Vérifier la liste SID personnalisée à partir des capteurs Firepower à l'aide de l'interface de ligne de commande et de l'interface utilisateur graphique FMC

Introduction

Ce document décrit comment obtenir une liste SID personnalisée à partir de Firepower Threat Defense (FTD) ou du module FirePOWER à l'aide de l'interface utilisateur graphique CLI et FMC. Les informations SID se trouvent sur l'interface graphique de FMC si vous naviguez jusqu'à ***Objets > Règles d'intrusion***. Dans certains cas, il est nécessaire d'obtenir une liste des SID disponibles auprès de l'interface de ligne de commande.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les sujets suivants :

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA avec fonctionnalités FirePOWER
- Cisco Firepower Management Center (FMC)
- Connaissances de base Linux

Components Used

Les informations de ce document sont basées sur la version logicielle suivante :

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- Module FirePOWER 6.2.3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Une ***règle d'intrusion*** est un ensemble de mots clés et d'arguments que le système utilise pour détecter les tentatives d'exploitation des vulnérabilités sur votre réseau. Lorsque le système analyse le trafic réseau, il compare les paquets aux conditions spécifiées dans chaque règle. Si les données de paquet correspondent à toutes les conditions spécifiées dans une règle, la règle se déclenche. Si une règle est une règle d'alerte, elle génère un événement d'intrusion. S'il s'agit d'une règle de passe, elle ignore le trafic. Pour une règle d'abandon dans un déploiement en ligne, le système abandonne le paquet et génère un événement. Vous pouvez afficher et évaluer les

événements d'intrusion à partir de la console Web Firepower Management Center.

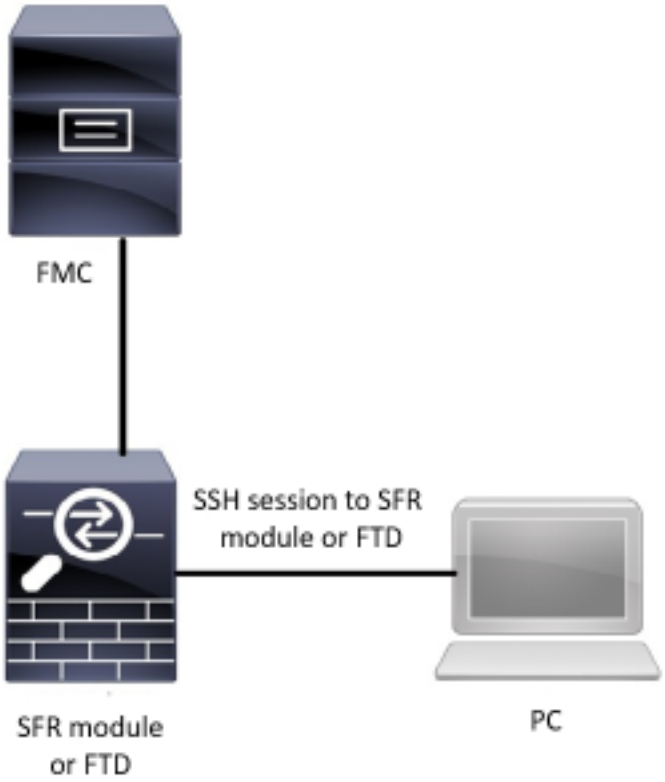
Le système Firepower fournit deux types de règles d'intrusion : ***règles d'objet partagées*** et ***règles de texte standard***. Le Cisco Talos Security Intelligence and Research Group (Talos) peut utiliser des règles d'objet partagées pour détecter les attaques contre les vulnérabilités de manière que les règles de texte standard traditionnelles ne le peuvent pas. Il n'est pas possible de créer des règles d'objet partagé. Lorsque des règles d'intrusion sont écrites seules, une règle de texte standard doit être créée. Règles de texte standard personnalisées pour ajuster les types d'événements que vous êtes susceptible de voir. En écrivant des règles et en spécifiant le message d'événement de la règle, vous pouvez plus facilement identifier le trafic qui indique des attaques et des évasions de stratégie.

Lorsque vous activez une règle de texte standard personnalisée dans une stratégie d'intrusion personnalisée, gardez à l'esprit que certains mots clés et arguments de règle exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière.

Une ***règle locale personnalisée*** sur un système Firepower est une règle Snort standard personnalisée que vous importez dans un format de fichier texte ASCII à partir d'une machine locale. Un système Firepower vous permet d'importer des règles locales à l'aide de l'interface Web. Les étapes à suivre pour importer les règles locales sont très simples. Cependant, pour établir une règle locale optimale, un utilisateur doit posséder une connaissance approfondie des protocoles Snort et de réseau.

> **Avertissement :** Assurez-vous d'utiliser un environnement réseau contrôlé pour tester les règles d'intrusion que vous écrivez avant d'utiliser ces règles dans un environnement de production. Des règles d'intrusion mal écrites peuvent affecter sérieusement les performances du système

Diagramme du réseau

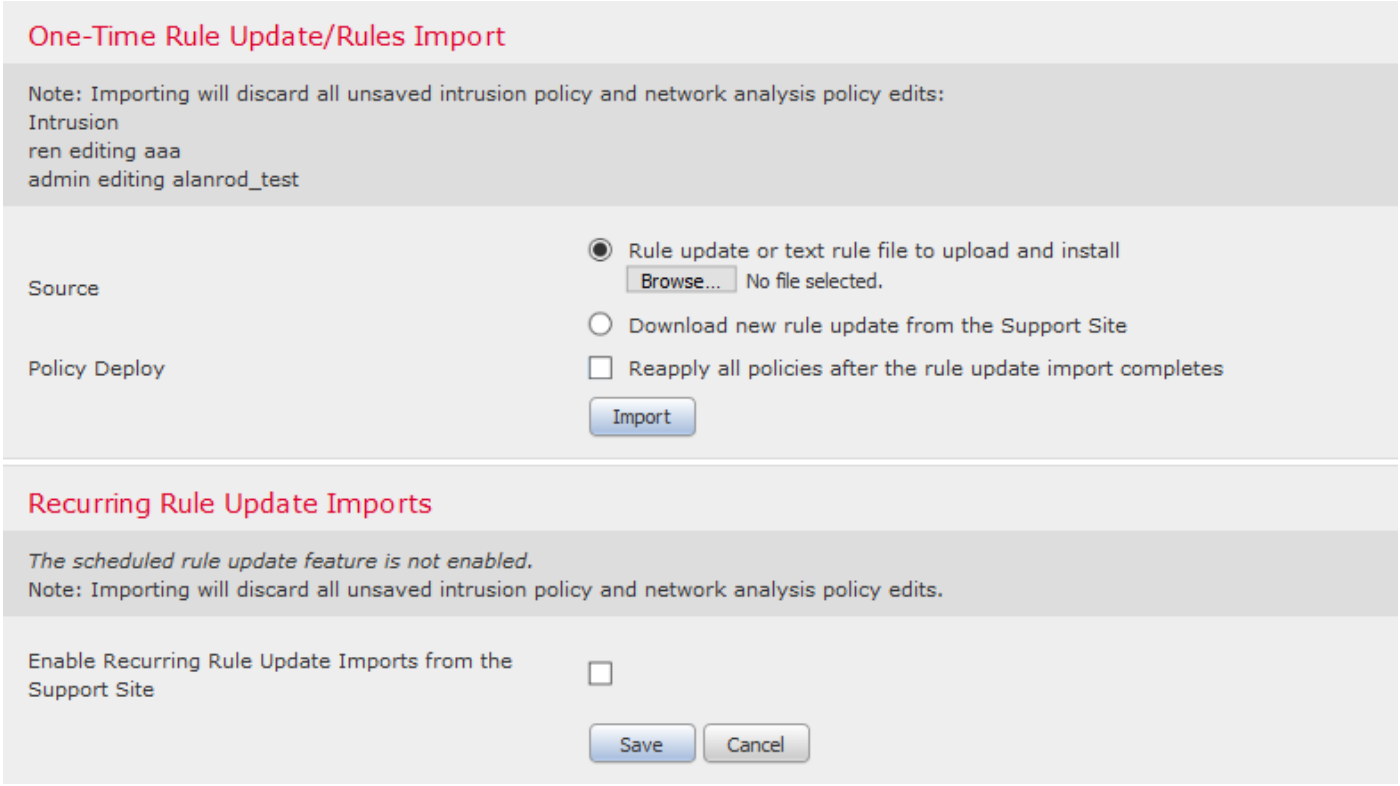


Configuration

Importer les règles locales

Avant de commencer, vous devez vous assurer que les règles répertoriées dans votre fichier personnalisé ne contiennent pas de caractères spéciaux. L'importateur de règles requiert l'importation de toutes les règles personnalisées à l'aide du codage ASCII ou UTF-8. La procédure ci-dessous explique comment importer des règles de texte standard locales à partir d'une machine locale.

Étape 1. Accédez à l'onglet **Importer les règles** en accédant à **Objets > Règles d'intrusion > Règles d'importation.** La page **Mises à jour des règles** s'affiche comme indiqué dans l'image ci-dessous :



Étape 2. Sélectionnez **Mise à jour de règle ou fichier de règle de texte à télécharger et installer** et cliquez sur **Parcourir** pour sélectionner le fichier de règle personnalisé

> **Note**: Toutes les règles téléchargées sont enregistrées dans la catégorie de **règles locales**

Étape 3. Cliquez sur **Import**. Le fichier de règle est importé

> **Remarque** : les systèmes Firepower 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 appliquer la stratégie.

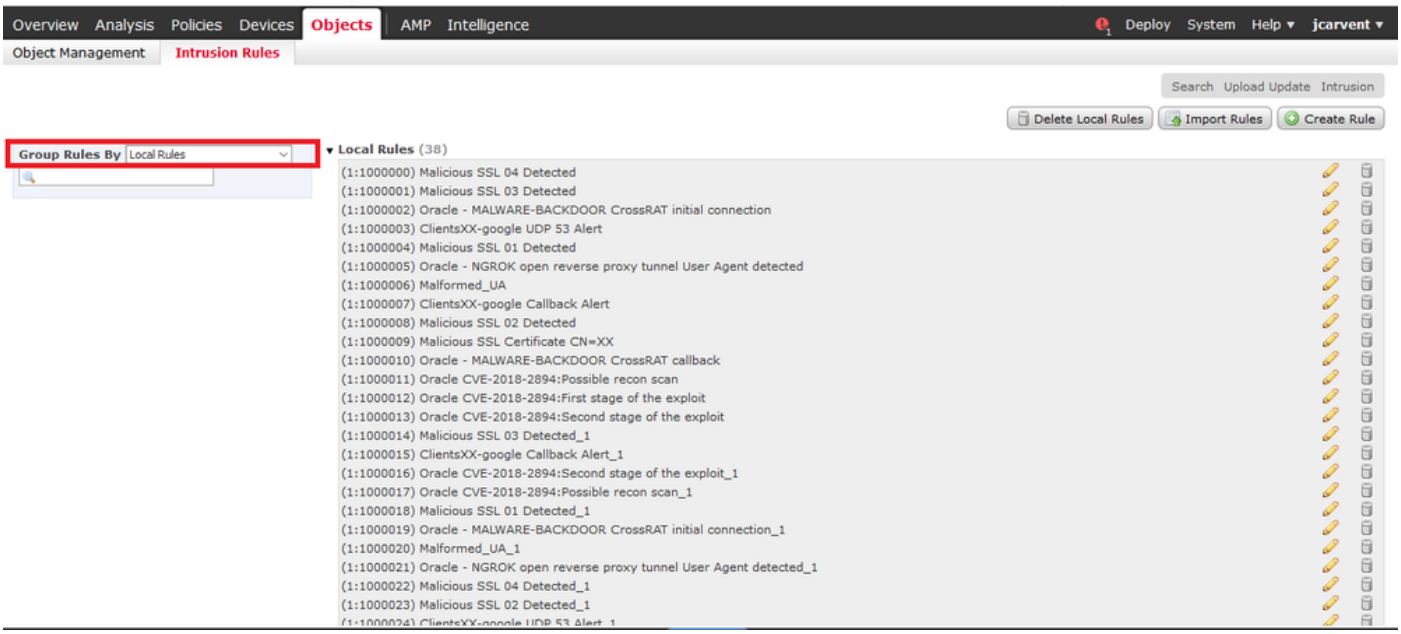
Vérification

À partir de l'interface utilisateur FMC

1. Afficher les règles locales importées à partir de l'interface utilisateur FMC

Étape 1. Accédez à **Objets > Règles d'intrusion**

Étape 2. Sélectionnez **Règles locales** dans **Règles de groupe**



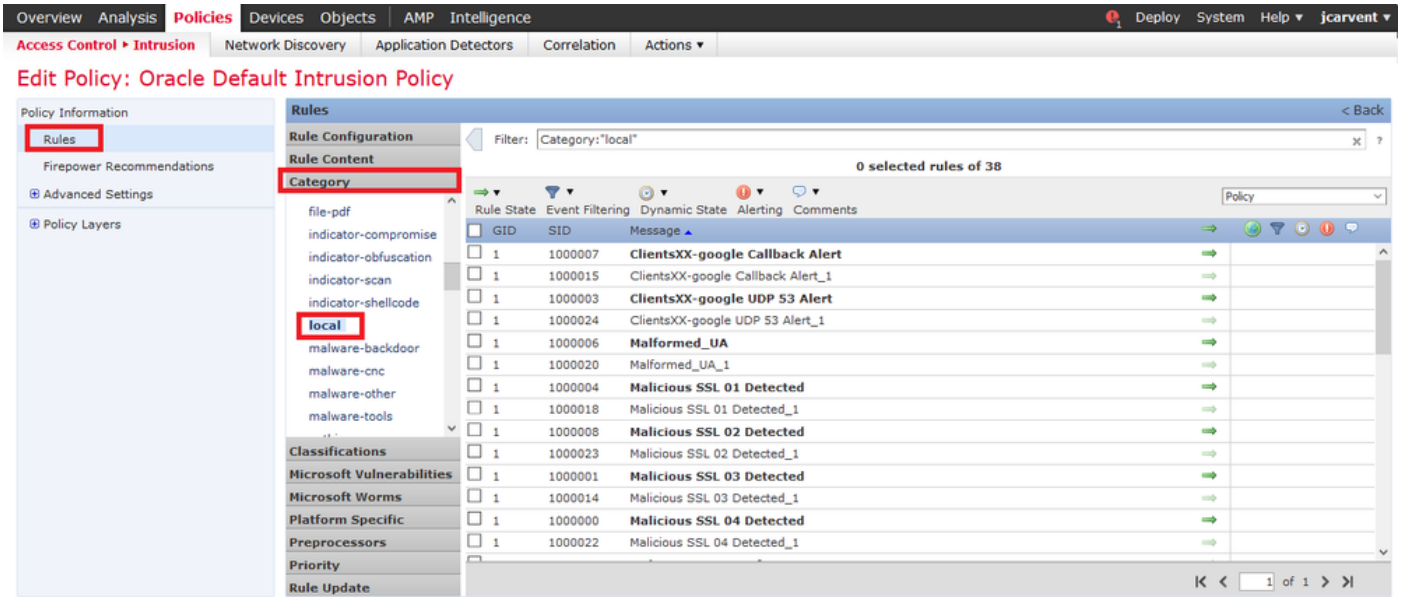
Par défaut, le système Firepower définit les règles locales dans un état désactivé. Ces règles locales doivent définir manuellement l'état des règles locales avant que vous puissiez les utiliser dans votre stratégie d'intrusion.

2. Activer une règle locale à partir d'une stratégie d'intrusion

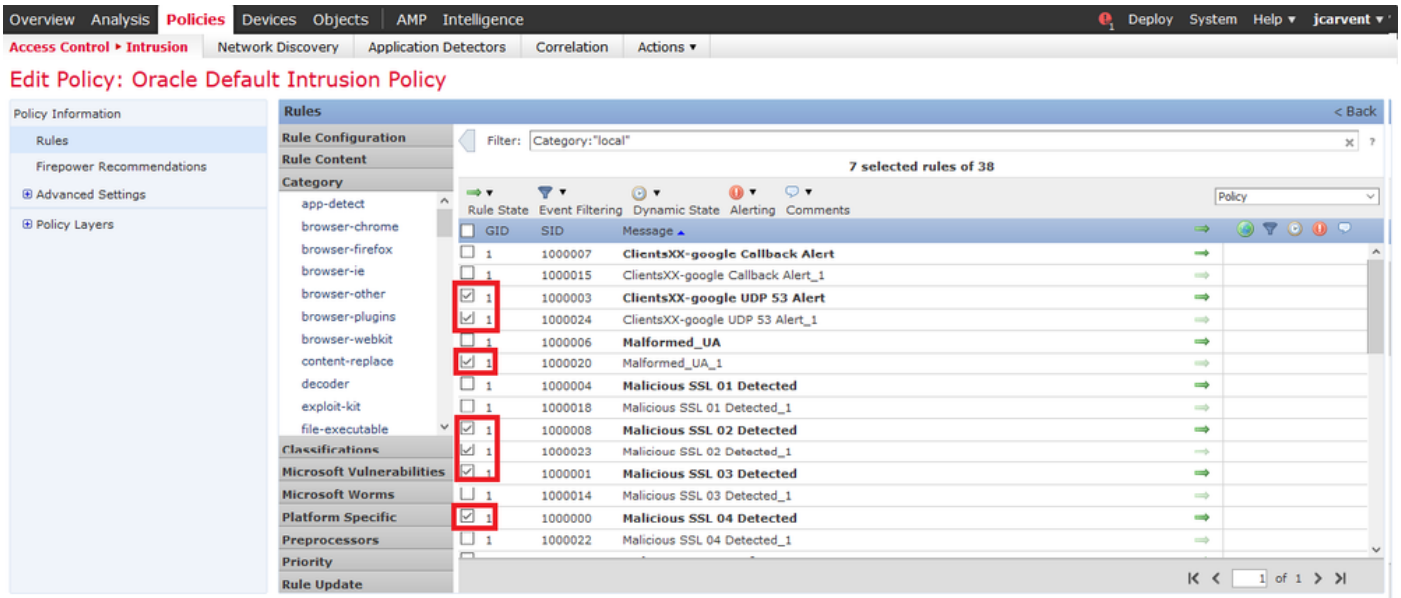
Étape 1. Accédez à la page Éditeur de stratégie sous **Stratégies > Intrusion > Stratégie d'intrusion**

Étape 2. Sélectionnez **Règles** dans le panneau de gauche

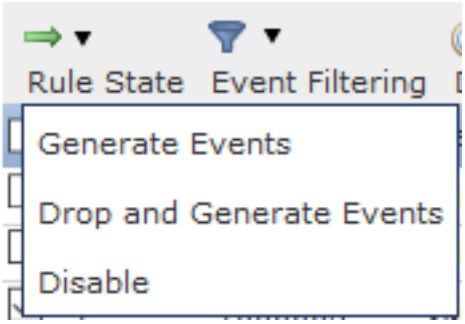
Étape 3. Sous la **catégorie**, sélectionnez **local.** Toutes les règles locales doivent apparaître si elles sont disponibles :



Étape 4. Sélectionnez les règles locales souhaitées :



Étape 5. Après avoir sélectionné les règles locales souhaitées, sélectionnez un état dans **État de la règle.**



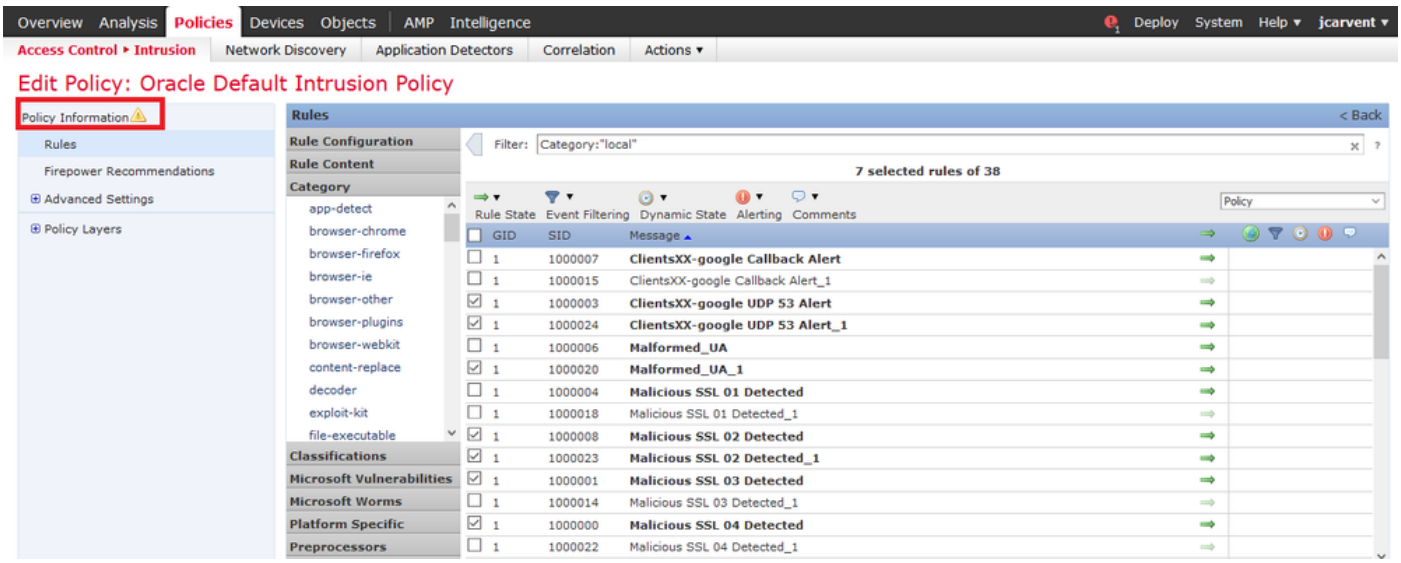
Les options suivantes sont disponibles :

- Générer des événements : Activer la règle et générer un événement

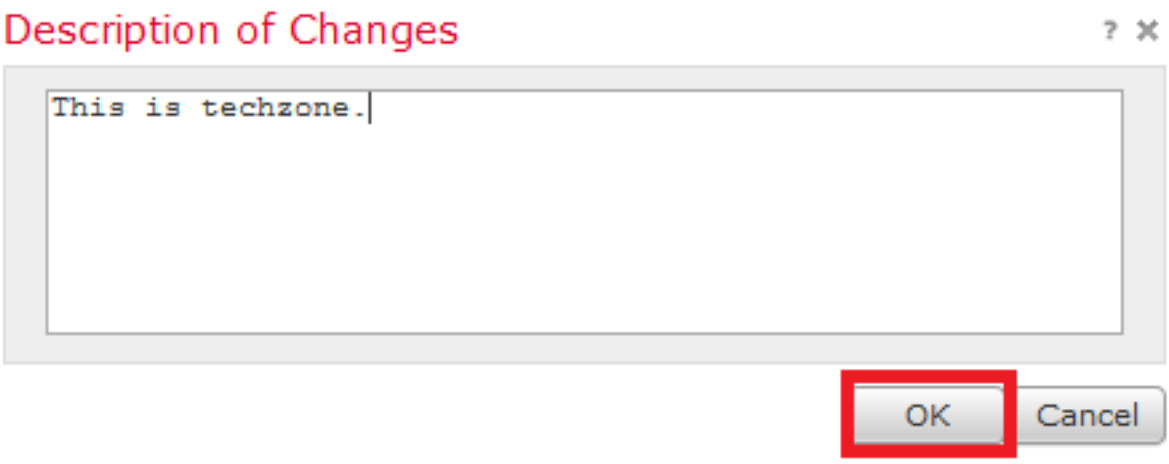
- Déposer et générer des événements : Activer la règle, abandonner le trafic et générer un événement

- **Désactiver :** Aucune activation de la règle, aucun événement

Étape 6. Une fois l'état de la règle sélectionné, cliquez sur Option **Informations de stratégie** du panneau de gauche



Étape 7. Cliquez sur le bouton **Valider les modifications** et fournissez une brève description des modifications. Cliquez sur **OK** plus tard. La stratégie d'intrusion est validée.



> **Remarque** : la validation de la stratégie échoue si vous activez une règle locale importée qui utilise le mot clé de seuil déconseillé en combinaison avec la fonctionnalité de seuil d'événement d'intrusion dans une stratégie d'intrusion.

Étape 8. Déployer les modifications

À partir de la CLI du module FTD ou SFR

1. Afficher les règles locales importées à partir de l'interface CLI du module FTD ou SFR

Étape 1. Établissez une session SSH ou CLI à partir de votre module SFR ou FTD

Étape 2. Passez en mode expert

```
> expert
admin@firepower:~$
```

Étape 3. Obtenir les privilèges d'administrateur

```
admin@firepower:~$ sudo su -
```

Étape 4. Tapez votre mot de passe

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Étape 5. Accédez à **/ngfw/var/sf/detection_engine/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

> **Note**: Si vous utilisez un module SFR, n'utilisez pas /ngfw/var/sf/detection_engine/*/intrusion path. Utilisation installée **/var/sf/detection_engine/*/intrusion**

Étape 6. Présentez la commande suivante :

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

Reportez-vous à l'image ci-dessous comme exemple de fonctionnement :

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

La liste des SID du client qui est activée par le module FTD ou SFR s'affiche.

Dépannage

Étape 1. Assurez-vous que la session SSH est établie sur le module SFR ou FTD, à partir de FMC detection_engine n'est pas répertoriée

Étape 2. La commande grep -Eo « sid:*([0-9]{1,8})" */*local.rules fonctionne uniquement sous le répertoire d'intrusion, la commande ne peut pas être utilisée à partir d'un autre répertoire

Étape 3. Utilisez la commande grep -Eo « sid:*([0-9]{1,8})" */*.rules afin d'obtenir une liste SID complète de toutes les catégories

Meilleures pratiques pour l'importation de règles d'intrusion

locales

Respectez les consignes lors de l'importation d'un fichier de règles local :

- L'importateur de règles exige que toutes les règles personnalisées soient importées dans un fichier texte brut codé en ASCII ou en UTF-8
- Le nom du fichier texte peut inclure des caractères alphanumériques, des espaces et aucun caractère spécial autre que le trait de soulignement (_), le point (.) et le tiret (-)
- Le système importe des règles locales précédées d'un caractère de livre unique (#), mais elles sont signalées comme supprimées
- Le système importe des règles locales précédées d'un caractère dièse (#) et n'importe pas de règles locales précédées de caractères dièse (##)
- Les règles ne peuvent contenir aucun caractère d'échappement
- Vous n'avez pas besoin de spécifier un ID de générateur (GID) lors de l'importation d'une règle locale. Si vous le faites, spécifiez uniquement GID 1 pour une règle de texte standard
- Lors de l'importation d'une règle pour la première fois, procédez comme suit : *non* spécifier un ID de noeud (SID) ou numéro de révision. Cela évite les collisions avec les SID d'autres règles, y compris les règles supprimées. Le système attribue automatiquement à la règle le prochain SID de règle personnalisée disponible de 1000000 ou plus, et un numéro de révision de 1
- Si vous devez importer des règles avec des SID, les SID doivent être des numéros uniques compris entre 1 000 000 et 9 999 999
- Dans un déploiement multidomaine, le système attribue des SID à des règles importées à partir d'un pool partagé utilisé par tous les domaines de la Centre de gestion Firepower. Si plusieurs administrateurs importent des règles locales en même temps, les SID d'un domaine donné peuvent sembler non séquentiels, car le système a attribué les numéros intermédiaires de la séquence à un autre domaine
- Lors de l'importation d'une version mise à jour d'une règle locale que vous avez précédemment importée ou lors de la restauration d'une règle locale que vous avez supprimée, vous ***devez*** inclure le SID attribué par le système et un numéro de révision supérieur au numéro de révision actuel. Vous pouvez déterminer le numéro de révision d'une règle actuelle ou supprimée en modifiant la règle

  Remarque : le système 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. Toutes les règles locales supprimées sont déplacées de la catégorie de règles locales vers la catégorie de règles supprimée.

- Importer des règles locales sur le Firepower Management Center principal dans une paire haute disponibilité pour éviter les problèmes de numérotation SID
- L'importation échoue si une règle contient l'un des éléments suivants :Un SID est supérieur à 2147483647Liste des ports source ou de destination de plus de 64 caractères
- La validation de la stratégie échoue si vous activez une règle locale importée qui utilise le mot clé ***threshold*** déconseillé en combinaison avec la fonctionnalité de seuil d'événement d'intrusion dans une stratégie d'intrusion
- Toutes les règles locales importées sont automatiquement enregistrées dans la catégorie de règles locales
- Le système définit toujours les règles locales que vous importez à l'état désactivé. Vous

devez définir manuellement l'état des règles locales avant de pouvoir les utiliser dans votre stratégie d'intrusion

Informations connexes

Voici quelques documents de référence relatifs au SID de snort :

Mettre à jour les règles d'intrusion

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

Éditeur de règles d'intrusion

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html