Configurer des règles de sniffage local personnalisées dans Snort2 sur FTD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configuration
    - Étape 1. Confirmer la version Snort
    - Étape 2. Créer une règle de détection locale personnalisée dans Snort 2
    - Étape 3. Confirmer la règle de détection locale personnalisée
    - Étape 4. Action Modifier la règle
    - Étape 5. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)
    - Étape 6. Déployer les modifications
- Vérifier
  - La règle d'analyse locale personnalisée n'est pas déclenchée
    - Étape 1. Définition du contenu du fichier dans le serveur HTTP
    - Étape 2. Requête HTTP initiale
  - La règle d'analyse locale personnalisée est déclenchée
    - Étape 1. Définition du contenu du fichier dans le serveur HTTP
    - Étape 2. Requête HTTP initiale
    - Étape 3. ConfirmIntrusion, événement
- Dépannage

Introduction

Ce document décrit la procédure pour configurer des règles de détection locale personnalisées dans Snort2 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 :

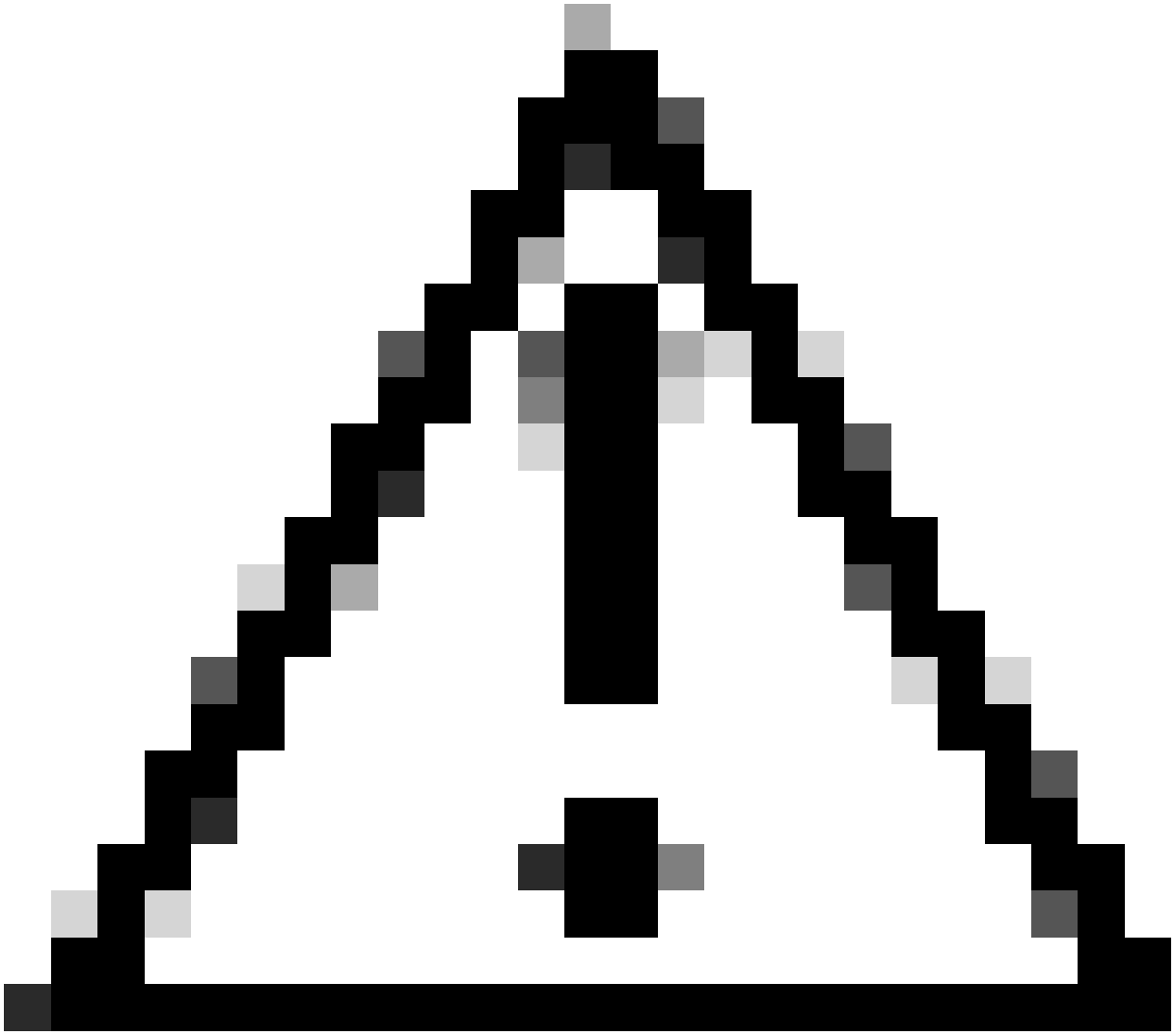
- Cisco Firepower Management Center pour VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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 règle Snort locale personnalisée fait référence à une règle définie par l'utilisateur que vous pouvez créer et mettre en oeuvre dans le système de détection et de prévention des intrusions Snort intégré au FTD. Lorsque vous créez une règle Snort locale personnalisée dans Cisco FTD, vous définissez essentiellement un nouveau modèle ou un nouvel ensemble de conditions que le moteur Snort peut surveiller. Si le trafic réseau correspond aux conditions spécifiées dans votre règle personnalisée, Snort peut effectuer l'action définie dans la règle, comme la génération d'une alerte ou l'abandon du paquet. Les administrateurs utilisent des règles Snort locales personnalisées pour traiter des menaces spécifiques qui ne sont pas couvertes par les ensembles de règles générales.

Dans ce document, vous apprendrez à configurer et à vérifier une règle de détection locale personnalisée conçue pour détecter et supprimer les paquets de réponse HTTP contenant une chaîne spécifique (nom d'utilisateur).

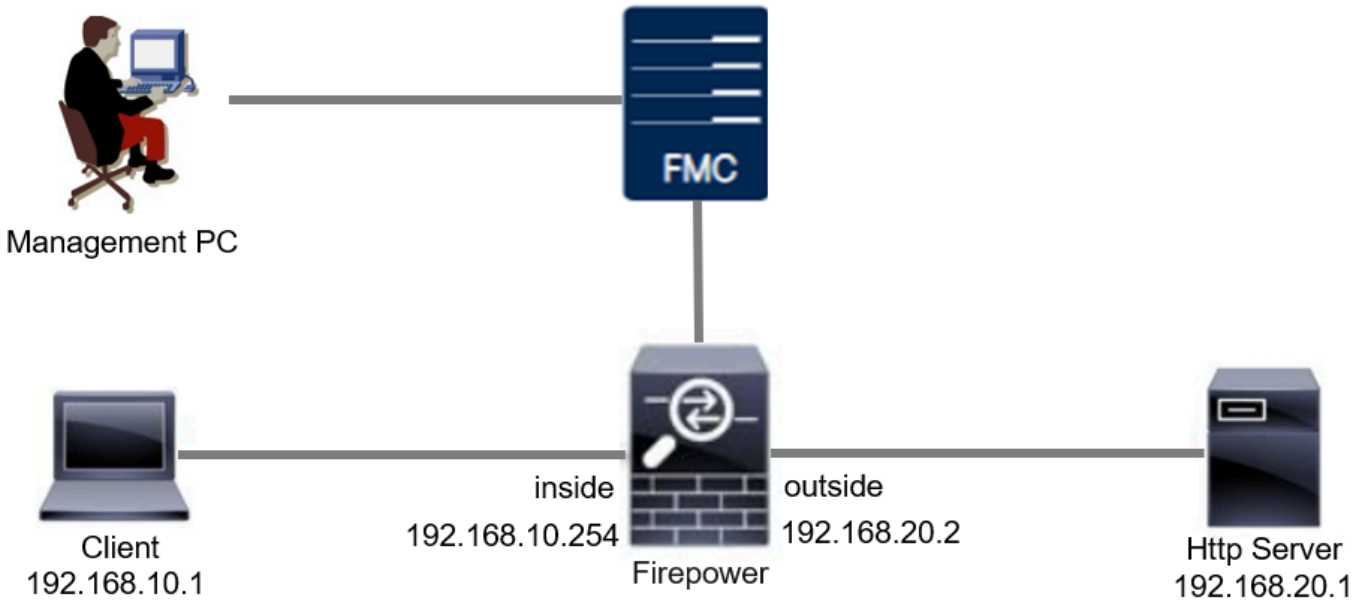


Attention : la création de règles Snort locales personnalisées et leur prise en charge ne sont pas couvertes par le centre d'assistance technique. Par conséquent, ce document ne peut être utilisé qu'à titre de référence et vous demandez de créer et de gérer ces règles personnalisées à votre discrétion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

Configurer

Diagramme du réseau

Ce document présente la configuration et la vérification de la règle de sniffage local personnalisée dans Snort2 sur ce schéma.

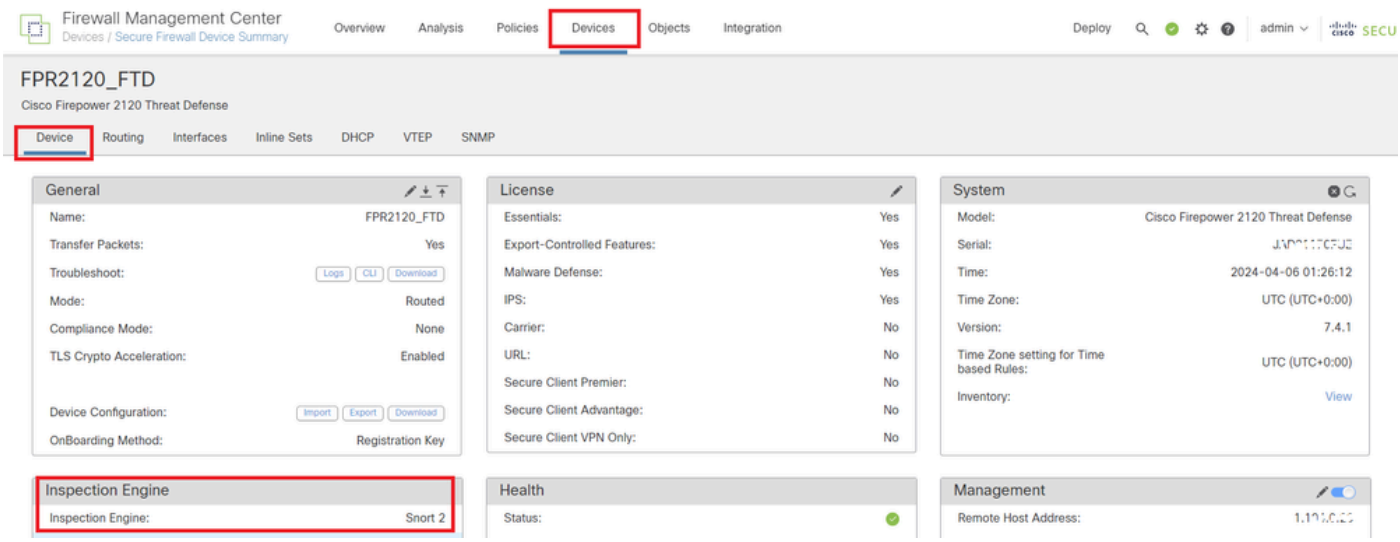


Configuration

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).

Étape 1. Confirmer la version Snort

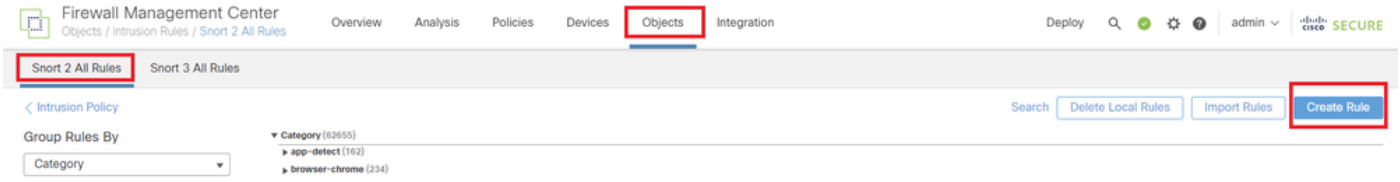
Accédez à Périphériques > Gestion des périphériques sur FMC, cliquez sur l'onglet Périphérique. Confirmation de la version Snort2.



Version Snort

Étape 2. Créer une règle de détection locale personnalisée dans Snort 2

Accédez à Objets > Règles d'intrusion > Snort 2 All Rules sur FMC, cliquez sur le bouton Create Rule .

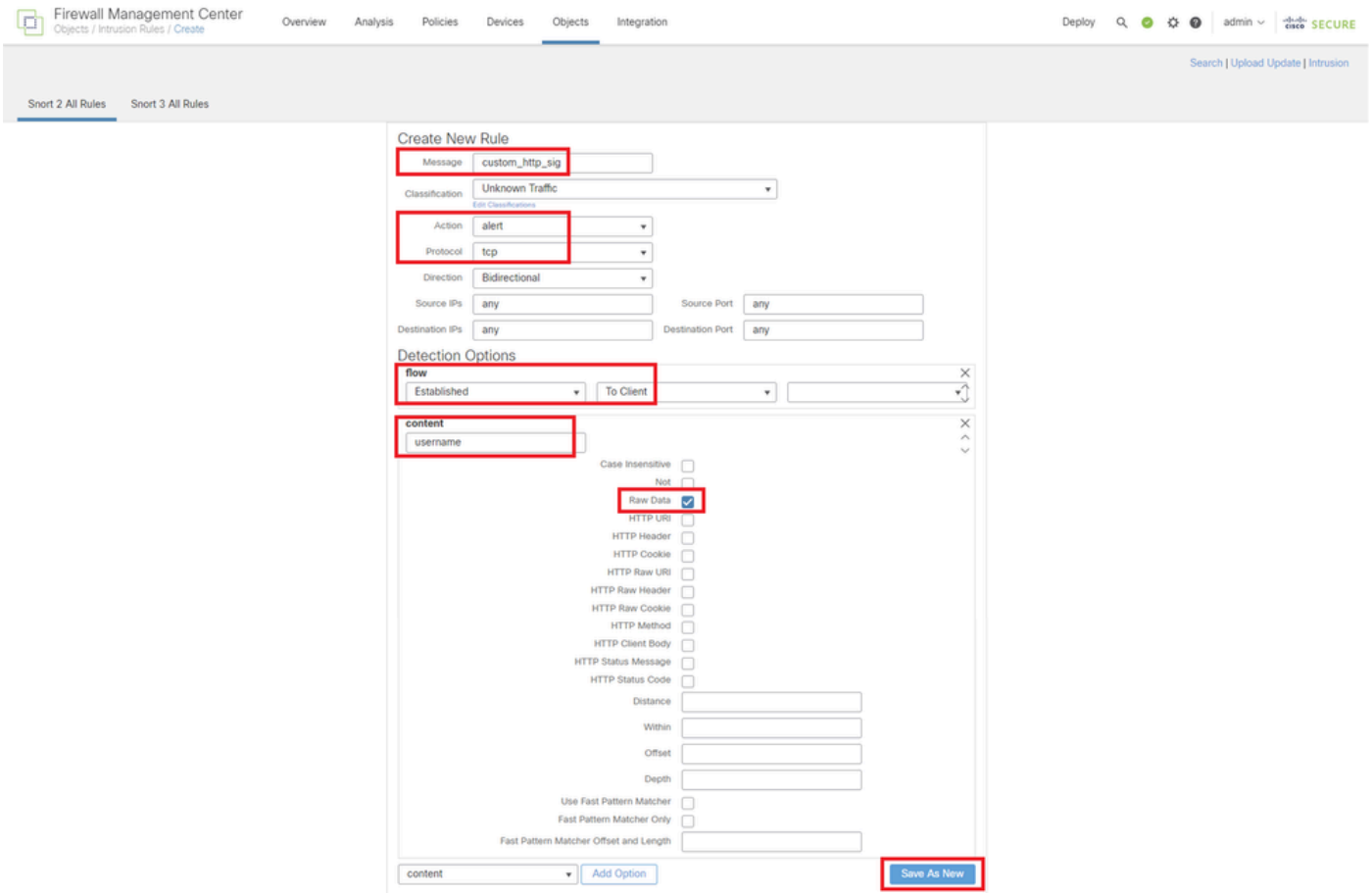


Créer une règle personnalisée

Entrez les informations nécessaires pour la règle de sniffage local personnalisée.

- Intrusion : custom_http_sig
- Action : alerte
- Protocole : TCP
- flux : établi, au client

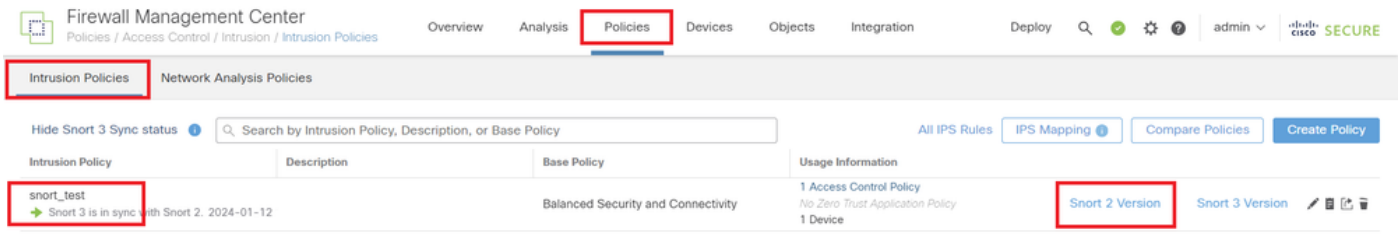
- content : username (Raw Data)



Informations requises pour la règle

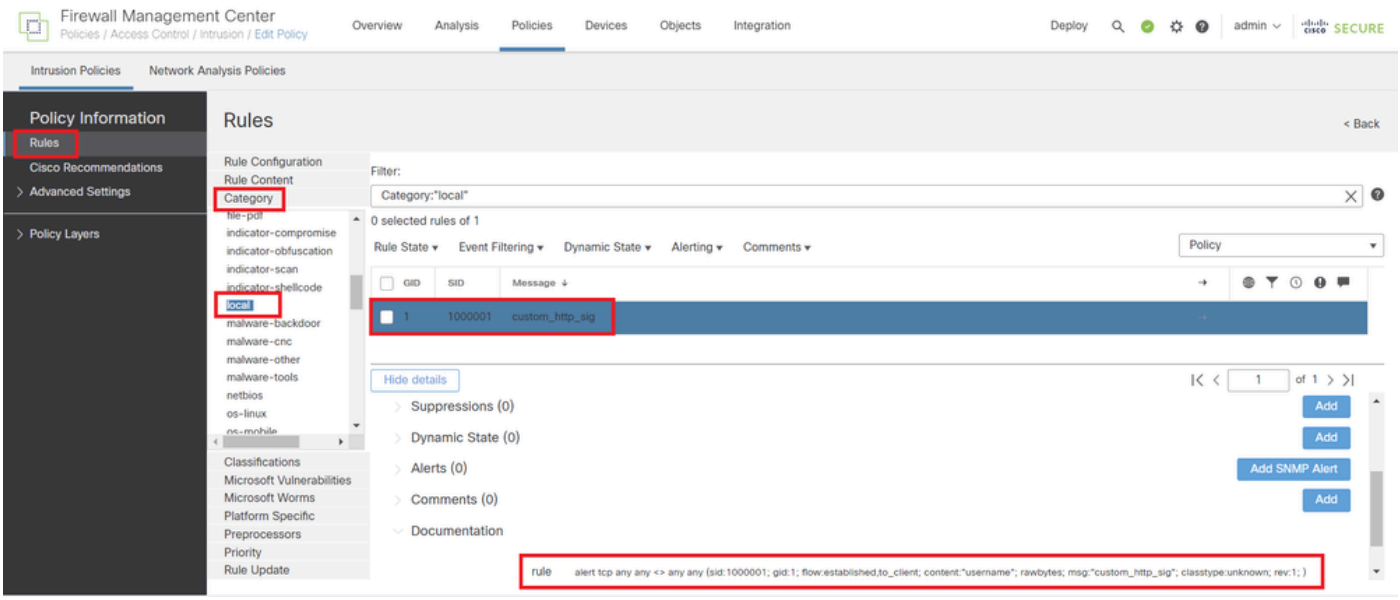
Étape 3. Confirmer la règle de détection locale personnalisée

Accédez à Policies > Intrusion Policies sur FMC, cliquez sur le bouton Snort 2 Version.



Confirmer la règle personnalisée

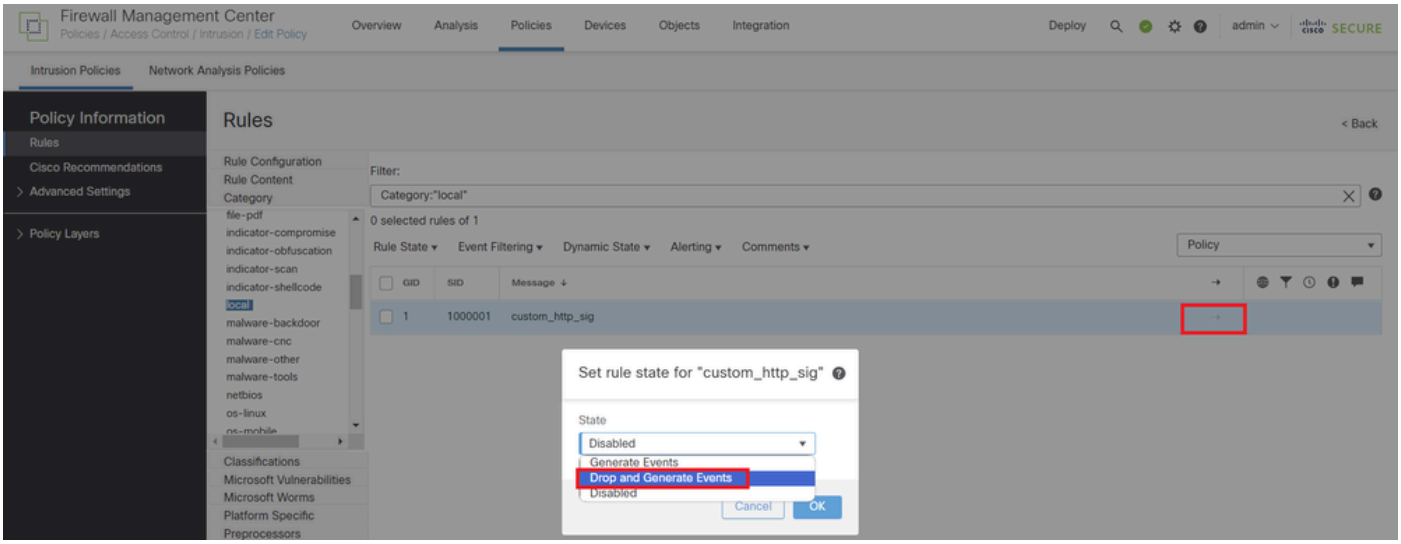
Accédez à Rules > Category > local sur FMC, confirmez le détail de Custom Local Snort Rule.



Détail de la règle personnalisée

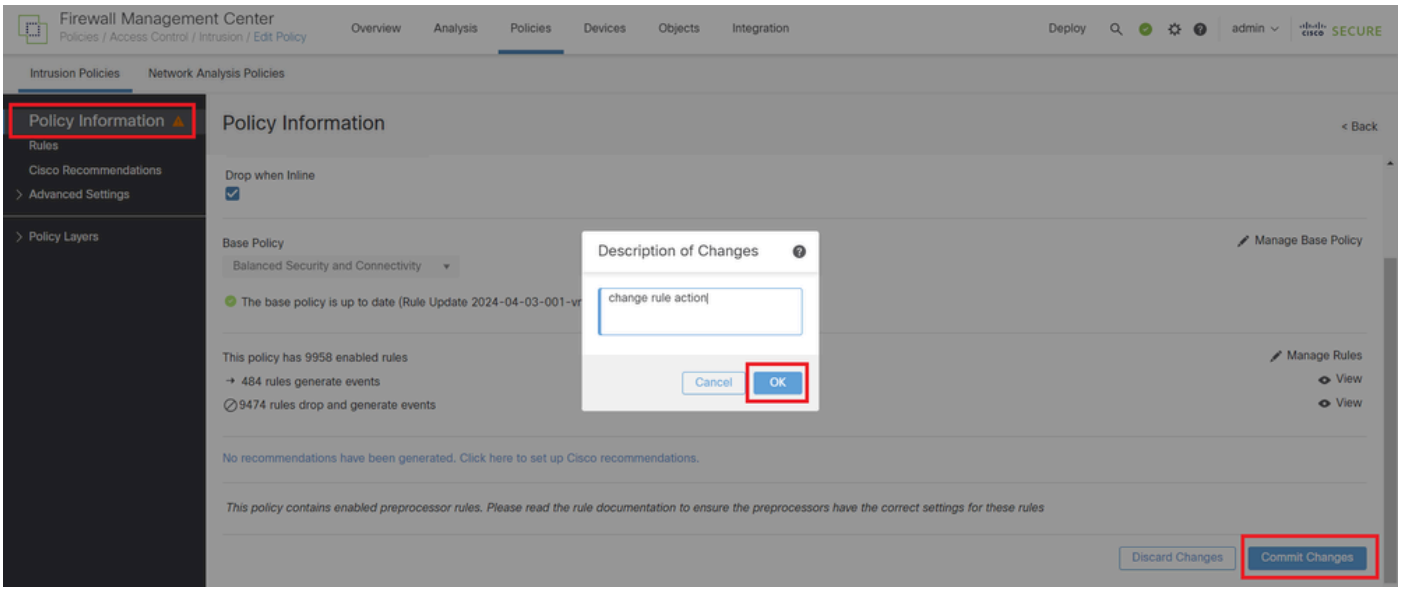
Étape 4. Action Modifier la règle

Cliquez sur le bouton State, définissez l'état sur Drop and Generate Events et cliquez sur le bouton OK.



Action Modifier la règle

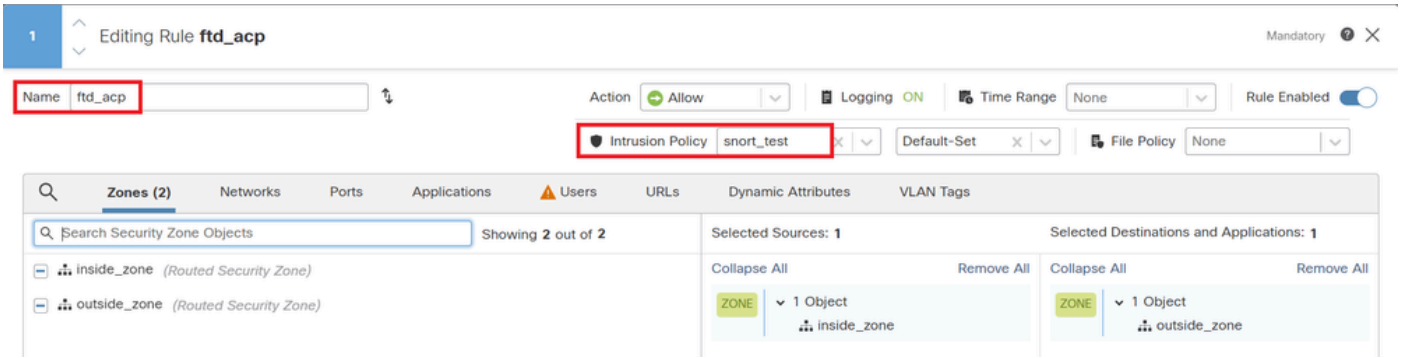
Cliquez sur le bouton Policy Information , cliquez sur Commit Changes pour enregistrer les modifications.



Valider les modifications

Étape 5. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)

Accédez à Policies > Access Control sur FMC, associez Intrusion Policy à ACP.



Associer à la règle ACP

Étape 6. Déployer les modifications

Déployez les modifications sur FTD.

Déployer les modifications

Vérifier

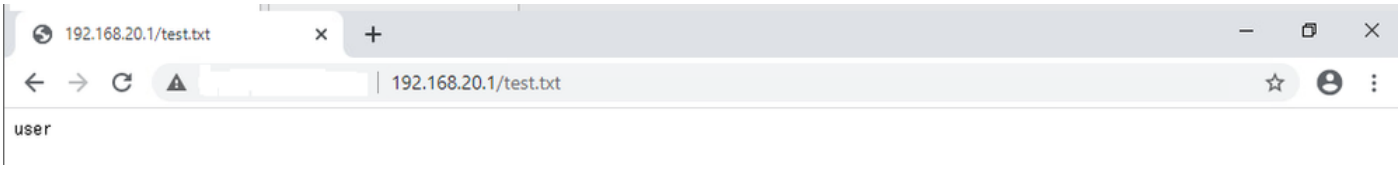
La règle d'analyse locale personnalisée n'est pas déclenchée

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

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

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 autorisée.



Requête HTTP initiale

La règle d'analyse locale personnalisée est déclenchée

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

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

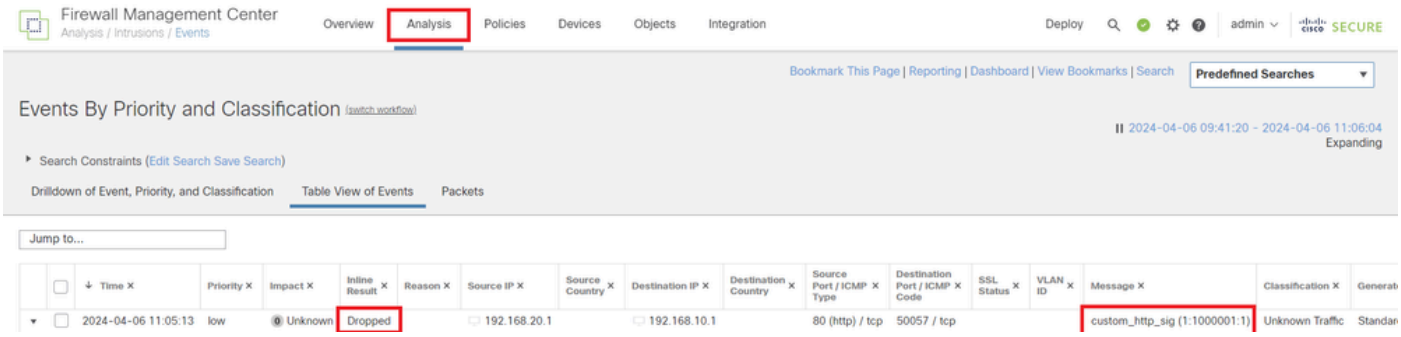
Étape 2. Requête HTTP initiale

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

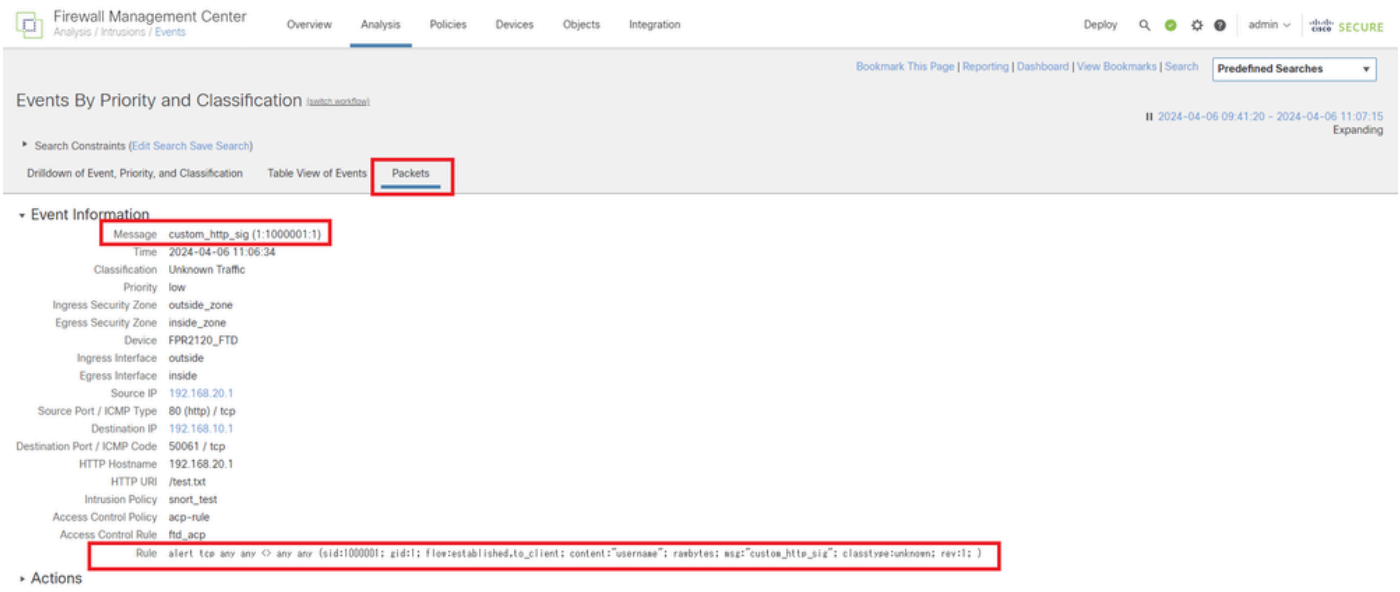
Étape 3. Confirmer l'incident

Accédez à Analysis > Intrusions > Events sur FMC, confirmez que l'événement d'intrusion est généré par la règle de détection locale personnalisée.



Événement D'Intrusion

Cliquez sur l'onglet Packets, confirmez le détail de l'événement Intrusion.



Détail de l'incident

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 (gid 1, sid 1000001).

```
<#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:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

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.