quelques conseils et une assistance pour écrire une règle locale personnalisée. Les instructions sur la création de règles locales sont disponibles dans le *Snort Users Manual,* qui est disponible à l'adresse snort.org. Cisco vous recommande de télécharger et de lire le Manuel d'utilisation avant d'écrire une règle locale personnalisée.

> **Note**: Les règles fournies dans un package Sourcefire Rule Update (SRU) sont créées et testées par le groupe Cisco Talos Security Intelligence and Research et prises en charge par le centre d'assistance technique Cisco (TAC). Le TAC Cisco ne fournit aucune assistance pour l'écriture ou le réglage d'une règle locale personnalisée. Toutefois, si vous rencontrez des problèmes avec la fonctionnalité d'importation de règles de votre système FireSIGHT, contactez le TAC Cisco.

> **Avertissement :** Une règle locale personnalisée mal écrite peut affecter les performances d'un système FireSIGHT, ce qui peut entraîner une dégradation des performances de l'ensemble du réseau. Si vous rencontrez des problèmes de performances sur votre réseau et que certaines règles Snort locales personnalisées sont activées sur votre système FireSIGHT, Cisco vous recommande de désactiver ces règles locales.

Conditions préalables

Exigences

Cisco vous recommande de connaître les règles Snort et le système FireSIGHT.

Composants utilisés

Les informations de ce document sont basées sur les versions matérielles et logicielles suivantes :

- FireSIGHT Management Center (également appelé Defense Center)
- Version de logiciel 5.0 ou ultérieure

Utilisation des règles locales personnalisées

Importer les règles locales

Avant de commencer, vous devez vous assurer que les règles du fichier ne contiennent aucun caractère d'échappement. L'importateur de règles nécessite que toutes les règles personnalisées soient importées à l'aide du codage ASCII ou UTF-8.

La procédure suivante explique comment importer des règles de texte standard locales à partir d'un ordinateur local :

1. Accédez à la page **Éditeur de règles** en sélectionnant **Stratégies > Intrusion > Éditeur de règles**.

2. Cliquez sur **Importer des règles**. La page **Mises à jour des règles** apparaît.

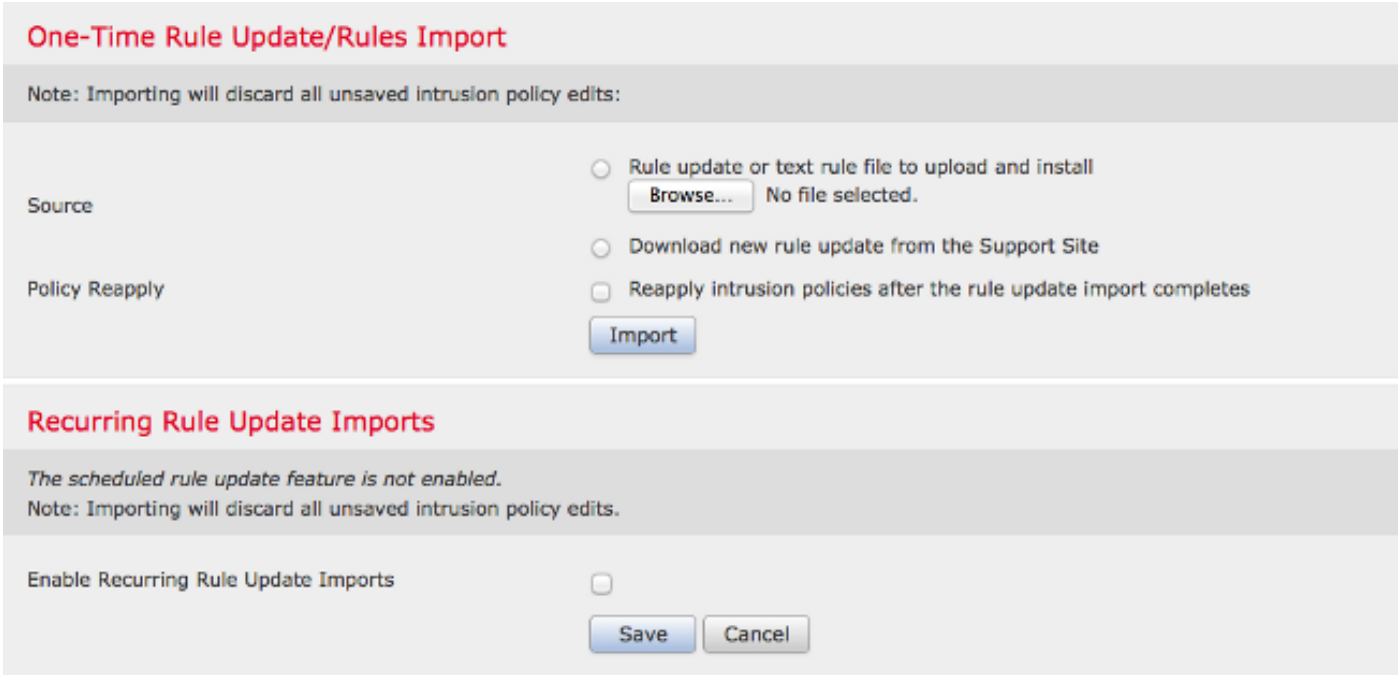


Figure : Capture d'écran de la page Mises à jour des règles

3. Sélectionnez **Mise à jour de la règle ou Fichier de règles texte à télécharger et installer** et cliquez sur **Parcourir** pour sélectionner le fichier de règles.

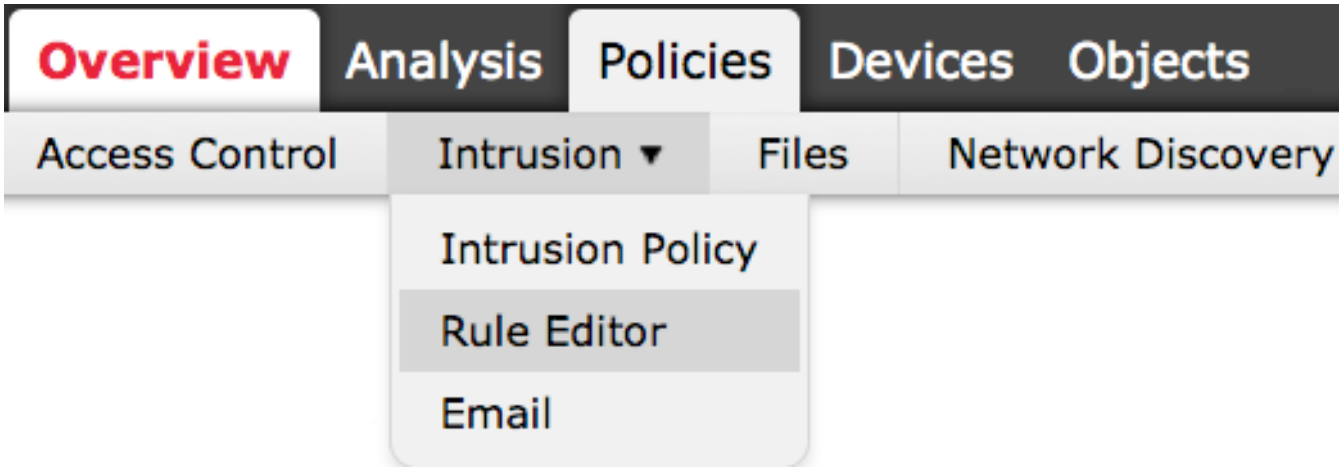
> **Note**: Toutes les règles téléchargées sont enregistrées dans la catégorie de **règle locale**.

4. Cliquez sur **Importer**. Le fichier de règles est importé.

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

Afficher les règles locales

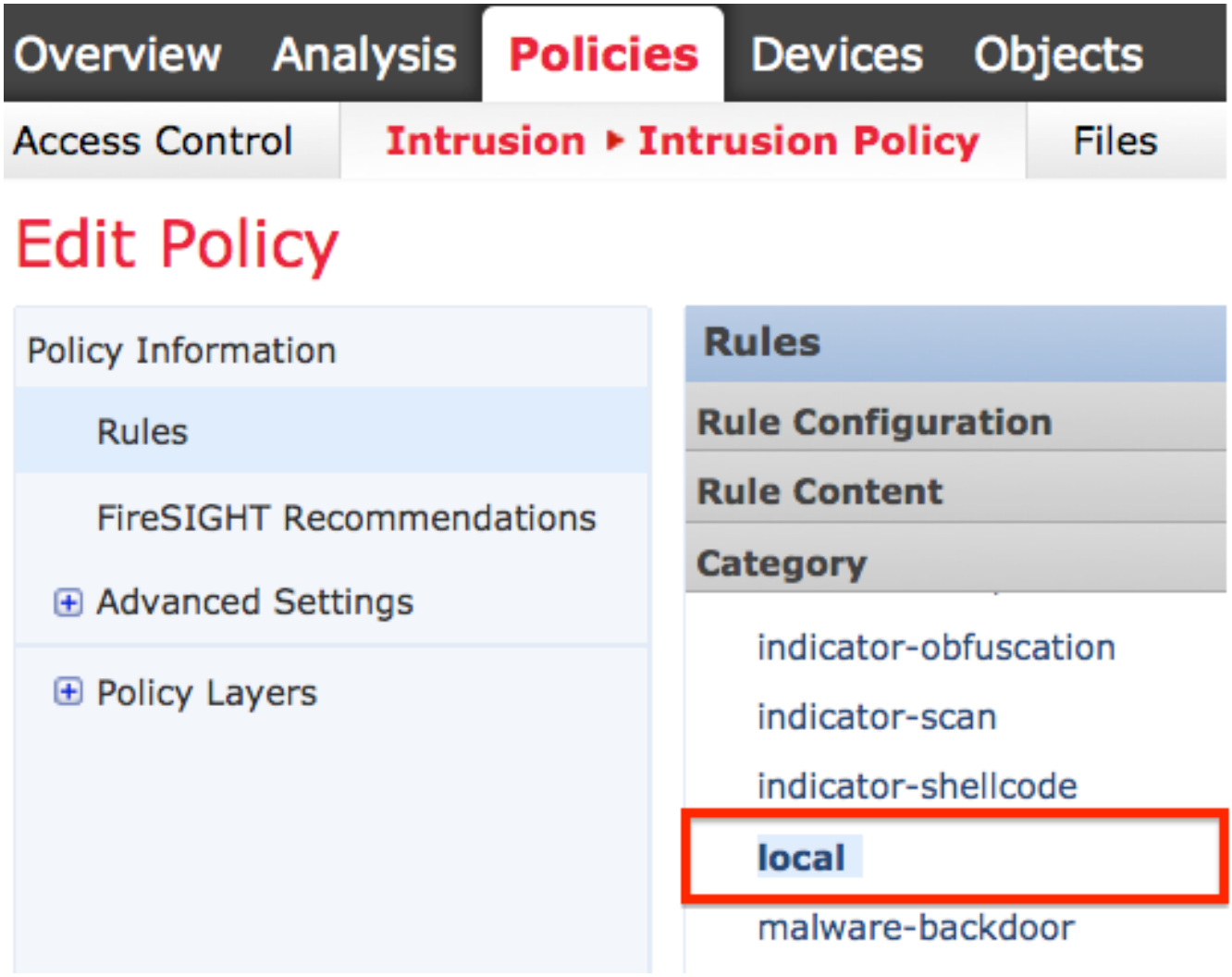
- Pour afficher le numéro de révision d'une règle locale en cours, accédez à la page **Éditeur de règle** (**Politiques** > **Intrusion** > **Éditeur de règle**).



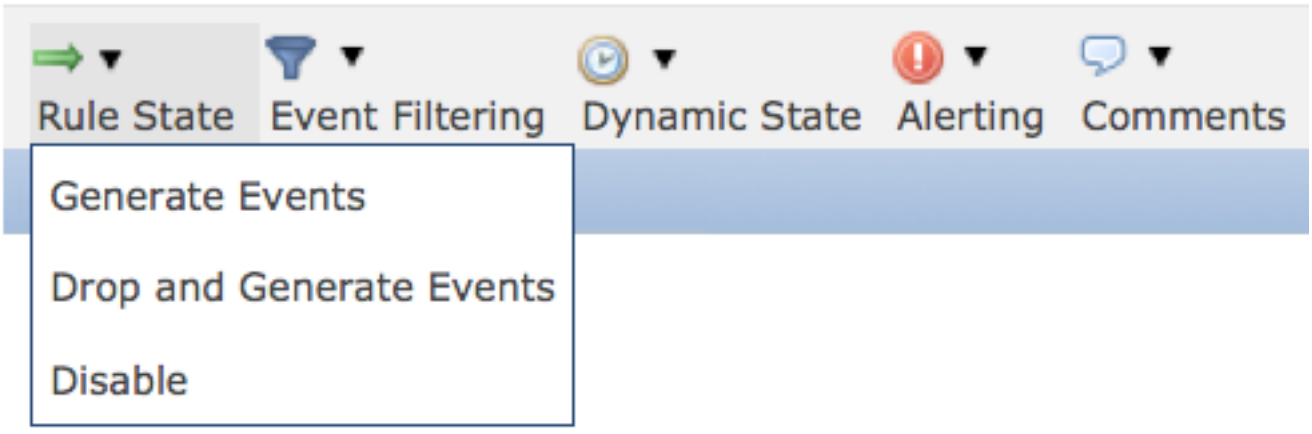
- Dans la page Éditeur de règle, cliquez sur la catégorie **Règle locale** pour développer le dossier, puis cliquez sur **Modifier** en regard de la règle.
- Toutes les règles locales importées sont automatiquement enregistrées dans la catégorie de **règles locales**.

Activer les règles locales

- Par défaut, FireSIGHT System définit les règles locales dans un état désactivé. Vous devez définir manuellement l'état des règles locales avant de pouvoir les utiliser dans votre stratégie d'intrusion.
- Afin d'activer une règle locale, accédez à la page Éditeur de stratégie (**Politiques** > **Intrusion** > **Stratégie d'intrusion**). Sélectionnez **Règles** dans le panneau de gauche. Sous la **catégorie**, sélectionnez **local**. Toutes les règles locales doivent apparaître, si elles sont disponibles.



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



- Une fois l'état de la règle sélectionné, cliquez sur l'option **Informations sur la politique** sur le panneau de gauche. Cliquez sur le bouton **Valider les modifications**. La politique d'intrusion est validée.

  Note: La validation de la stratégie échoue si vous activez une règle locale importée qui utilise le mot clé deprecated threshold en combinaison avec la fonctionnalité de seuil d'événement d'intrusion dans une stratégie d'intrusion.

Afficher les règles locales supprimées

- Toutes les règles locales supprimées sont déplacées de la catégorie de règle locale vers la catégorie de règle supprimée.
- Pour afficher le numéro de révision d'une règle locale supprimée, accédez à la page **Éditeur de règle**, cliquez sur la catégorie **supprimée** pour développer le dossier, puis cliquez sur l'icône de *crayon* pour afficher les détails de la règle dans la page de l'**Éditeur de règle**.

Numérotation des règles locales

- Vous n'avez pas besoin de spécifier un générateur (GID) ; Si vous le faites, vous pouvez spécifier uniquement GID 1 pour une règle de texte standard ou 138 pour une règle de données sensibles.
- Lors de la première importation d'une règle, ne spécifiez pas d'ID de renfort (SID) ou de numéro de révision ; cela évite les collisions avec les SID d'autres règles, y compris les règles supprimées.
- FireSIGHT Management Center attribue automatiquement le prochain SID de règle personnalisé disponible, 1000000 ou supérieur, et le numéro de révision 1.
- Si vous tentez d'importer une règle d'intrusion avec un SID supérieur à 2147483647, une erreur de validation se produit.
- Vous devez inclure le SID attribué par IPS et un numéro de révision supérieur au numéro de révision actuel lors de l'importation d'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 à l'aide du SID attribué par IPS et d'un numéro de révision supérieur au numéro de révision actuel. Notez que FireSIGHT Management Center incrémente automatiquement le numéro de révision lorsque vous supprimez une règle locale ; il s'agit d'un périphérique qui vous permet de rétablir les règles locales.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.