Configurer des actions de règle Snort 3 supplémentaires sur FMC

Table des matières

Introduction

Ce document décrit la prise en charge par Firepower Management Center (FMC) de la fonctionnalité d'actions de règles supplémentaires Snort 3 ajoutée dans la version 7.1.

Informations générales

Bien que la défense contre les menaces Firepower (FTD) prenne en charge sept actions de règle de stratégie d'intrusion Alert/Disable/Block/Reject/Rewrite/Pass/Drop dans 7.0, FMC ne prend en charge que trois actions de règle Snort 3 : « Alerte », « Désactiver » et « Bloquer ».

Depuis Firepower 7.1.0, FMC prend en charge pour configurer de nouvelles actions de règle.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :
· Connaissance de l'open source Snort
· Firepower Management Center (FMC) 7.1.0+
· Firepower Threat Defense (FTD) 7.0.0+

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
· Ce document s'applique à toutes les plates-formes Firepower exécutant Snort 3
· Cisco Firepower Threat Defense Virtual (FTD) qui exécute la version 7.4.2 du logiciel
· Firepower Management Center Virtual (FMC) qui exécute la version 7.4.2 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.

Détails des fonctionnalités

Les nouvelles actions de règle Snort 3 ajoutées et leurs descriptions sont les suivantes :

Passe : Aucun événement généré, permet au paquet de passer sans autre évaluation par les règles Snort suivantes.

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

Rejeter : Génère un événement, abandonne le paquet correspondant, bloque le trafic supplémentaire dans cette connexion et envoie la réinitialisation TCP ou le port ICMP inaccessible aux hôtes source et de destination.

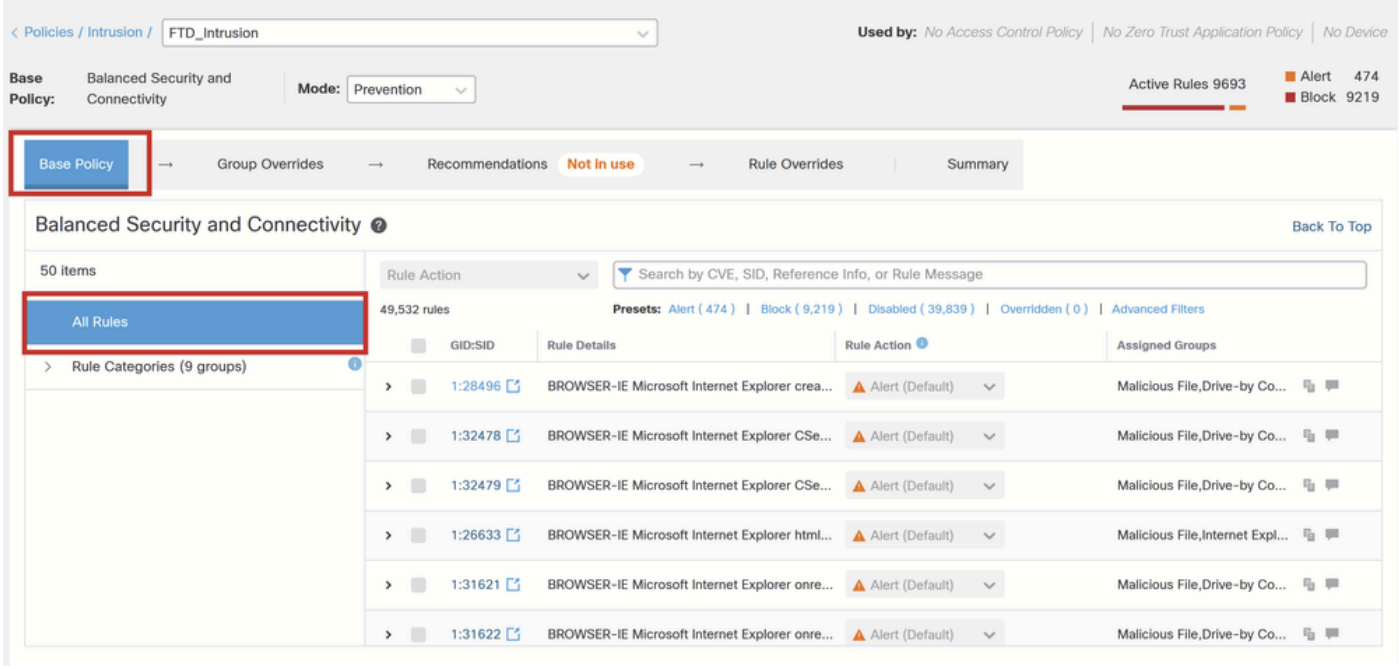
Réécrire : Génère un événement et écrase le contenu du paquet en fonction de l'option replace de la règle.

Procédure pas à pas FMC

Pour afficher les règles Snort 3 dans une stratégie d'intrusion, accédez àFMC Policies > Access Control > Intrusion,puis cliquez sur l'option Snort 3 Version dans le coin supérieur droit de la stratégie, comme illustré dans l'image :

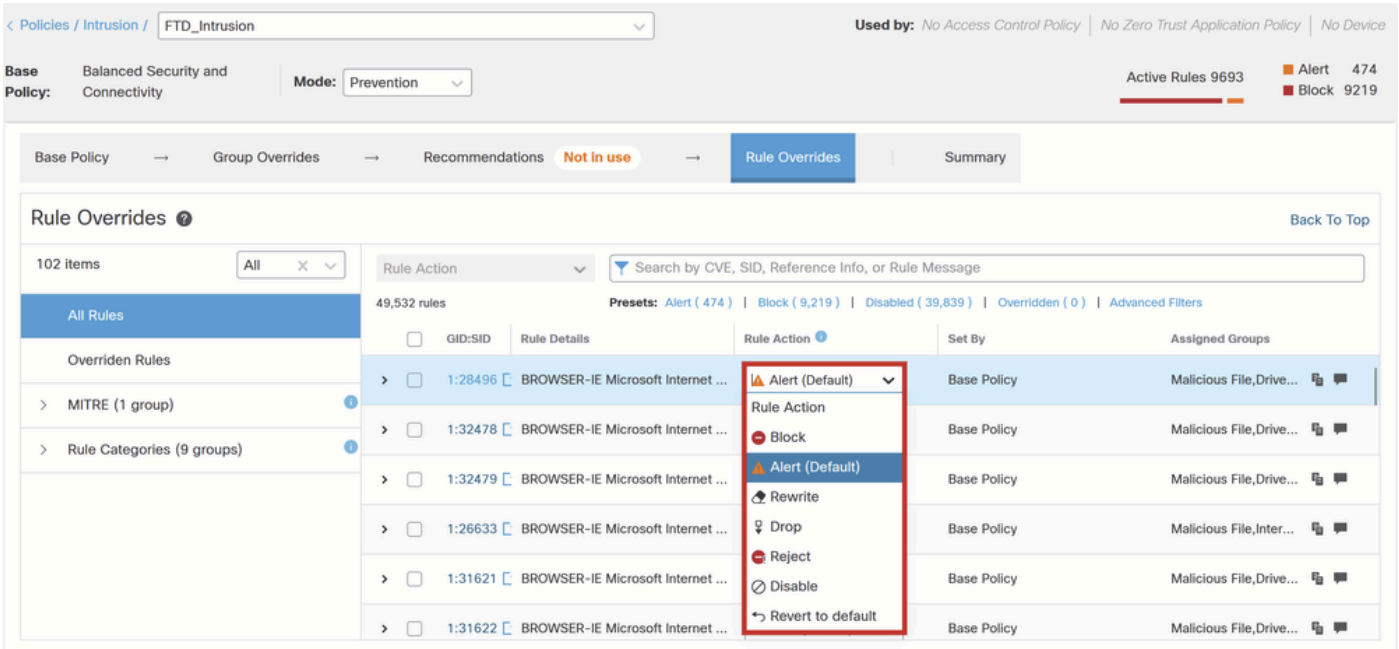
Version Snort 3

Cliquez sur Base Policy > All Rules, vous pouvez voir les actions par défaut de toutes les règles Snort 3 définies par le système.

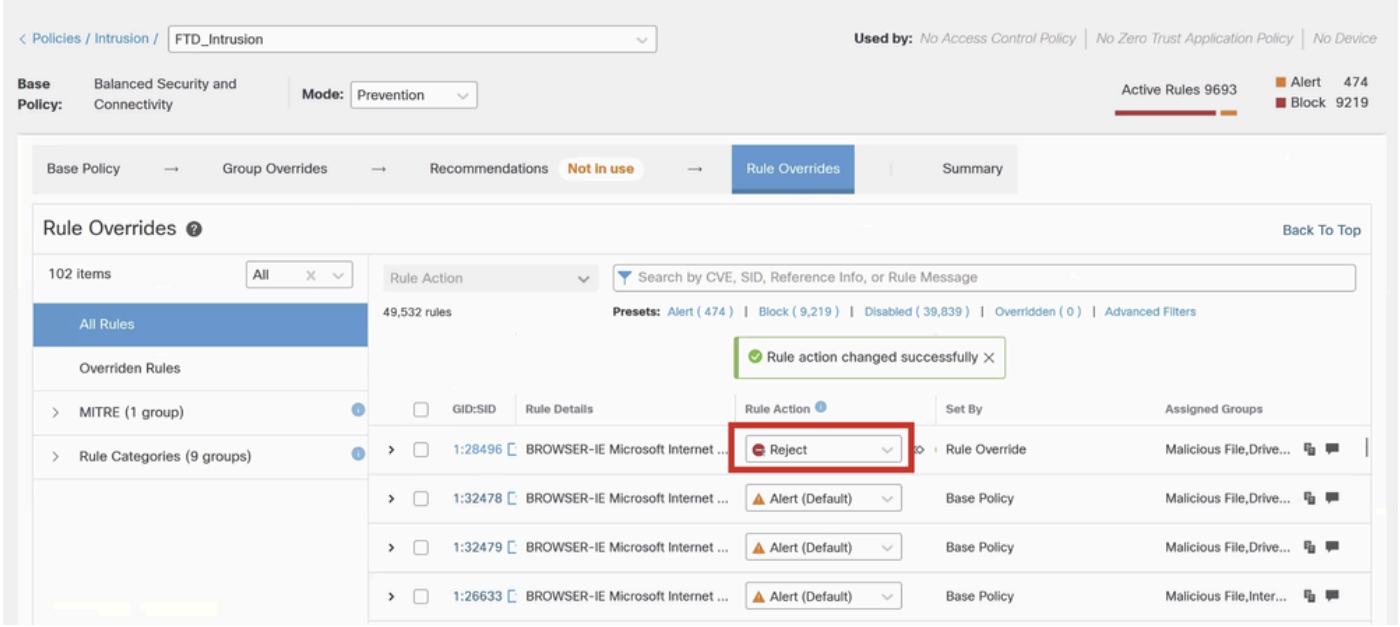


Politique de base

Pour modifier l'action de règle en une de ces nouvelles actions de règle, accédez à Remplacements de règle > Toutes les règles et sélectionnez l'action de règle dans la liste déroulante pour la règle sélectionnée.

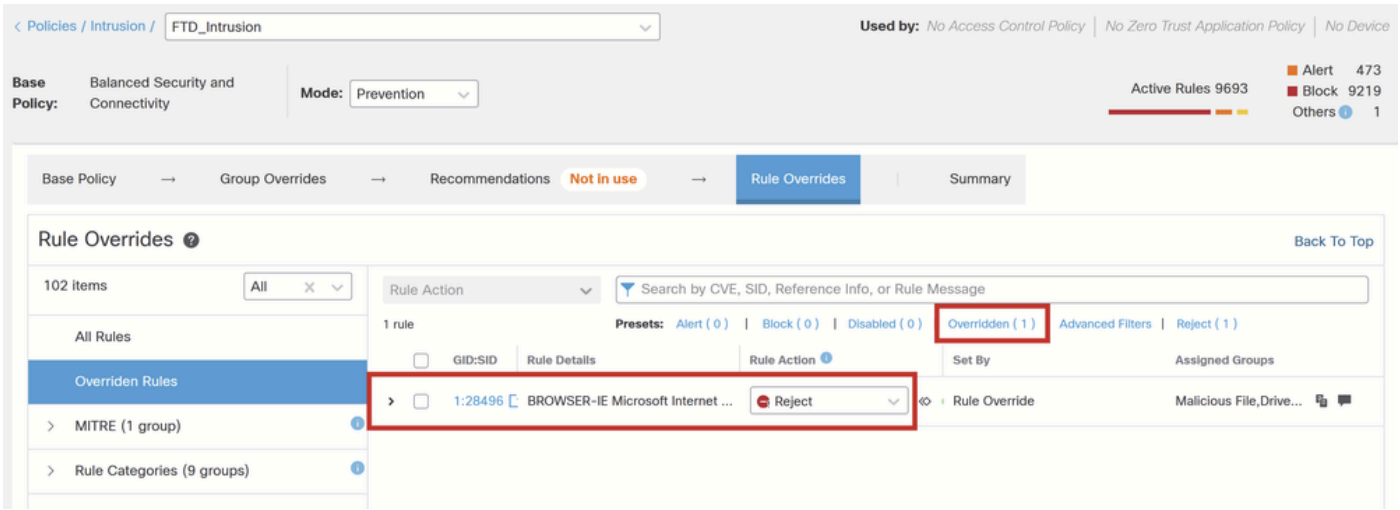


Actions de règle supplémentaires



Modification de l'action Règle

Les règles remplacées se trouvent sous Remplacements de règles > Règles remplacées.



Règles remplacées

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.