Filtrer les règles de détection en fonction de la version SRU et LSP des périphériques Firepower gérés par FMC

Table des matières

Introduction

Ce document décrit comment filtrer les règles de détection basées sur la version Cisco Secure Rule Update (SRU) et Link State Packet (LSP) des périphériques firepower gérés par le centre de gestion Firepower (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de l'open source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Composants utilisés

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

- Cet article s'applique à toutes les plates-formes Firepower
- Cisco Firepower Threat Defense (FTD), qui exécute la version 7.0.0 du logiciel
- Firepower Management Center Virtual (FMC) qui exécute la version 7.0.0 du logiciel

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

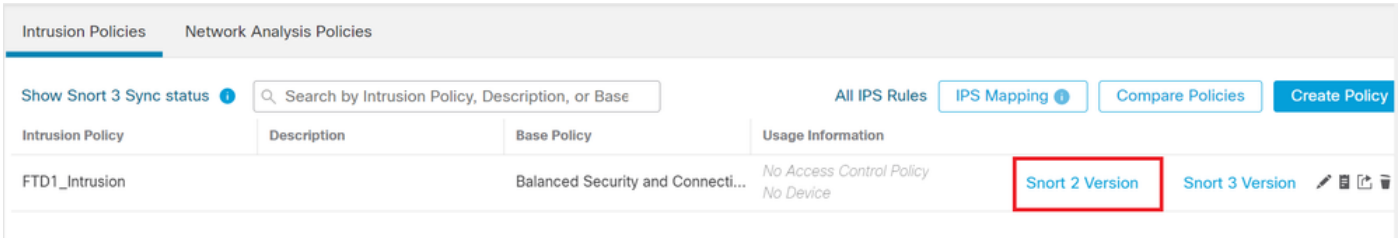
Dans le contexte des systèmes de détection des intrusions (IDS) et des systèmes de prévention des intrusions (IPS), « SID » signifie « Signature ID » ou « Snort Signature ID ».

Un SID (Snort Signature ID) est un identifiant unique attribué à chaque règle ou signature dans son ensemble de règles. Ces règles sont utilisées pour détecter des modèles ou des comportements spécifiques dans le trafic réseau qui peuvent indiquer une activité malveillante ou des menaces pour la sécurité. Chaque règle est associée à un SID pour faciliter la référence et la gestion.

Pour plus d'informations sur l'open-source Snort, veuillez visiter le site web SNORT.

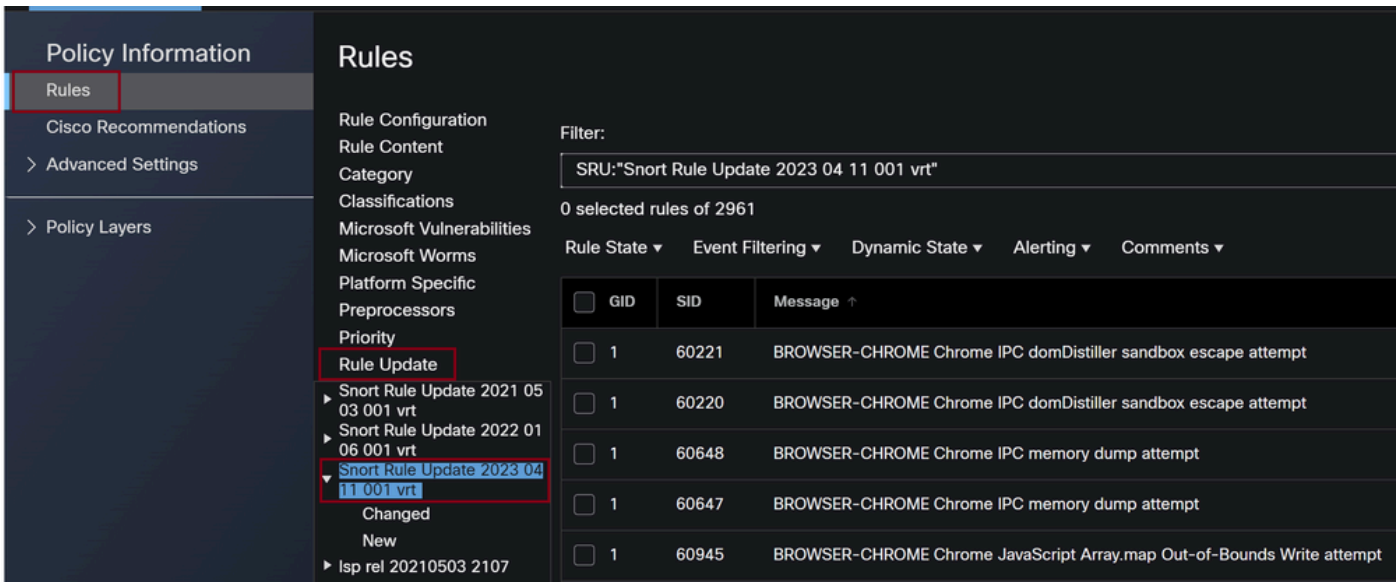
Procédure de filtrage des règles Snort

Pour afficher les SID de la règle Snort 2, accédez à FMC Policies > Access Control > Intrusion, cliquez ensuite sur l'option SNORT2 dans l'angle supérieur droit, comme indiqué dans l'image :

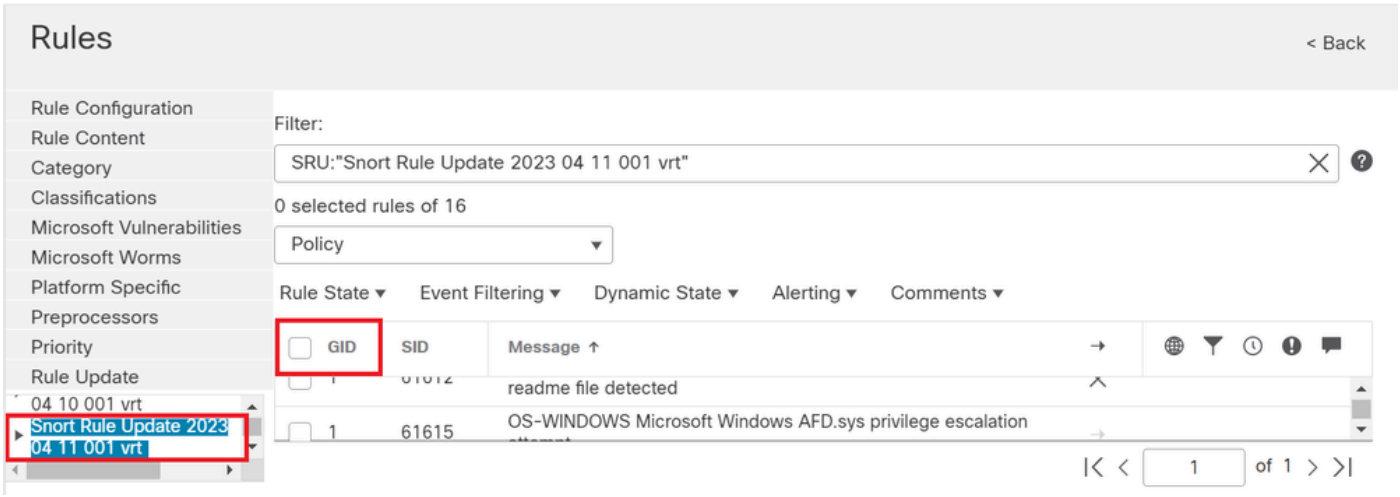


Snort 2

Naviguez jusqu'à Rules > Rule Update et sélectionnez la dernière date pour filtrer le SID.

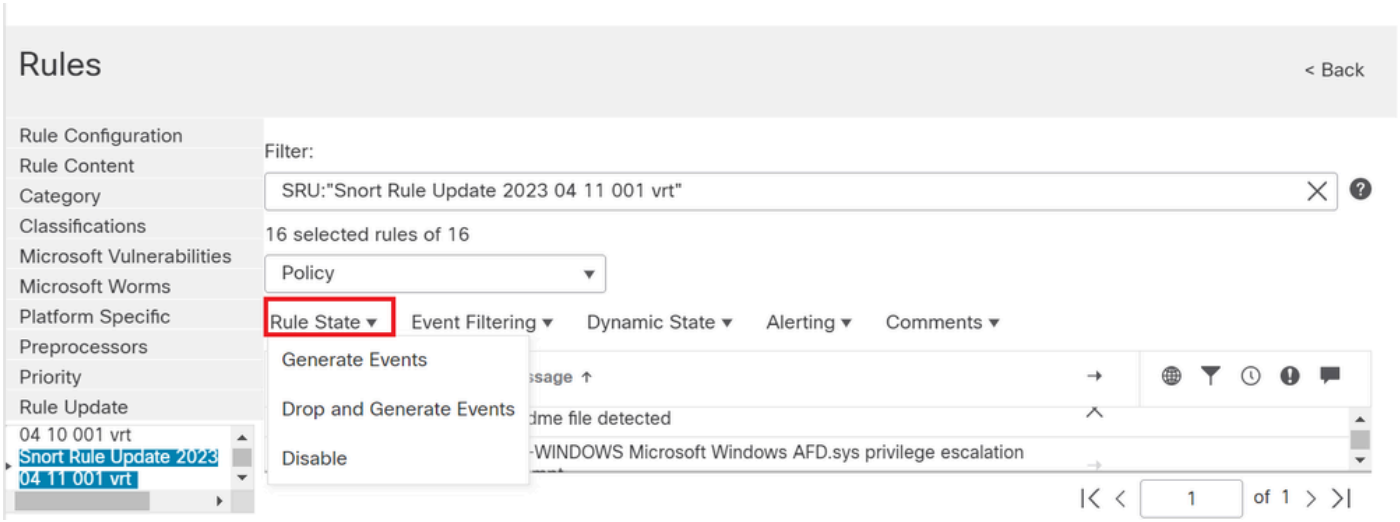


Mise à jour des règles



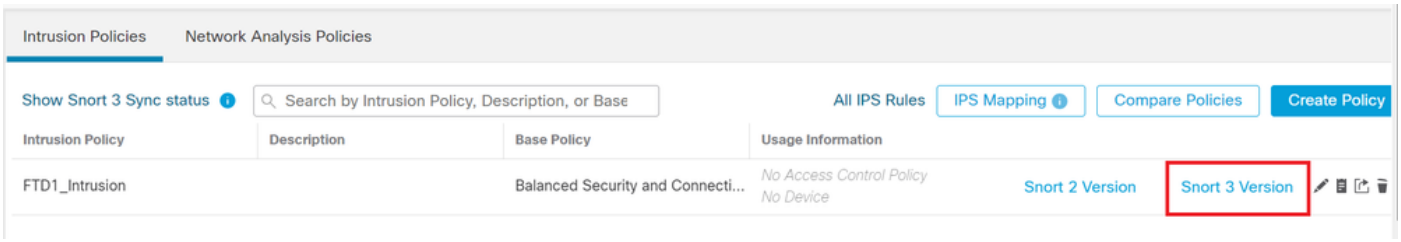
Disponible Sid's sous les règles de snort

Sélectionnez une option requise sous Rule State comme illustré dans l'image.



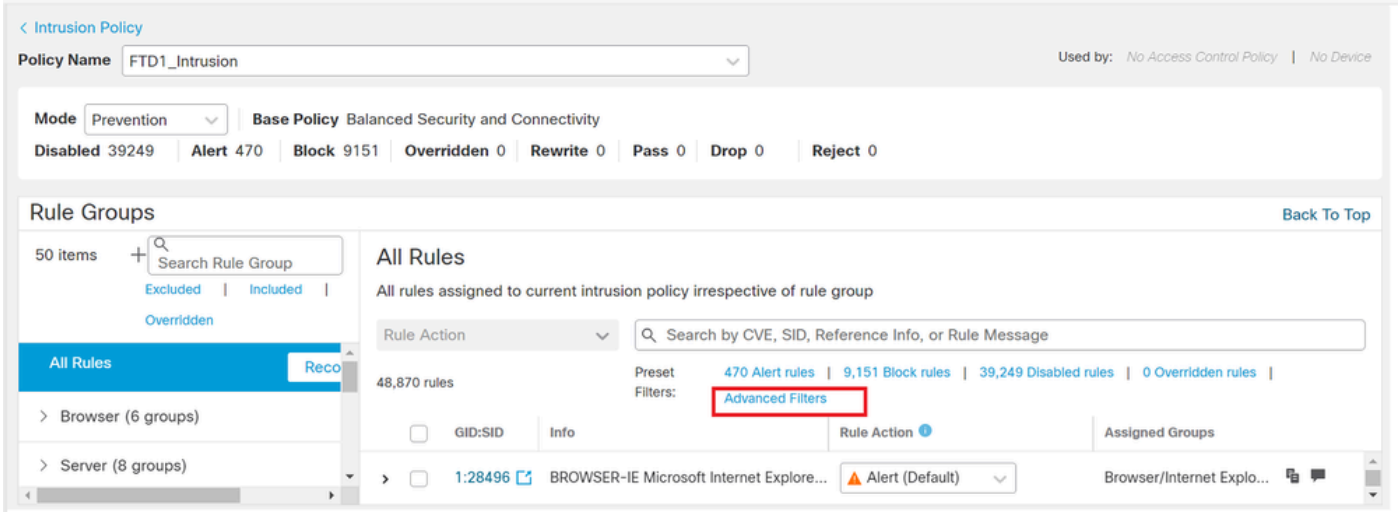
Sélection des états de règle

Pour afficher les SID de la règle Snort 3, accédez à FMC Policies > Access Control > Intrusion , puis cliquez sur l'option SNORT3 dans l'angle supérieur droit, comme indiqué dans l'image :

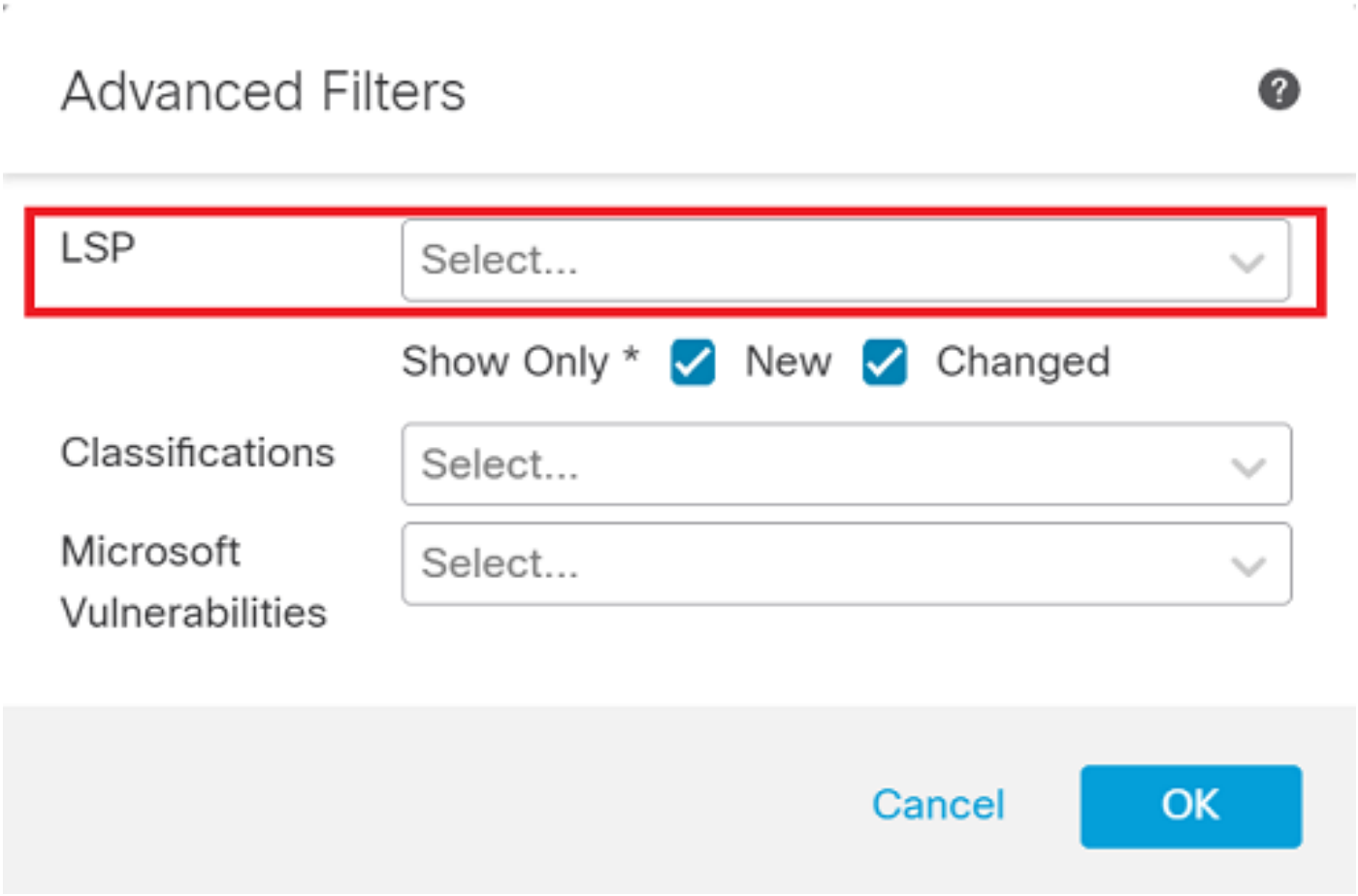


Snort 3

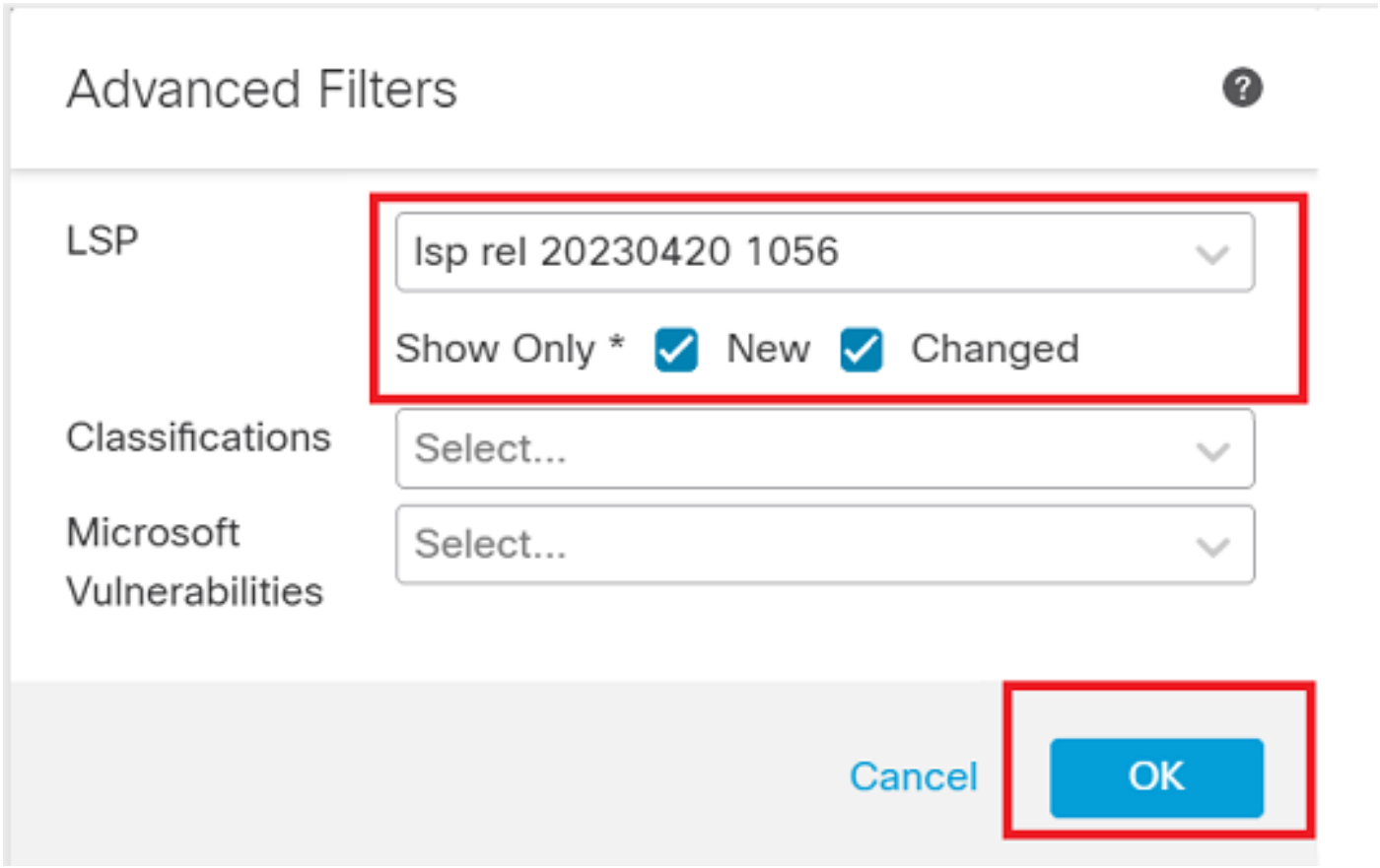
Naviguez jusqu'à Advanced Filters et sélectionnez la date la plus récente pour filtrer le SID comme indiqué dans l'image.



Filtres Snort 3



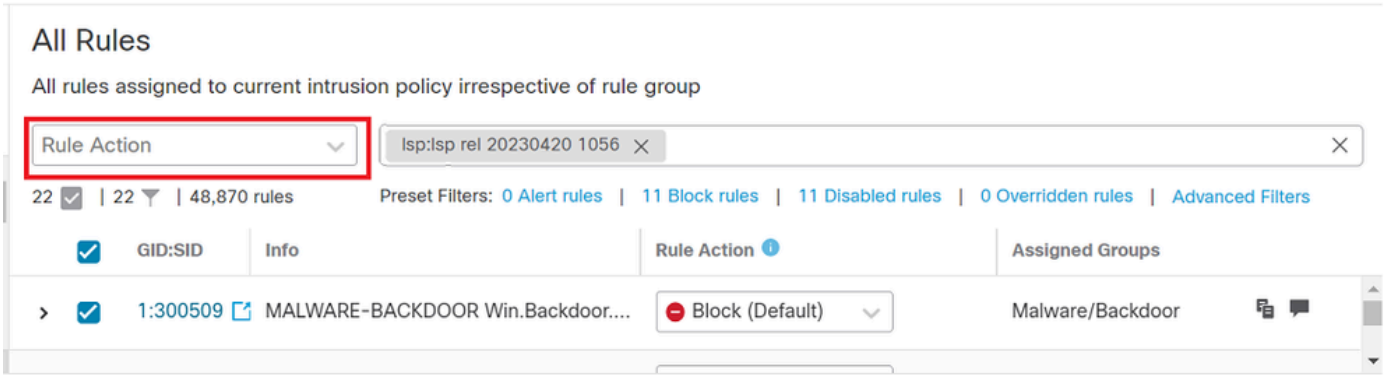
LSP sous filtre avancé



version LSP

Filtre prédéfini pour les Sid

Sélectionnez une option requise sous Rule state comme illustré dans l'image.



Action Règle

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.