# Configurer des règles de sniffage local personnalisées dans Snort3 sur FTD

## Table des matières



## Introduction

Ce document décrit la procédure pour configurer des règles de détection locale personnalisées dans Snort3 sur Firewall Threat Defense (FTD).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center (FMC)
- Protection contre les menaces par pare-feu

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

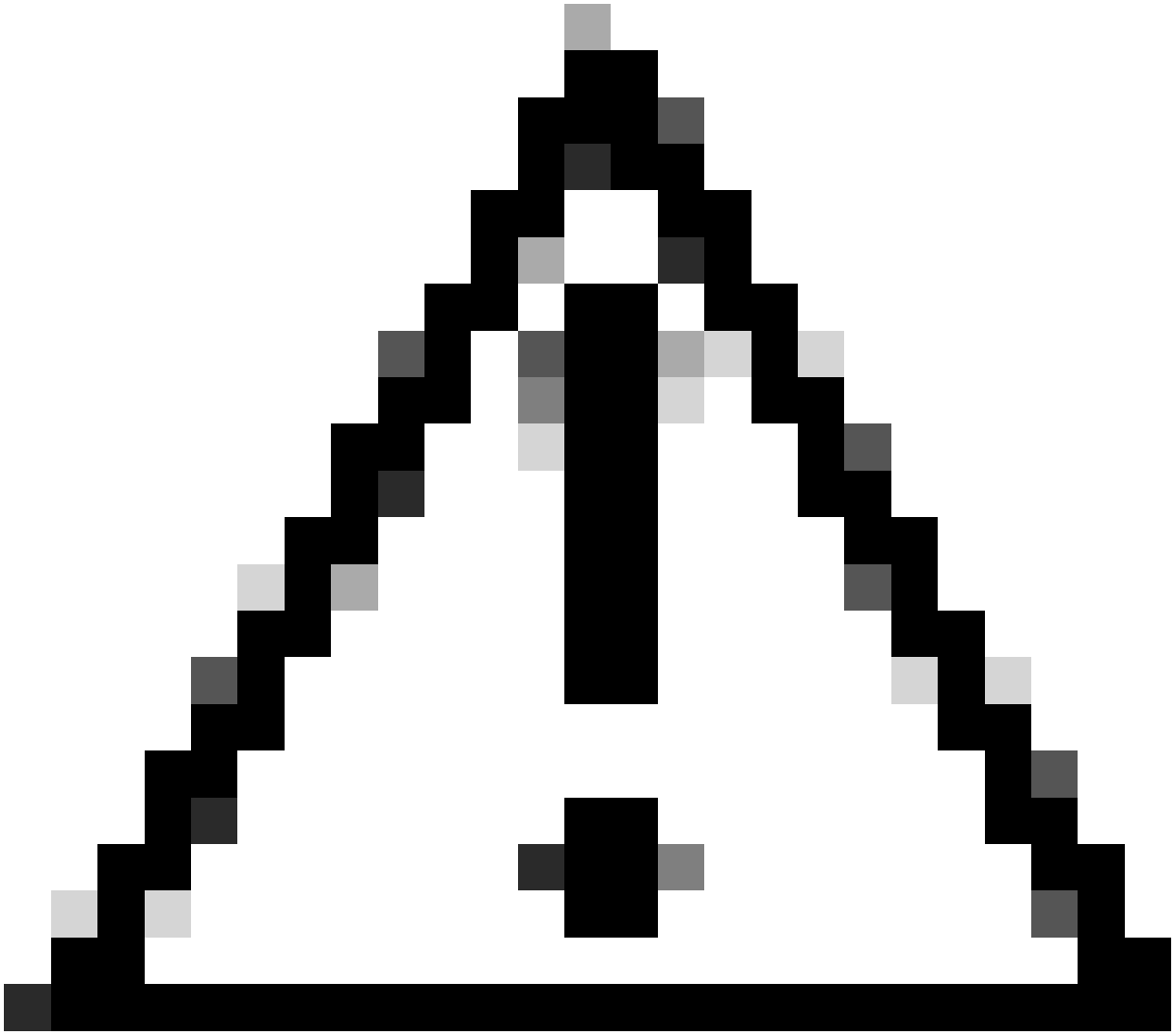
- Cisco Firepower Management Center pour VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

La prise en charge de Snort 3 dans la défense contre les menaces avec le centre de gestion commence dans la version 7.0. Pour les nouveaux périphériques et les périphériques réimagés des versions 7.0 et ultérieures, Snort 3 est le moteur d'inspection par défaut.

Ce document fournit un exemple de personnalisation des règles Snort pour Snort 3, ainsi qu'un exemple pratique de vérification. En particulier, vous apprendrez à configurer et à vérifier une stratégie d'intrusion avec une règle Snort personnalisée pour abandonner les paquets HTTP qui contiennent une certaine chaîne (nom d'utilisateur).



Attention : la création de règles Snort locales personnalisées et leur prise en charge ne sont pas prises en charge par le TAC. Par conséquent, ce document ne peut être utilisé qu'à titre de référence et vous demandez de créer et de gérer ces règles personnalisées à votre discrétion et sous votre responsabilité.

## Diagramme du réseau

Ce document présente la configuration et la vérification de la règle de sniffage local personnalisée dans Snort3 sur ce schéma.

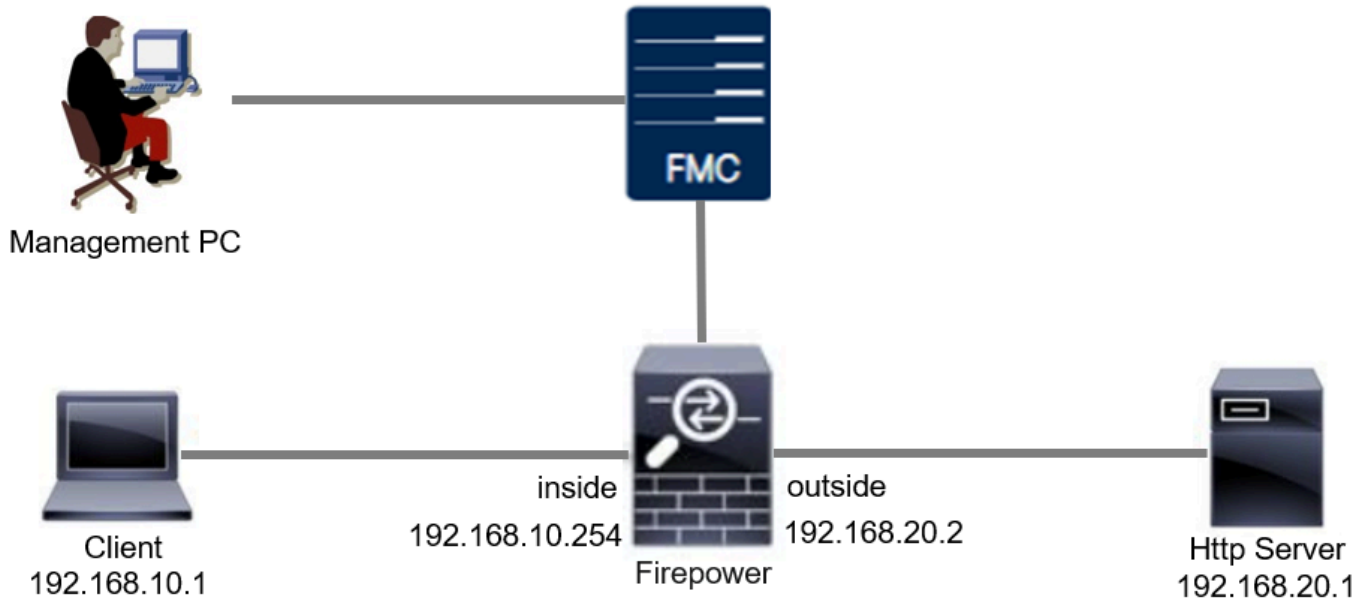
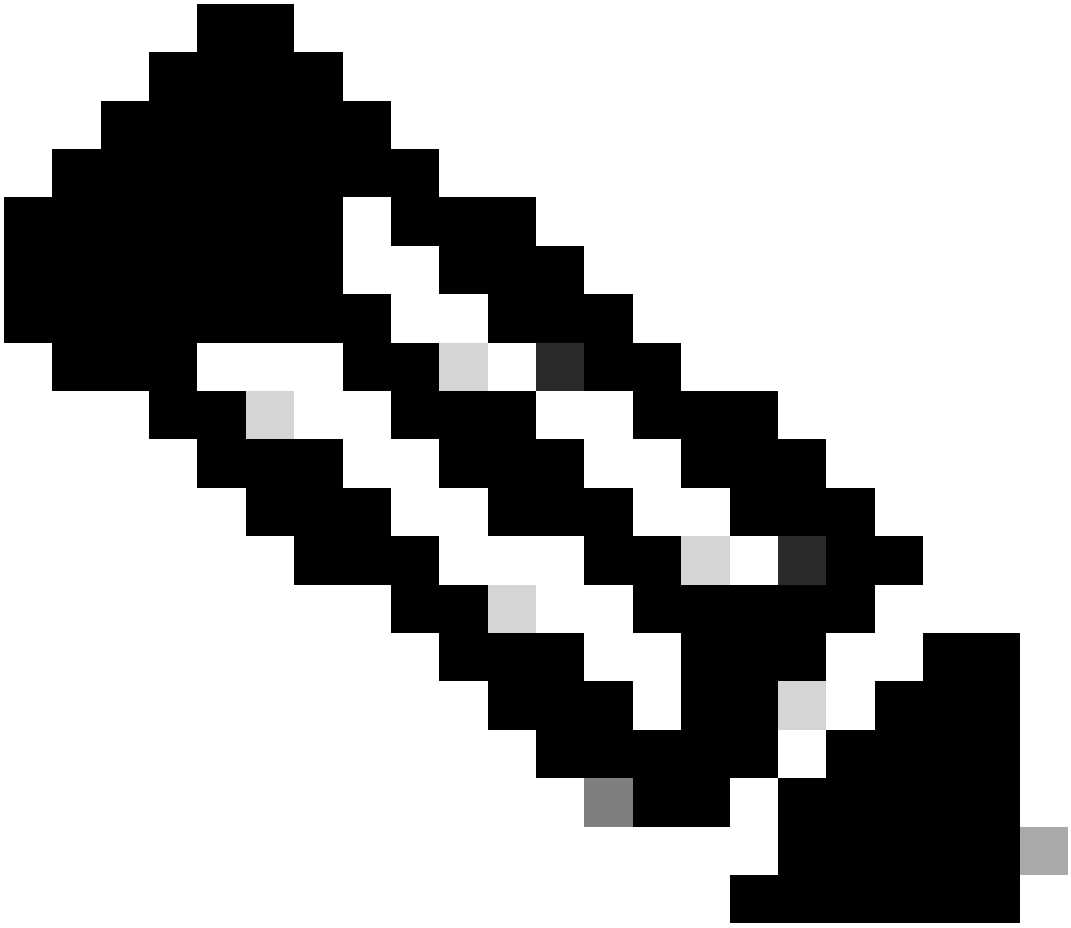



Diagramme du réseau

## Configuration

Il s'agit de la configuration de la règle de détection locale personnalisée pour détecter et supprimer les paquets de réponse HTTP contenant une chaîne spécifique (nom d'utilisateur).

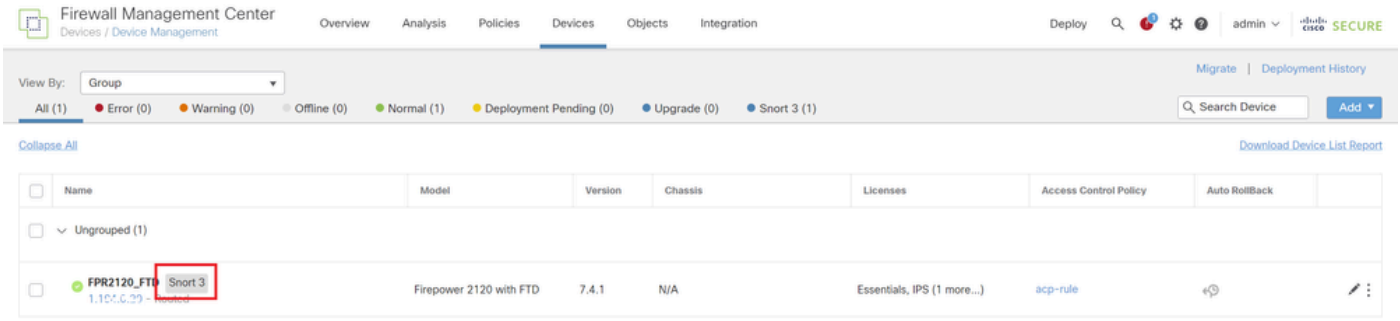


Remarque : il n'est pas possible d'ajouter des règles Snort locales personnalisées à partir de la page Toutes les règles Snort 3 de l'interface utilisateur graphique FMC. Vous devez utiliser la méthode présentée dans ce document.

## Méthode 1. Importer de Snort 2 vers Snort 3

Étape 1 : confirmation de la version Snort

Accédez àPériphériques>Gestion des périphériques sur FMC, cliquez sur l'onglet Périphérique. Vérifiez que la version de Snort est Snort3.



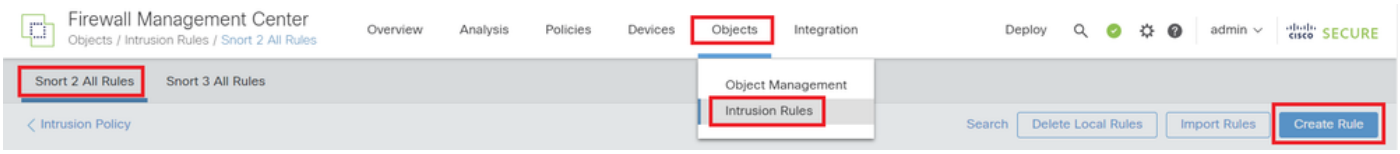

Version Snort

Étape 2. Créer ou modifier une règle de sniffage local personnalisée dans Snort 2

Accédez à Objets > Règles d'intrusion > Snort 2 All Rules sur FMC. Cliquez sur le bouton Créer une règle pour ajouter une règle de sniffage local personnalisée, ou accédez à Objets > Règles d'intrusion > Toutes les règles de sniffage 2 > Règles locales sur FMC, cliquez sur le bouton Modifier pour modifier une règle de sniffage local existante.

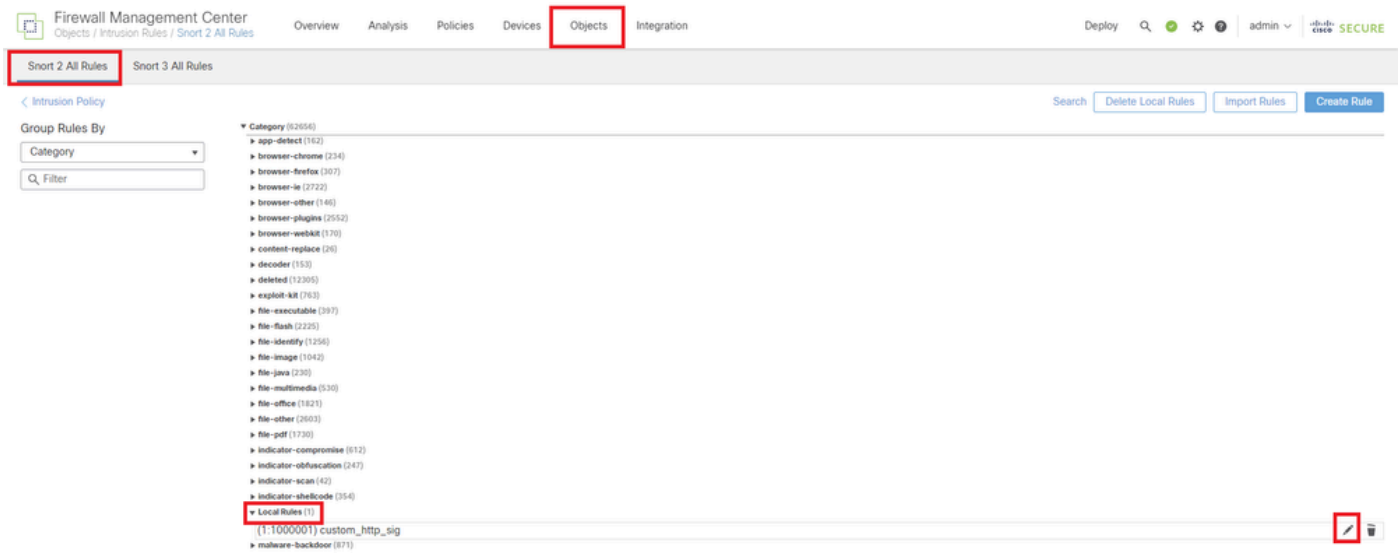
Pour des instructions sur la façon de créer des règles de Snort local personnalisées dans Snort 2, veuillez vous référer à Configurer des règles de Snort local personnalisées dans Snort2 sur FTD.

Ajoutez une nouvelle règle d'analyse locale personnalisée comme illustré dans l'image.




Ajouter une nouvelle règle personnalisée

Modifiez une règle de sniffage local personnalisée existante comme indiqué dans l'image. Dans cet exemple, modifie une règle personnalisée existante.

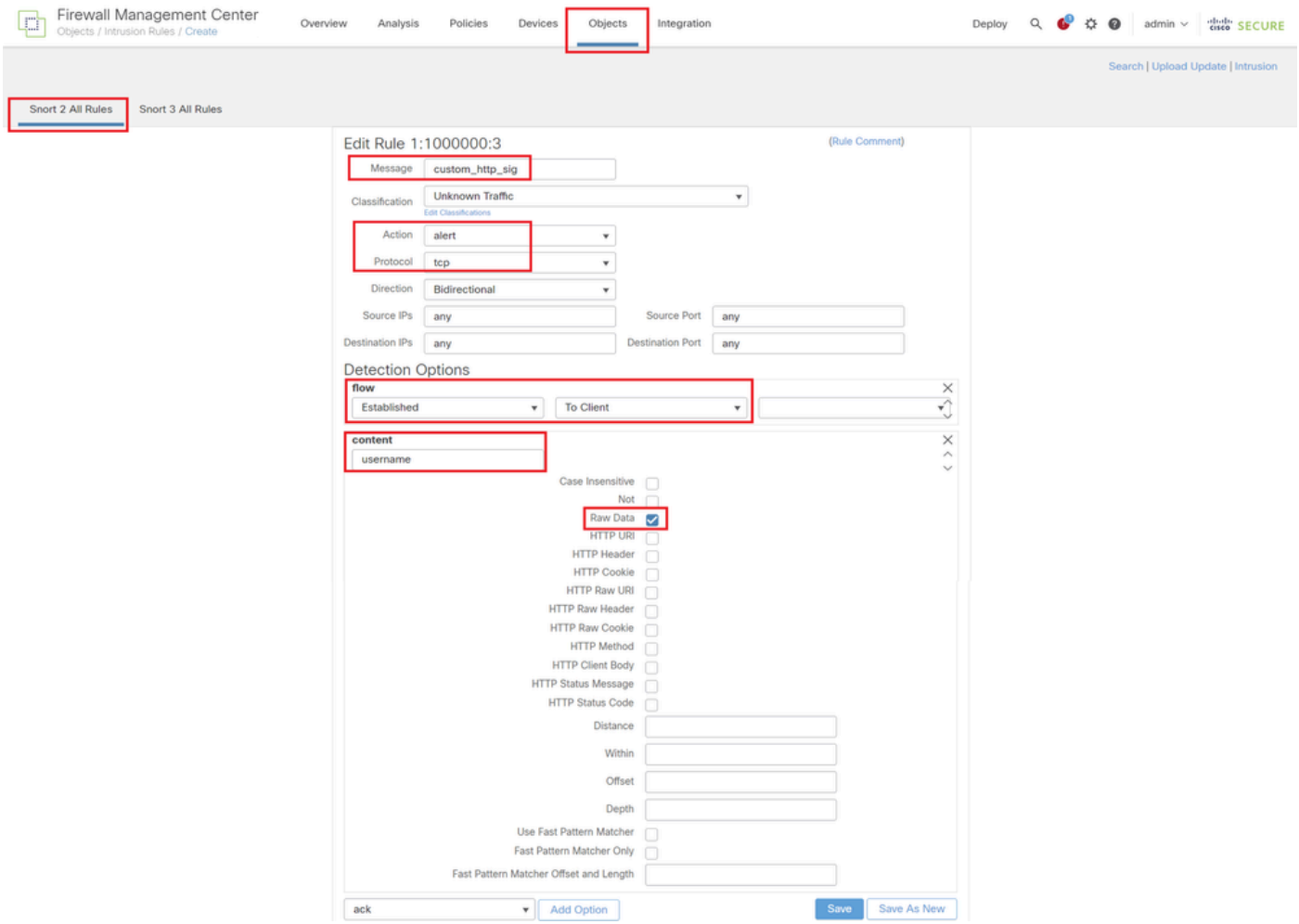



Modifier une règle personnalisée existante

Entrez les informations de signature pour détecter les paquets HTTP contenant une chaîne

spécifique (nom d'utilisateur).

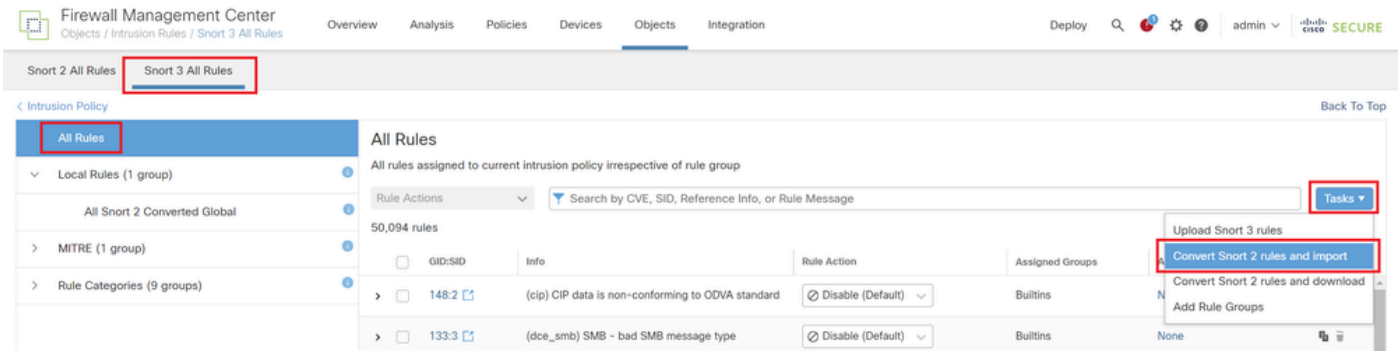
- Message : custom_http_sig
- Action : alerte
- Protocole : TCP
- flux : établi, au client
- content : username (Raw Data)



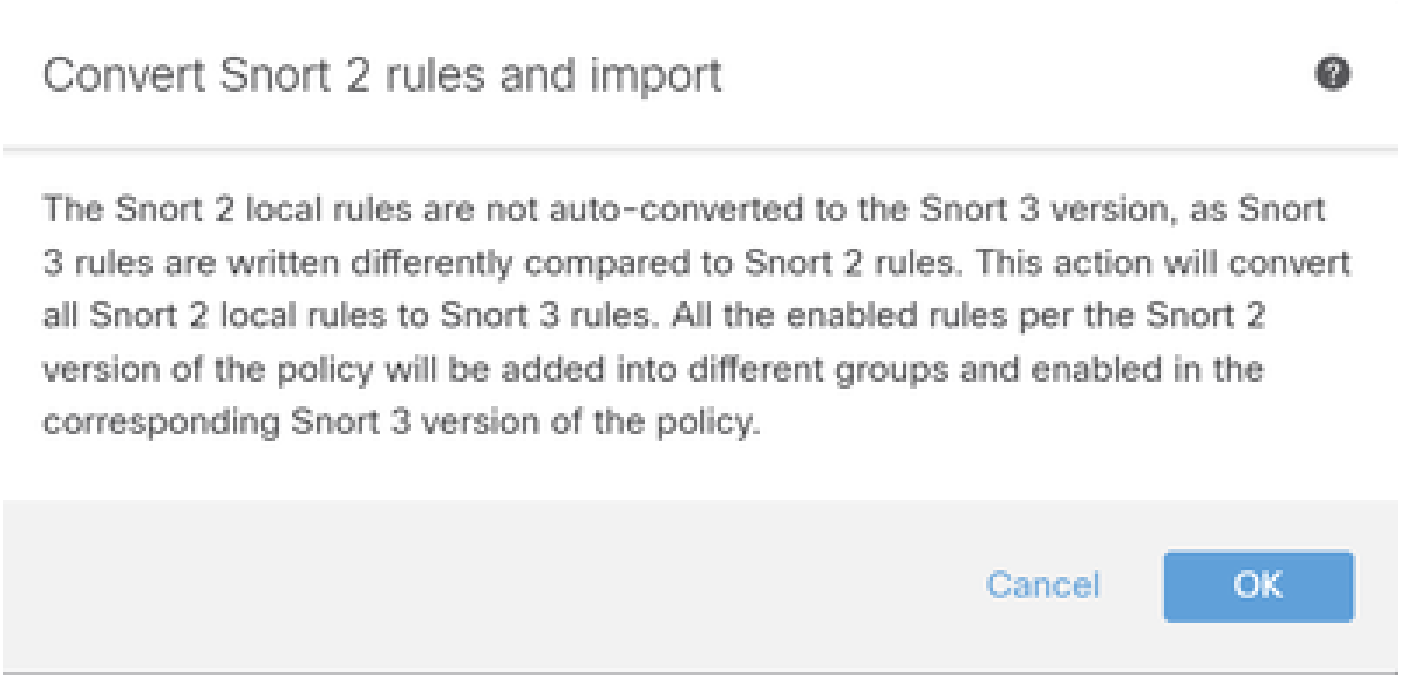

Informations requises pour la règle

Étape 3. Importer des règles de sniffage locales personnalisées de Snort 2 vers Snort 3

Accédez à Objets > Règles d'intrusion > Snort 3 Toutes les règles > Toutes les règles sur FMC, cliquez sur Convertir les règles Snort 2 et Importer à partir de la liste déroulante Tâches.

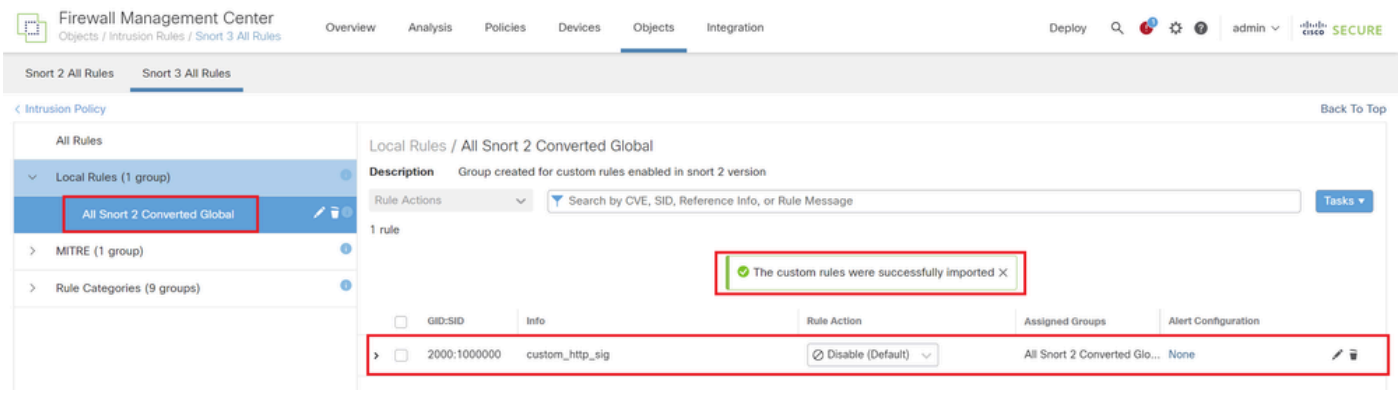


Vérifiez le message d'avertissement et cliquez sur OK.




Message d'avertissement

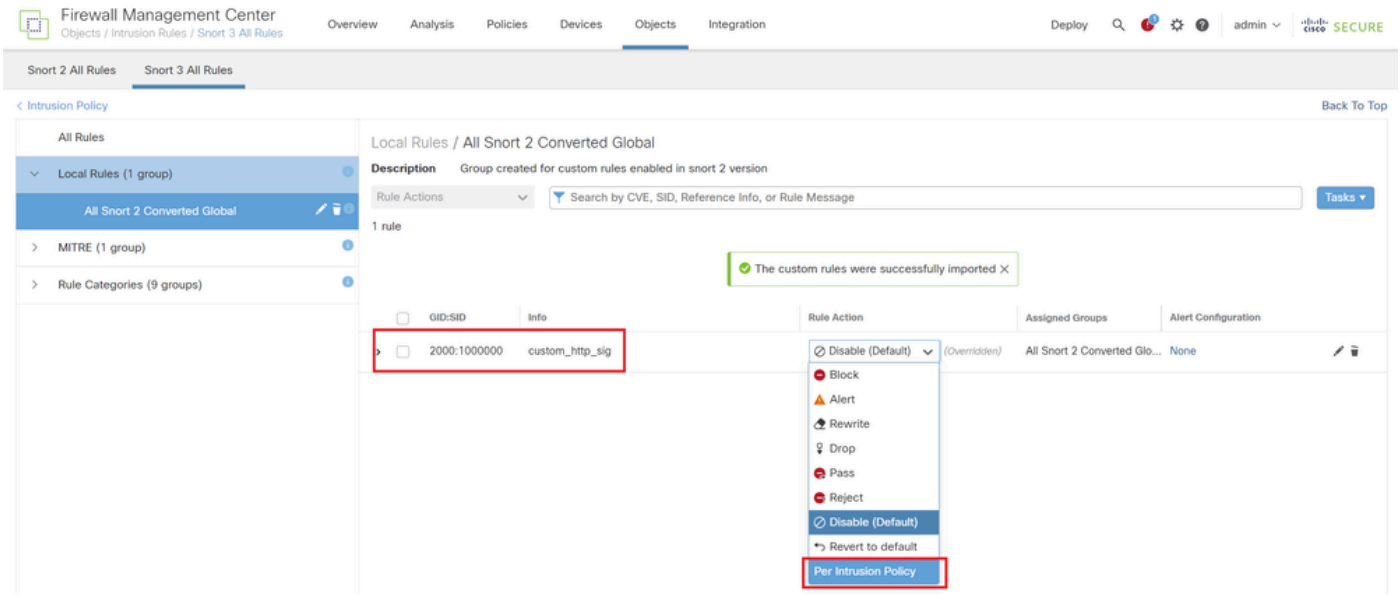
Accédez à Objets > Règles d'intrusion > Snort 3 All Rules sur FMC, cliquez sur All Snort 2 Converted Global pour confirmer la règle de snort locale personnalisée importée.




Confirmer la règle personnalisée importée

Étape 4. Action Modifier la règle

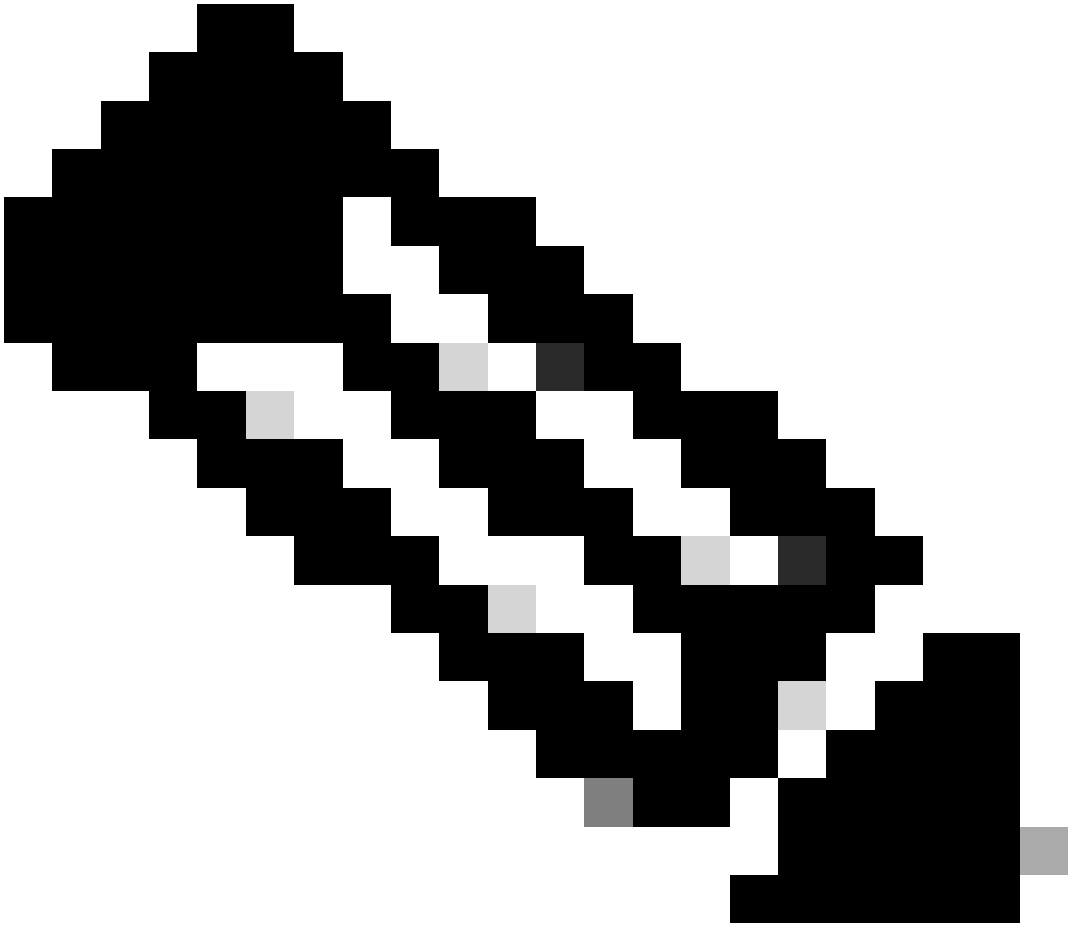
Cliquez sur Per Intrusion Policy selon l'action de règle de la règle personnalisée cible.




Action Modifier la règle

Dans l'écran Modifier l'action de règle, entrez les informations relatives à la stratégie et à l'action de règle.

- Stratégie : snort_test
- Action de la règle : BLOCK



Remarque : les actions de règle sont les suivantes :

Block : génère un événement, bloque le paquet correspondant actuel et tous les paquets suivants de cette connexion.

Alerte : génère uniquement des événements pour le paquet correspondant et ne supprime pas le paquet ou la connexion.

Rewrite : génère un événement et écrase le contenu du paquet en fonction de l'option replace de la règle.

Pass : aucun événement n'est généré, permet au paquet de passer sans autre évaluation par les règles Snort suivantes.

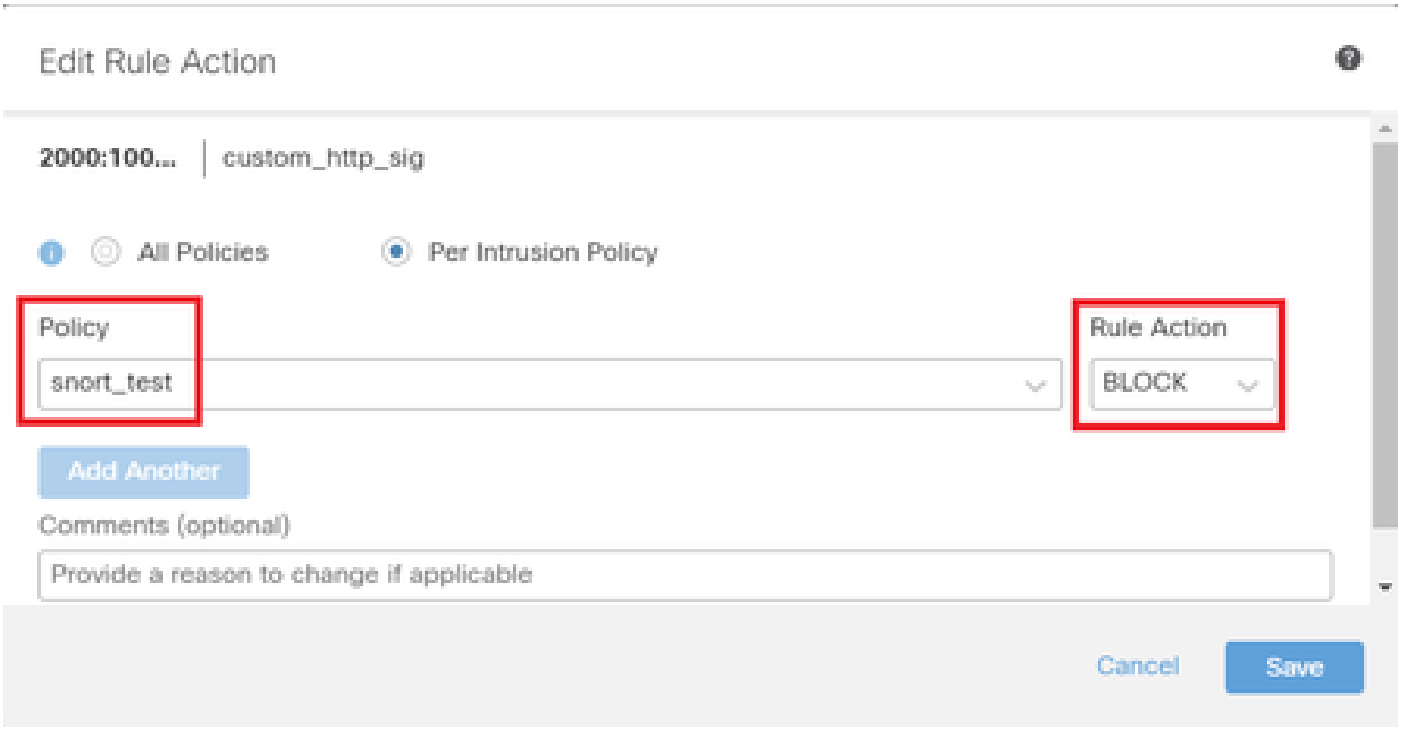
Drop : génère un événement, abandonne le paquet correspondant et ne bloque pas le trafic supplémentaire dans cette connexion.

Reject : génère un événement, abandonne le paquet correspondant, bloque le trafic supplémentaire dans cette connexion et envoie la réinitialisation TCP s'il s'agit d'un

protocole TCP aux hôtes source et de destination.

Disable : ne fait pas correspondre le trafic avec cette règle. Aucun événement n'est généré.

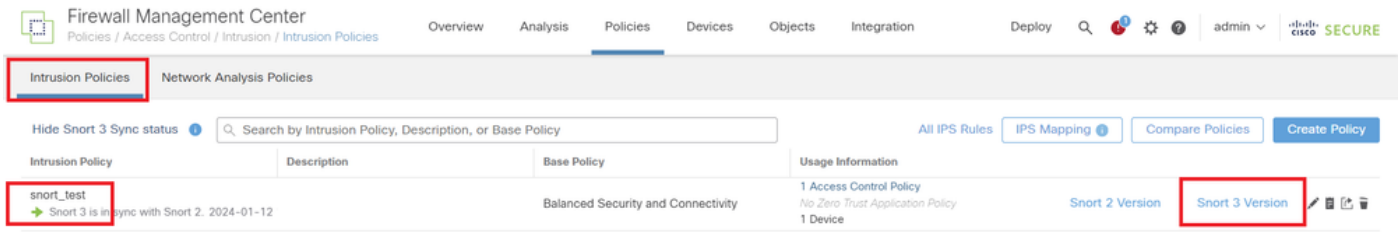
Par défaut : rétablit l'action par défaut du système.




Action Modifier la règle

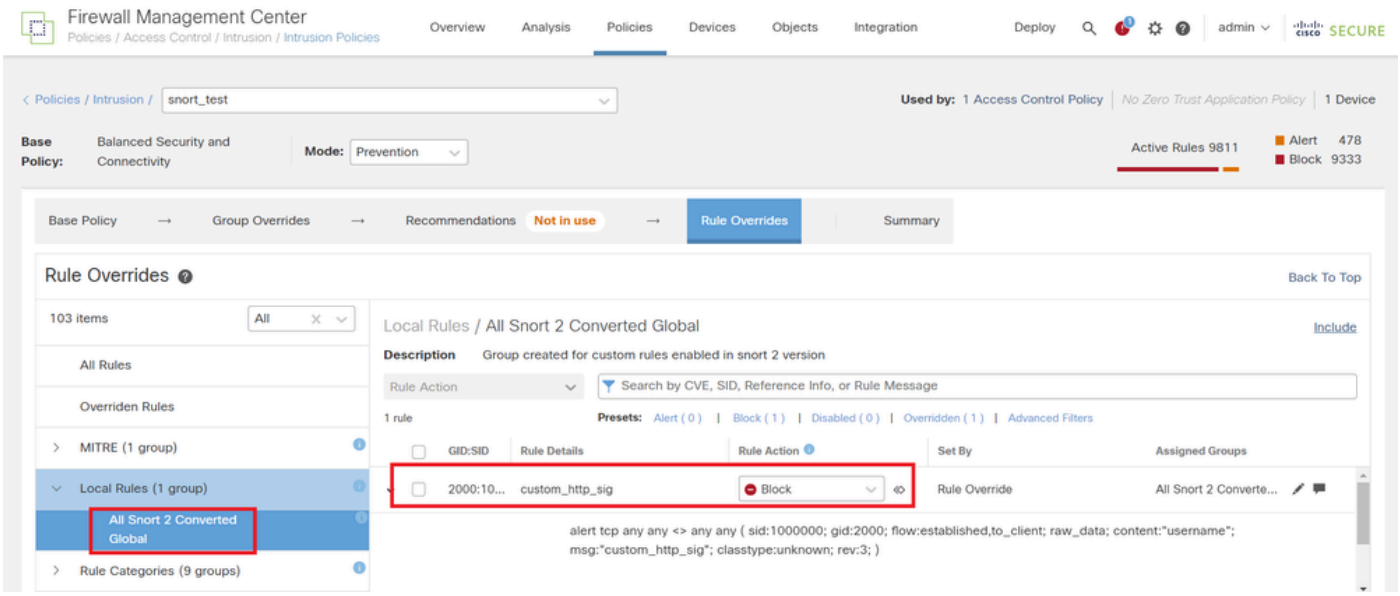
Étape 5. Confirmer la règle de sniffage local personnalisée importée

Accédez à Policies > Intrusion Policies sur FMC, cliquez sur Snort 3 Version correspondant à la stratégie d'intrusion cible dans la ligne.




Confirmer la règle personnalisée importée

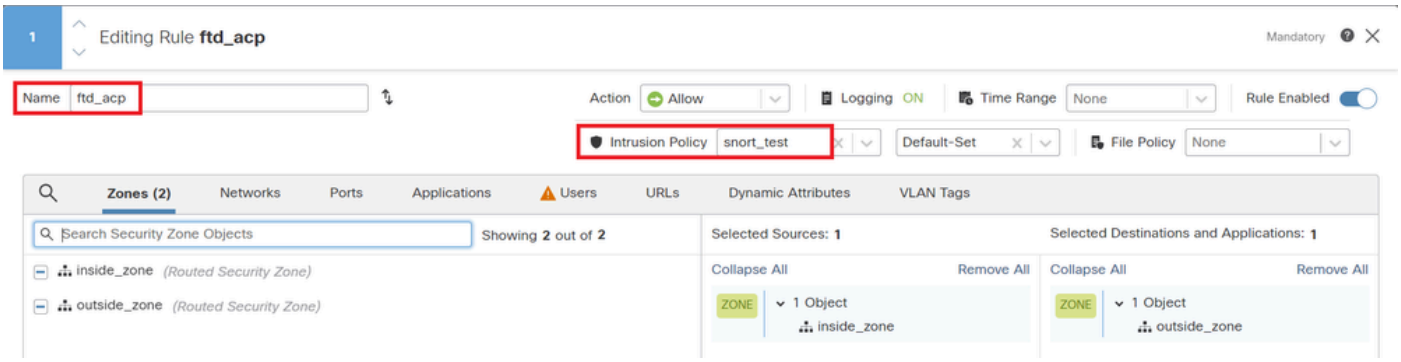
Cliquez sur Local Rules > All Snort 2 Converted Global pour vérifier les détails de la règle de snort local personnalisée.




Confirmer la règle personnalisée importée

Étape 6. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)

Accédez à Politiques>Contrôle d'accès sur FMC, associez la politique d'intrusion à ACP.




Associer à la règle ACP

Étape 7. Déployer les modifications

Déployez les modifications sur FTD.


Déployer les modifications

## Méthode 2. Télécharger un fichier local

Étape 1. Confirmer la version de Snort

Identique à l'étape 1 de la méthode 1.

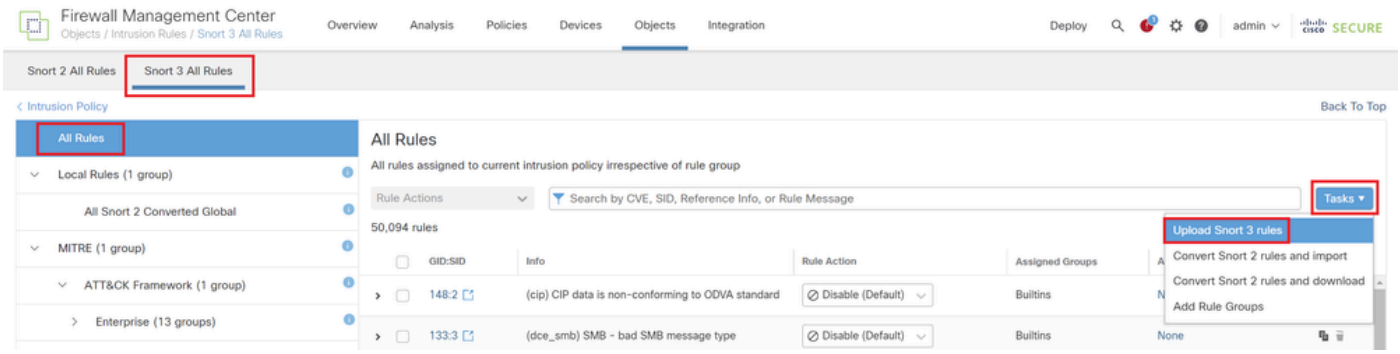
Étape 2. Créer une règle de détection locale personnalisée

Créez manuellement une règle d'analyse locale personnalisée et enregistrez-la dans un fichier local nommé custom-rules.txt.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

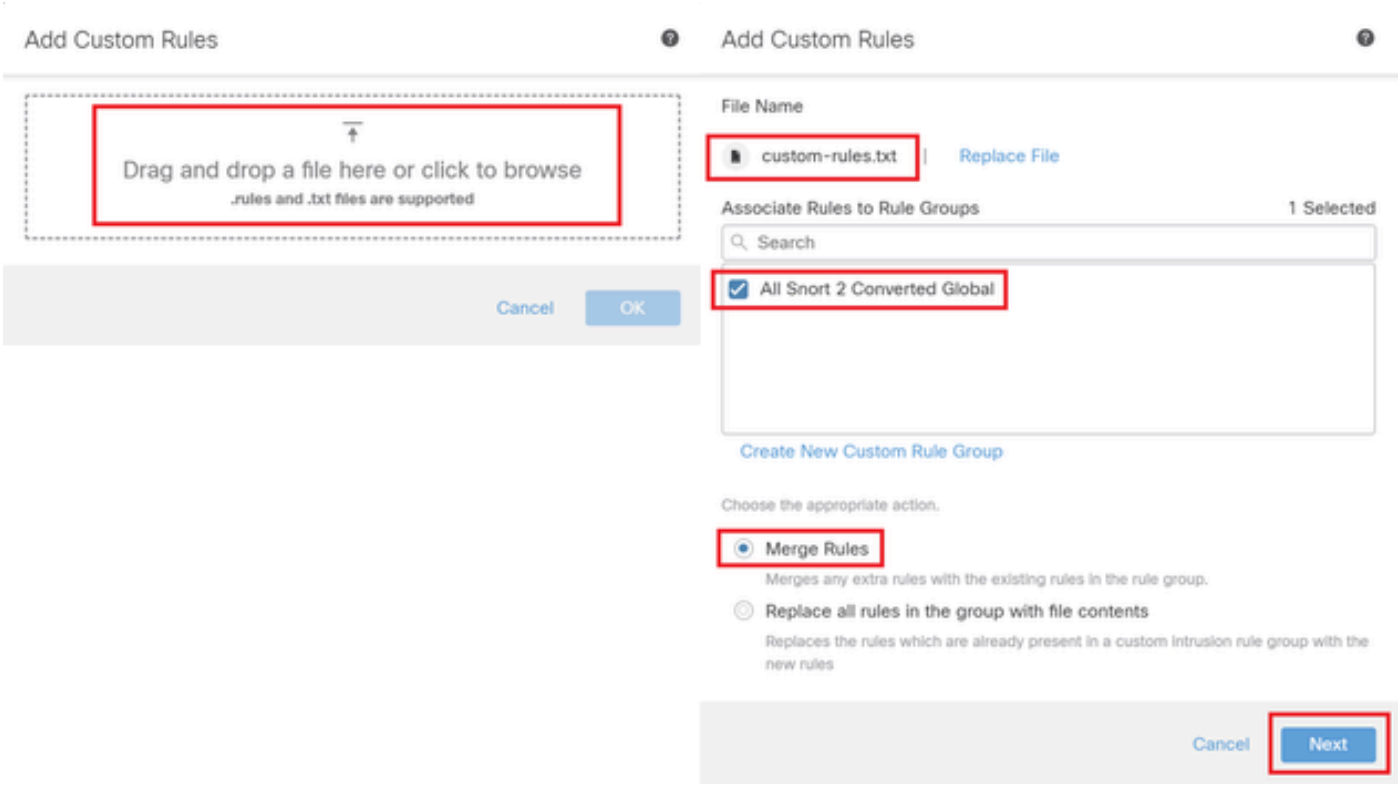
Étape 3. Télécharger la règle de détection locale personnalisée

Accédez à Objets > Règles d'intrusion > Snort 3 All Rules > All Rules sur FMC, cliquez sur Upload Snort 3 rules from Tasks pulldown list.



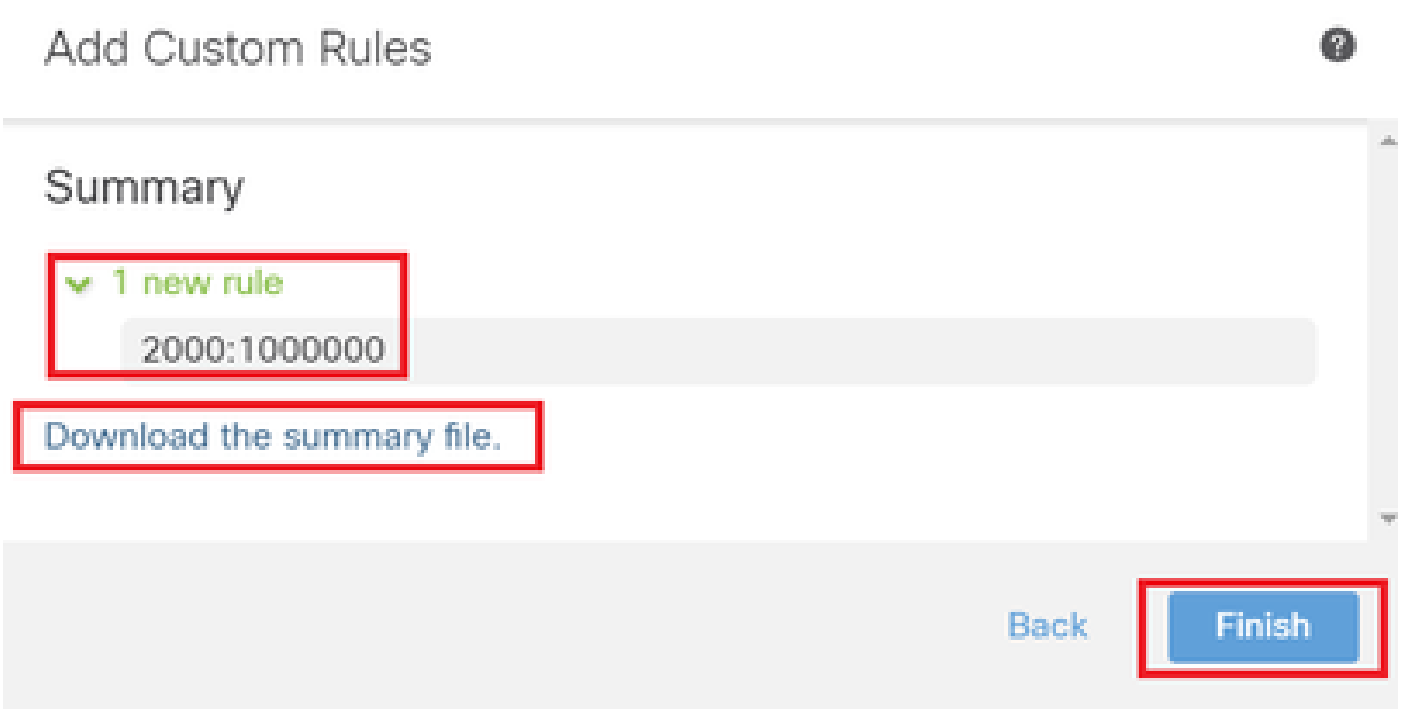

Télécharger une règle personnalisée

Dans l'écran Ajouter des règles personnalisées, faites glisser le fichier custom-rules.txt local, sélectionnez Groupes de règles et l'action appropriée (Fusionner les règles dans cet exemple), puis cliquez sur le bouton Suivant.



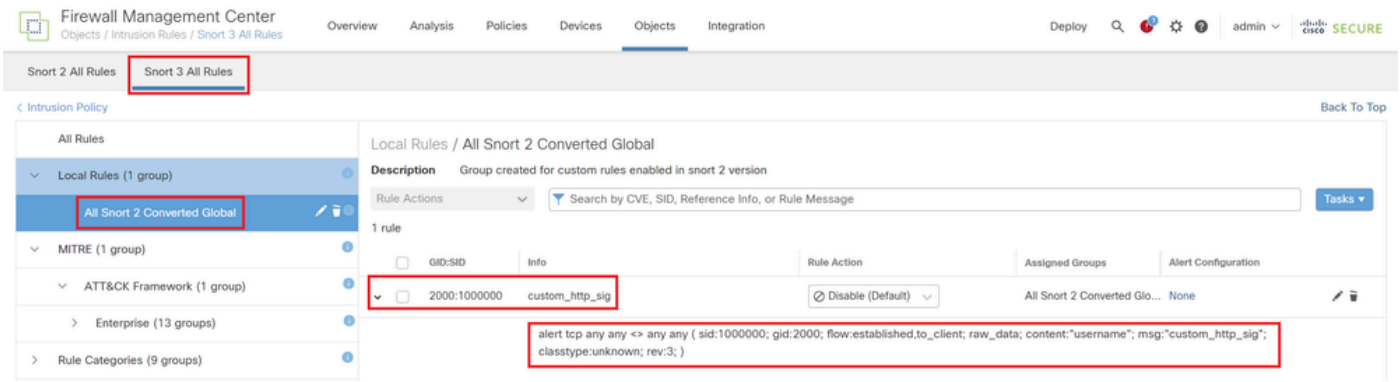

Ajouter une règle personnalisée

Vérifiez que le fichier de règle locale a bien été téléchargé.




Confirmer le résultat du téléchargement

Accédez à Objects > Intrusion Rules > Snort 3 All Rules sur FMC, cliquez sur All Snort 2 Converted Global pour confirmer la règle de détection locale personnalisée téléchargée.




Détail de la règle personnalisée

Étape 4. Action Modifier la règle

Identique à l'étape 4 de la méthode 1.

Étape 5. Confirmer la règle de détection locale personnalisée téléchargée

Identique à l'étape 5 de la méthode 1.

Étape 6. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)

Identique à l'étape 6 de la méthode 1.

Étape 7. Déployer les modifications

Identique à l'étape 7 de la méthode 1.

# Vérifier

Étape 1. Définition du contenu du fichier dans le serveur HTTP

Définissez le contenu du fichier test.txt côté serveur HTTP sur username.

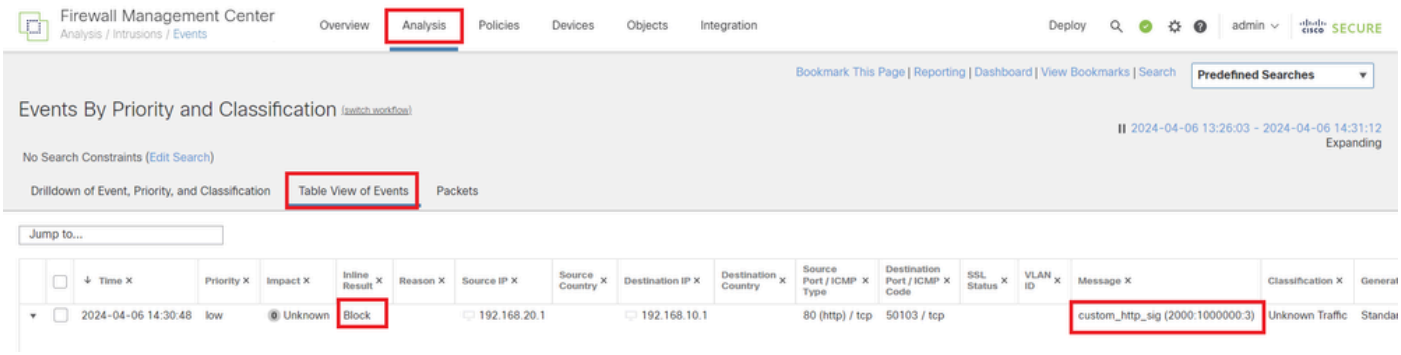
Étape 2. Requête HTTP initiale

Accédez au serveur HTTP (192.168.20.1/test.txt) à partir du navigateur du client (192.168.10.1) et vérifiez que la communication HTTP est bloquée.


Requête HTTP initiale

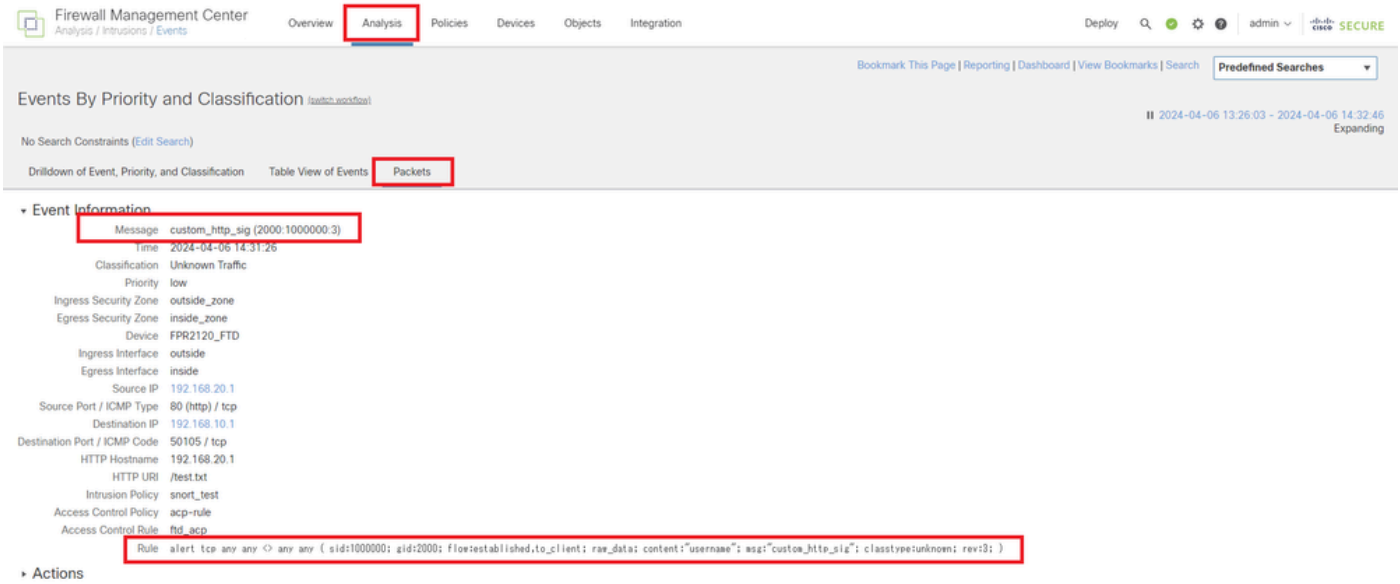
Étape 3. Confirmer l'incident

Accédez àAnalyse>Intrusions>ÉvénementsDans FMC, vérifiez que l'événement d'intrusion est généré par la règle de détection locale personnalisée.




Événement D'Intrusion

Cliquez sur l'onglet Paquets, confirmez les détails de l'événement Intrusion.




Détail de l'incident

# Foire aux questions (FAQ)

Q : Lequel est recommandé ? Snort 2 ou Snort 3 ?
R : Par rapport à Snort 2, Snort 3 offre des vitesses de traitement améliorées et de nouvelles fonctionnalités, ce qui en fait l'option la plus recommandée.

Q : Après la mise à niveau d'une version de FTD antérieure à 7.0 vers une version 7.0 ou ultérieure, la version de Snort est-elle automatiquement mise à jour vers Snort 3 ?
R : Non, le moteur d'inspection reste sur Snort 2. Pour utiliser Snort 3 après la mise à niveau, vous devez l'activer explicitement. Notez que Snort 2 est prévu pour être déconseillé dans une prochaine version et il est fortement recommandé d'arrêter de l'utiliser maintenant.

Q : Dans Snort 3, est-il possible de modifier une règle personnalisée existante ?
R : Non, vous ne pouvez pas le modifier. Pour modifier une règle personnalisée spécifique, vous devez la supprimer et la recréer.

# Dépannage

Exécutez system support trace la commande pour confirmer le comportement sur FTD. Dans cet exemple, le trafic HTTP est bloqué par la règle IPS (2000:1000000:3).

<#root>

>

**system support trace**

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
```

```
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '

ftd_acp

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

Event

:

2000:1000000:3

, Action

block


192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

ips, block
```

Référence

Guide de configuration de Cisco Secure Firewall Management Center Snort 3

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.