Reglas de filtrado de snort basadas en la versión de SRU y LSP de los dispositivos Firepower administrados por FMC

Contenido

Introducción

Este documento describe cómo filtrar reglas de snort basadas en la versión de actualización de reglas seguras (SRU) y paquete de estado de enlace (LSP) de Cisco de los dispositivos firepower administrados por Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Snort de código abierto
- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este artículo es aplicable a todas las plataformas Firepower
- Cisco Firepower Threat Defense (FTD), que ejecuta la versión de software 7.0.0
- Firepower Management Center Virtual (FMC), que ejecuta la versión de software 7.0.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

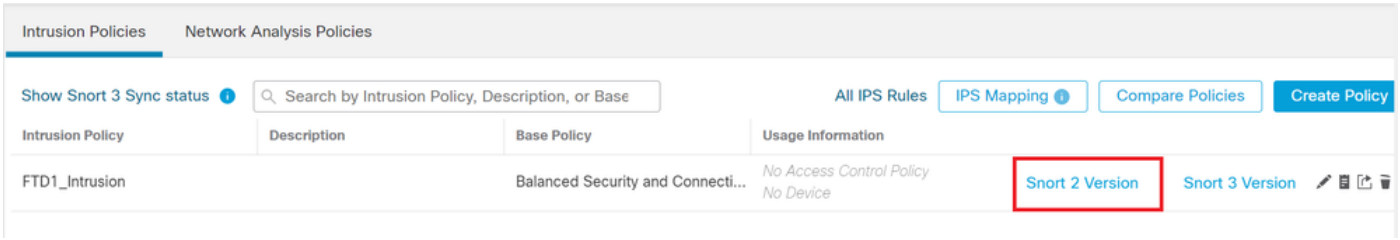
En el contexto de los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS), "SID" significa "ID de firma" o "ID de firma de Snort".

Un identificador de firma de Snort (SID) es un identificador único asignado a cada regla o firma dentro de su conjunto de reglas. Estas reglas se utilizan para detectar patrones o comportamientos específicos en el tráfico de red que pueden indicar actividad maliciosa o amenazas de seguridad. Cada regla se asocia a un SID para facilitar la referencia y la administración.

Para obtener información sobre Snort de código abierto, visite el sitio web de SNORT.

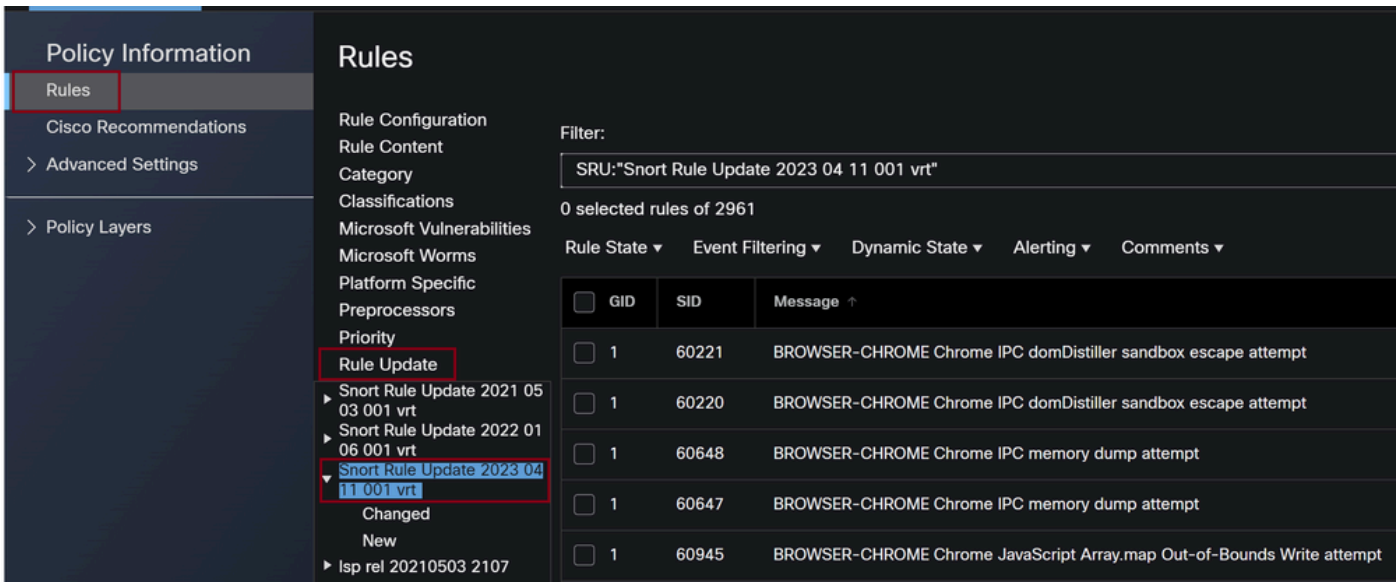
Procedimiento para filtrar reglas Snort

Para ver los SID de la regla de Snort 2, vaya a FMC Policies > Access Control > Intrusion, a continuación, haga clic en la opción SNORT2 en la esquina superior derecha, como se muestra en la imagen:

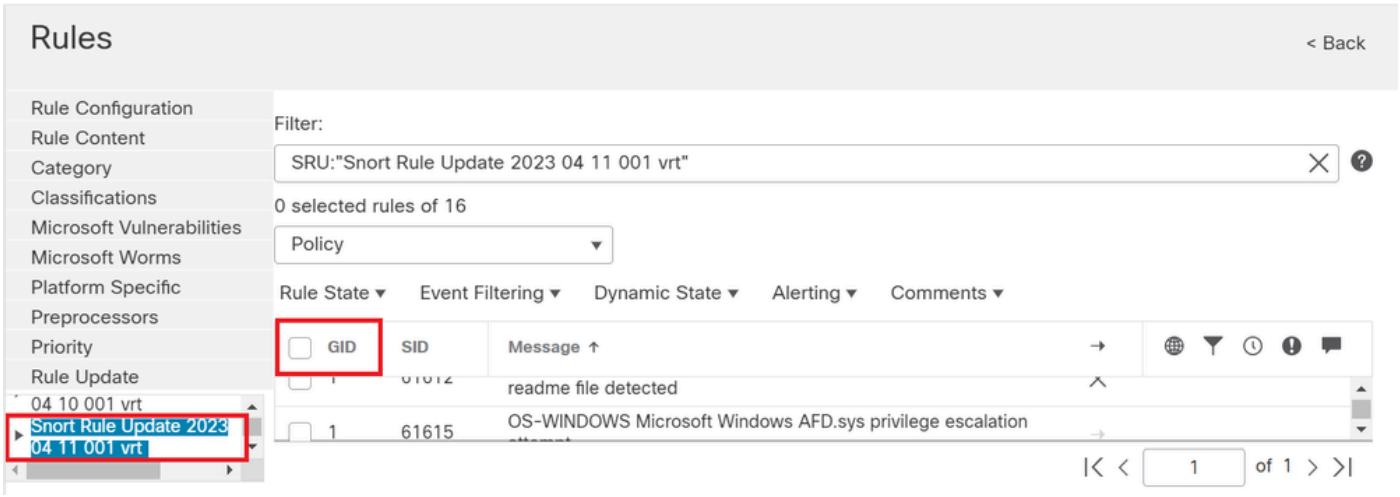


Snort 2

Desplácese hasta Rules > Rule Update y seleccione la fecha límite para filtrar el SID.

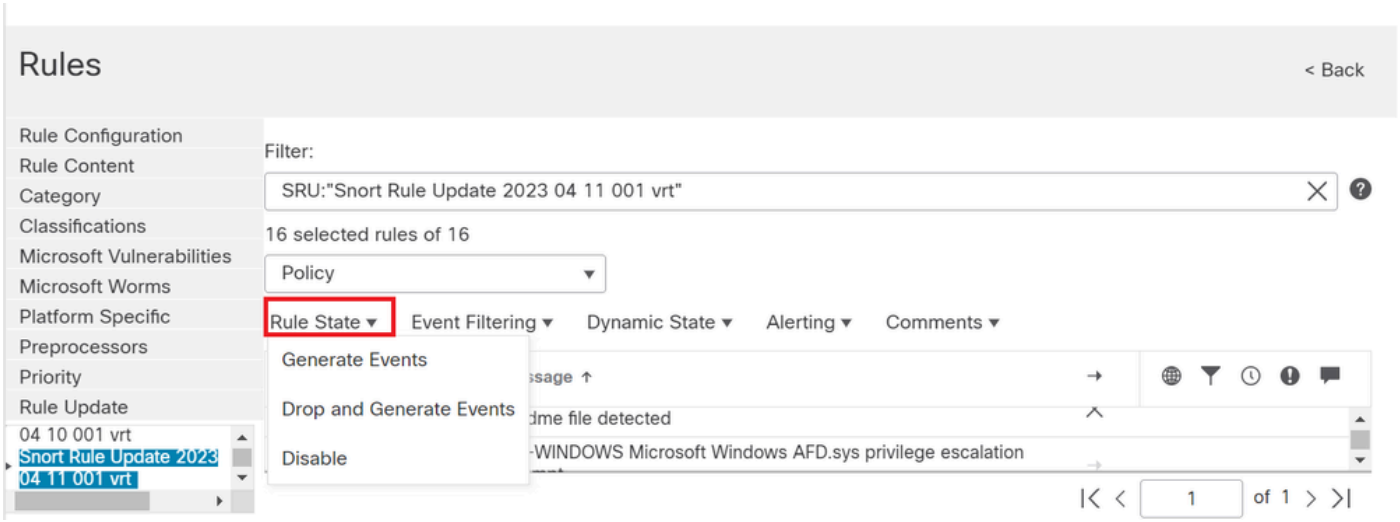


Actualización de reglas



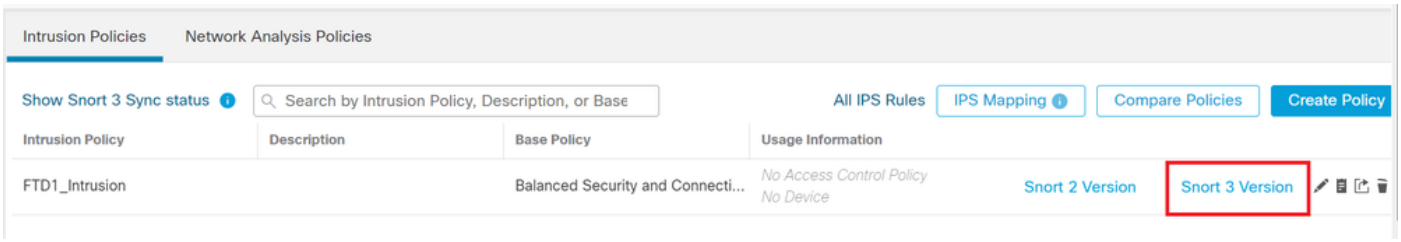
Sid disponibles bajo reglas de snort

Seleccione una opción necesaria en Rule State como se muestra en la imagen.



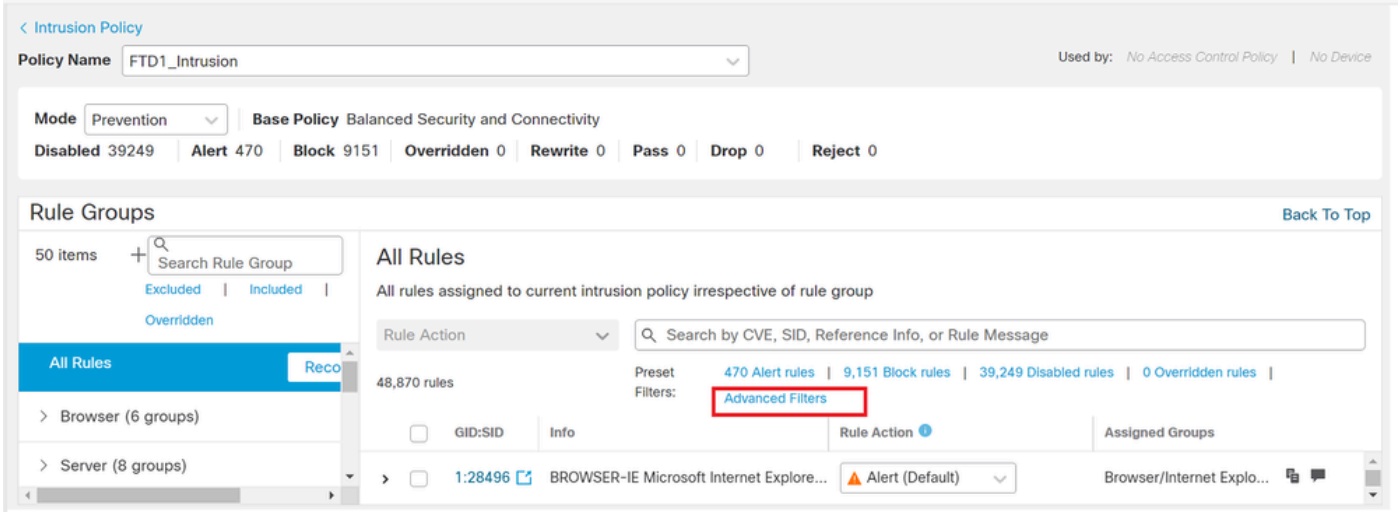
Selección de estados de regla

Para ver los SID de la regla Snort 3, vaya a FMC Policies > Access Control > Intrusion A continuación, haga clic en la opción SNORT3 de la esquina superior derecha, como se muestra en la imagen:

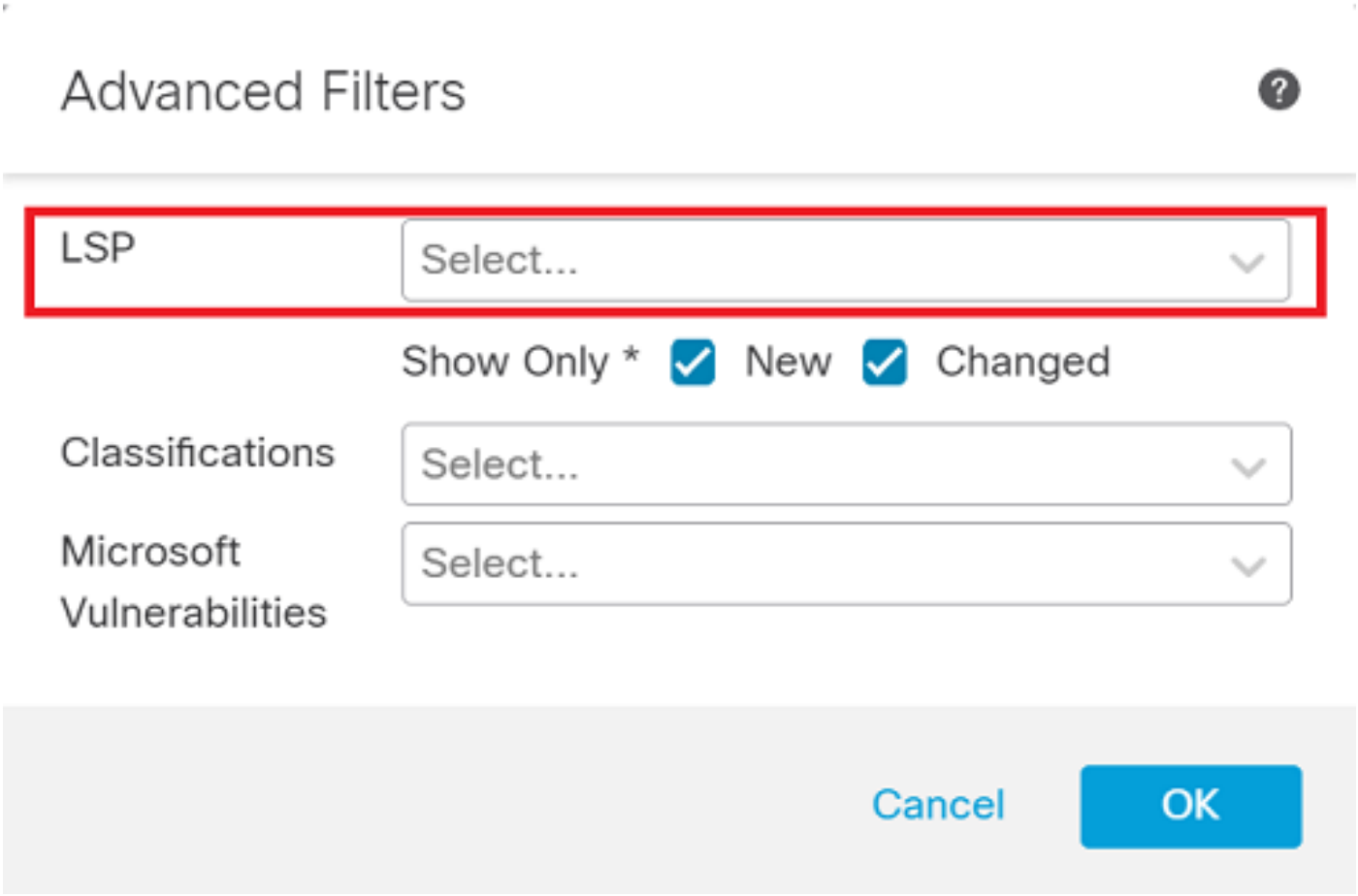


Snort 3

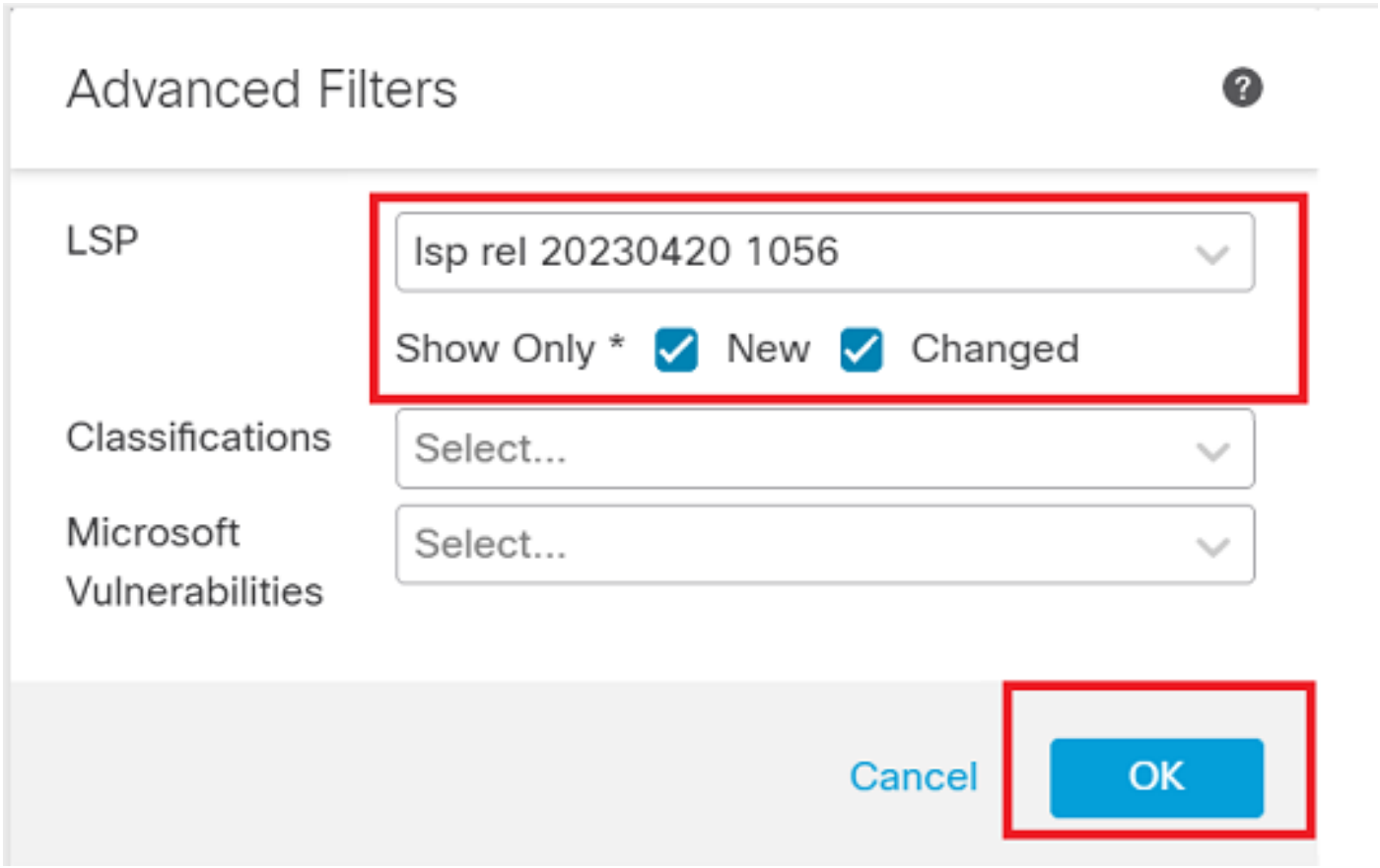
Desplácese hasta Advanced Filters y seleccione la fecha límite para filtrar el SID como se muestra en la imagen.



Filtros Snort 3



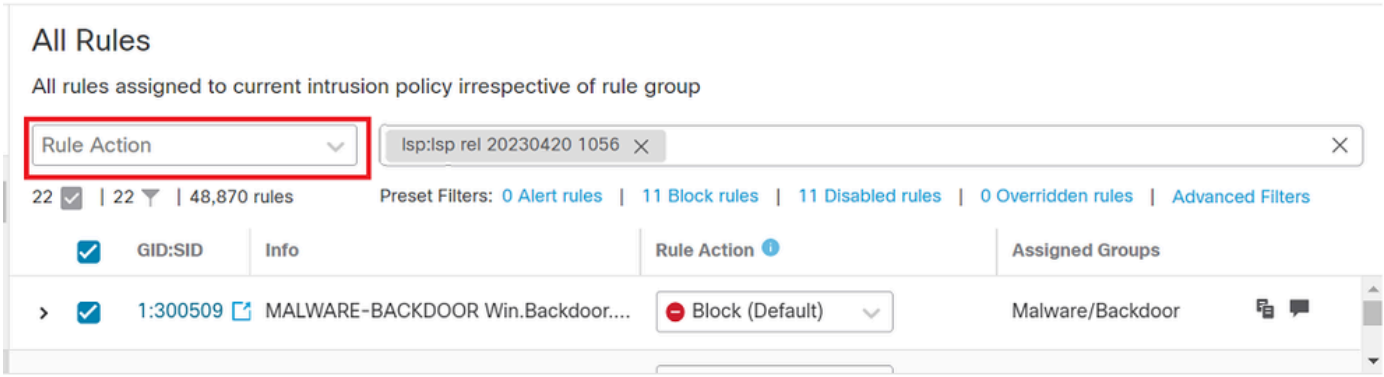
LSP bajo filtro avanzado



versión de LSP

Filtro predefinido para Sid's

Seleccione una opción necesaria en Rule state como se muestra en la imagen.



Acción de regla

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).