Actualización de Snort 2 a Snort 3 mediante FMC

Contenido

Introducción

Este documento describe cómo actualizar desde la versión 2 y 3 de Snort en Firepower Manager Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense
- Centro de administración FirePOWER
- Snort

Componentes Utilizados

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

- FMC 7.0
- FTD 7.0

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

La función Snort 3 se añadió en la versión 6.7 para Firepower Device Manager (FDM) y Cisco Defense Orchestrator (CDO); en la versión 7.0 para Firepower Management Center (FMC).

Snort 3.0 se ha diseñado para hacer frente a estos retos:

1. Reduzca el uso de memoria y CPU.
2. Mejore la eficacia de la inspección HTTP.
3. Carga de configuración más rápida y reinicio de Snort.
4. Mejor programabilidad para una incorporación más rápida de funciones.

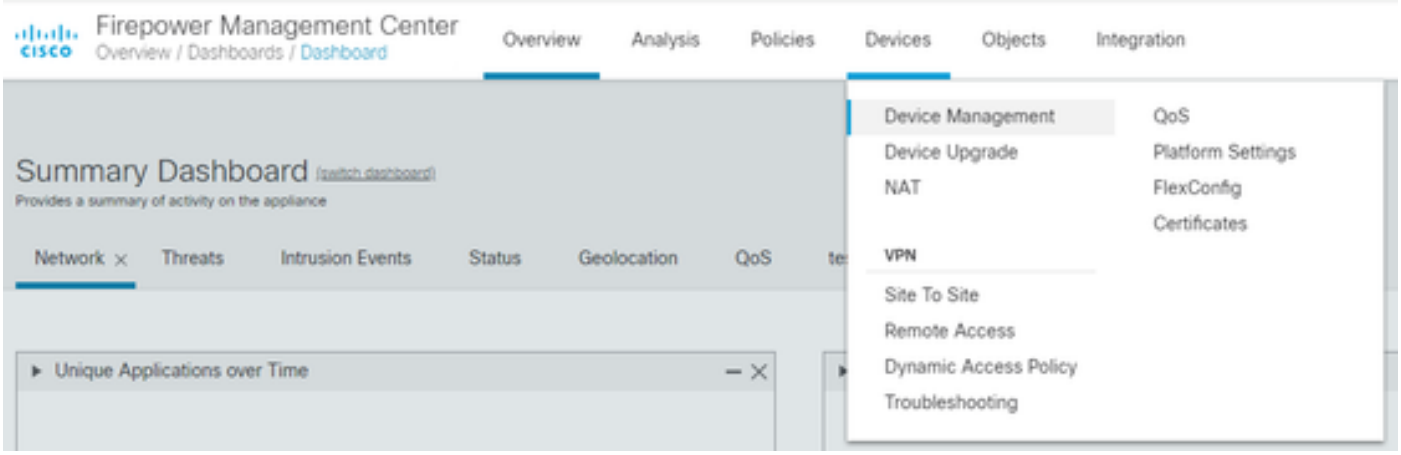
Configurar

Actualización de la versión de Snort

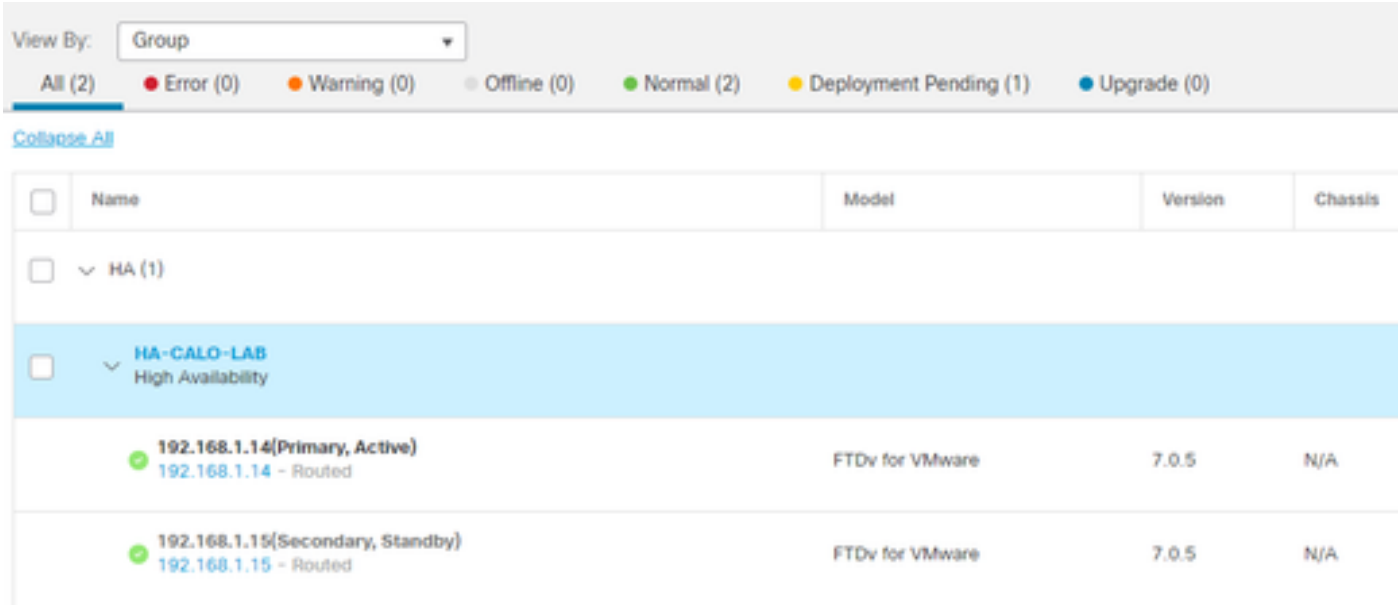
Método 1

1. Inicie sesión en Firepower Management Center.

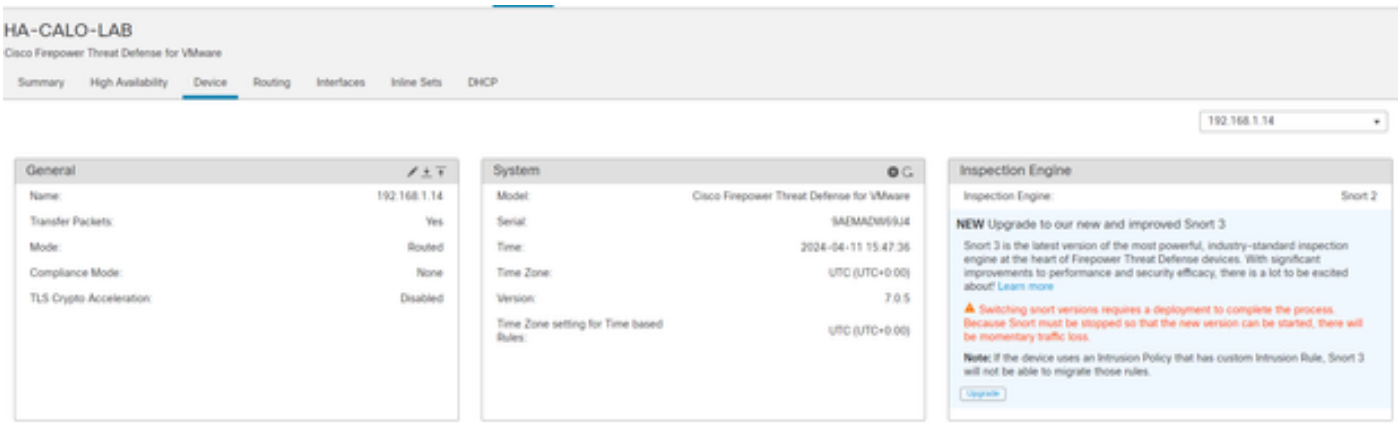
2. En la pestaña Device, navegue hasta Devices > Device Manager.



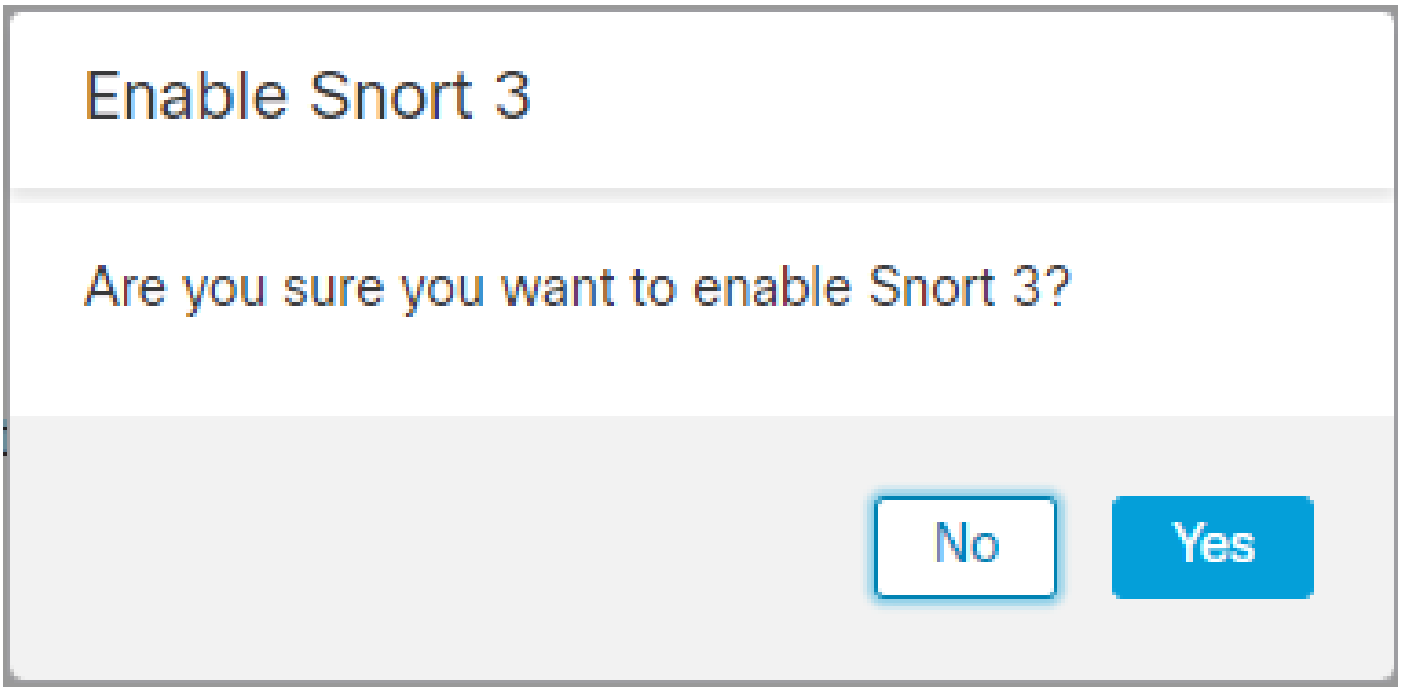
3. Seleccione el dispositivo cuya versión de Snort desea cambiar.



4. Haga clic en la pestaña Device y haga clic en el botón Upgrade en la sección Inspection Engine.



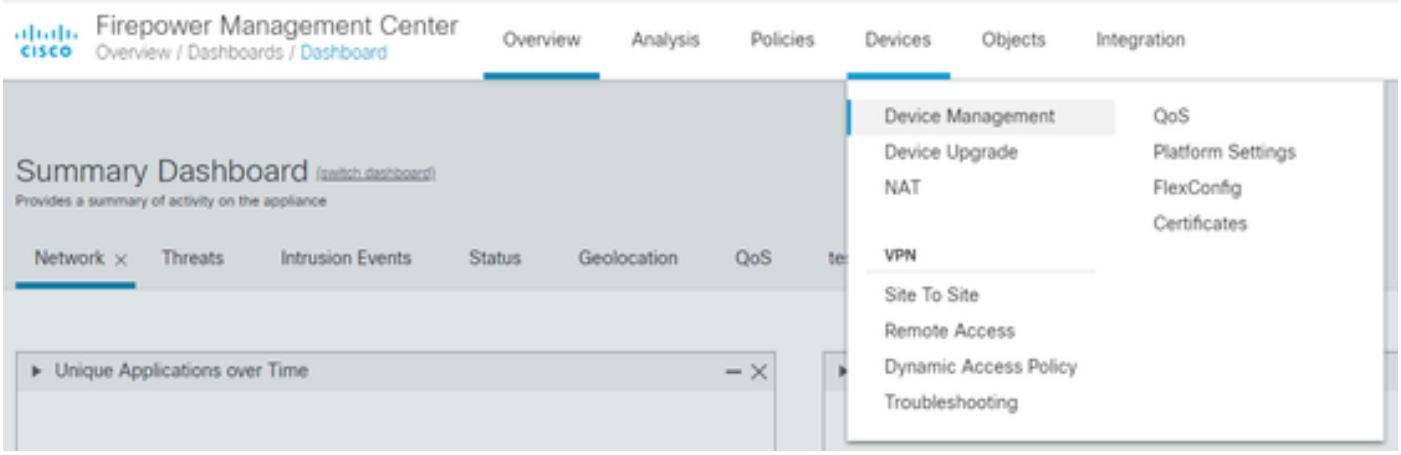
5. Confirme su selección.



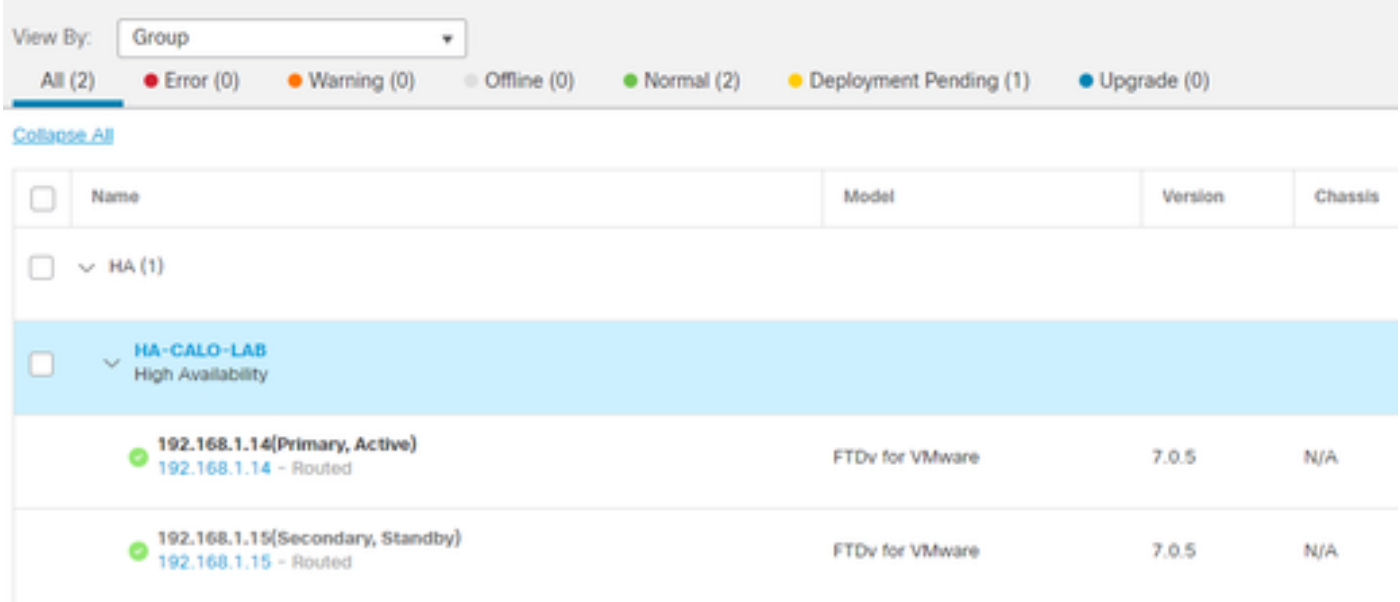
Método 2

1. Inicie sesión en Firepower Management Center.

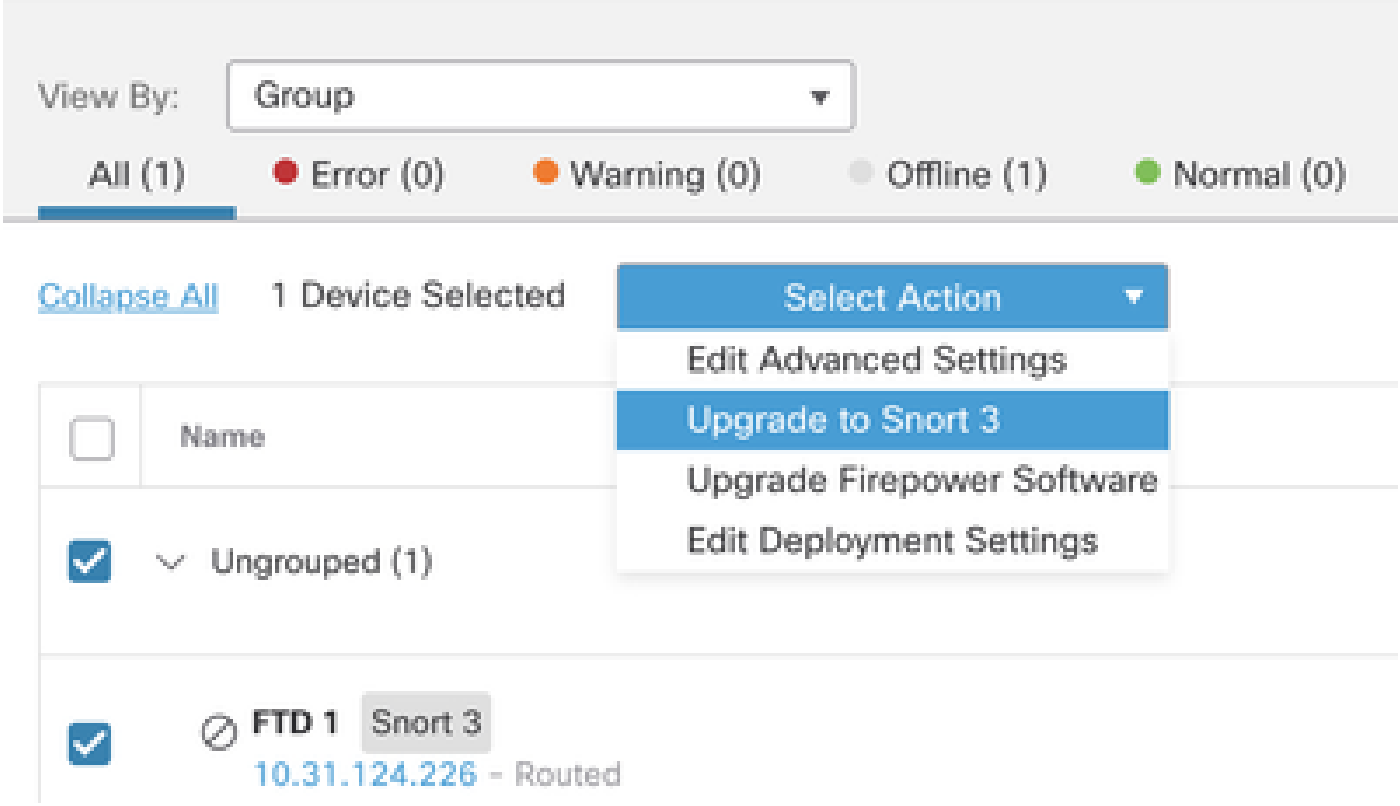
2. En la pestaña Device, navegue hasta Devices > Device Manager.



3. Seleccione el dispositivo cuya versión de Snort desea cambiar.



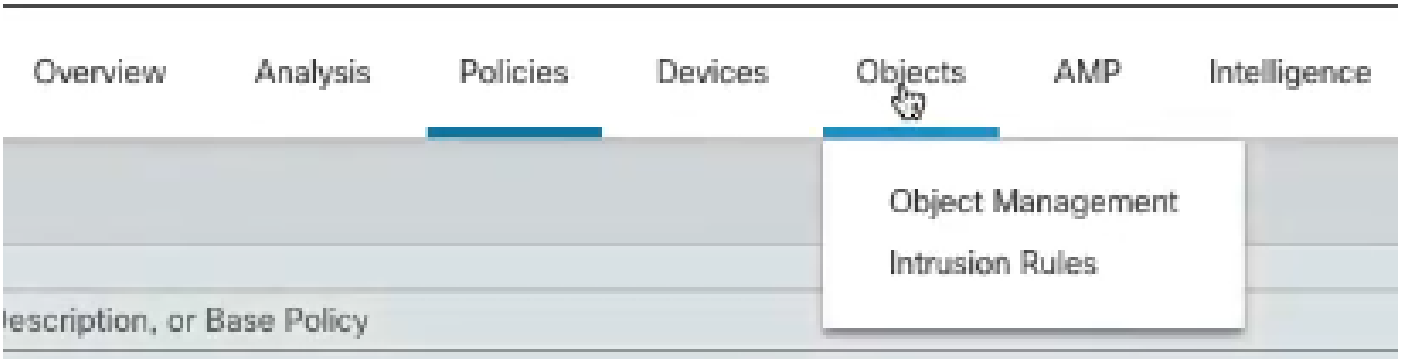
4. Haga clic en el botón Select Action y seleccione Upgrade to Snort 3.



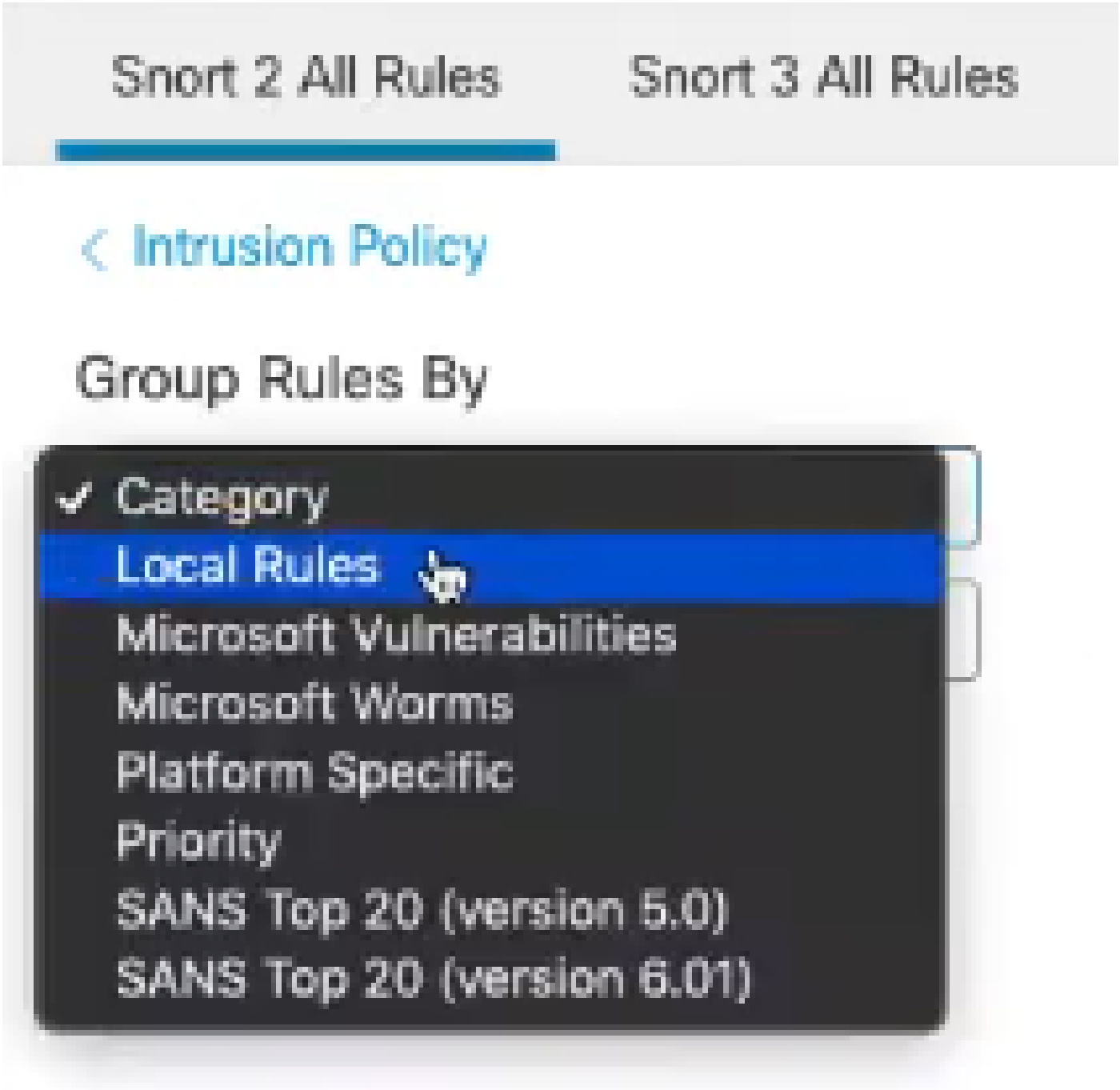
Actualización de reglas de intrusión

Además, debe convertir las reglas de Snort 2 en reglas de Snort 3.

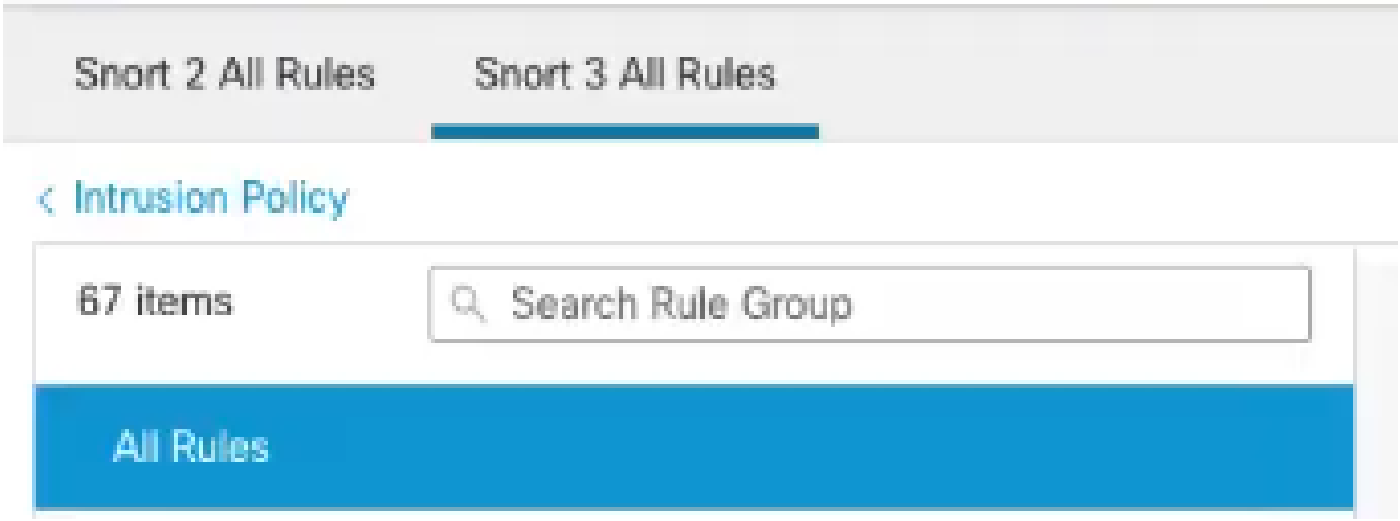
1. Seleccione en el menú Objetos > Reglas de intrusión.



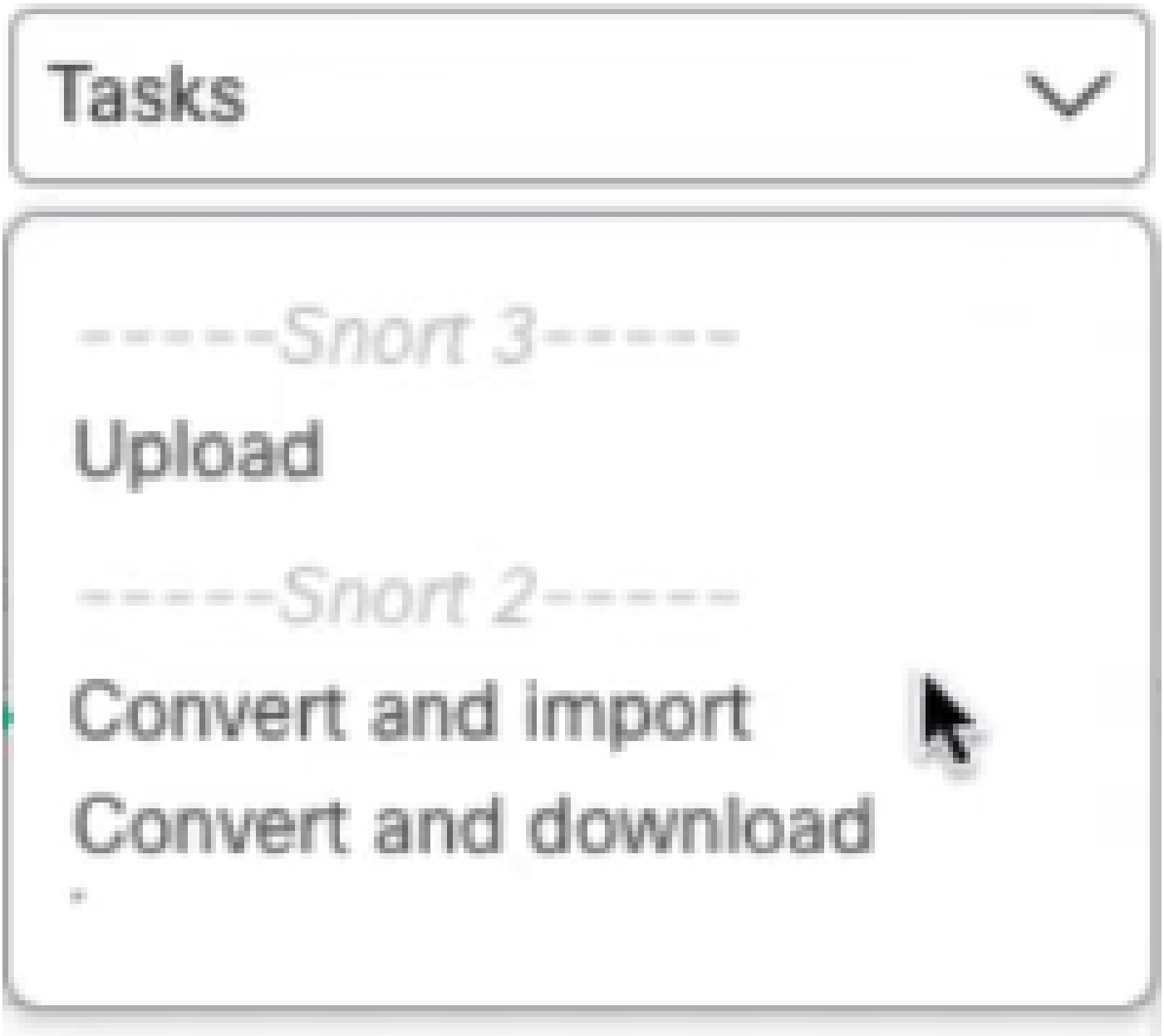
2. Seleccione en el menú Snort 2 All Rules (Todas las reglas) > Group Rules By (Agrupar reglas por) > Local Rules (Reglas locales).



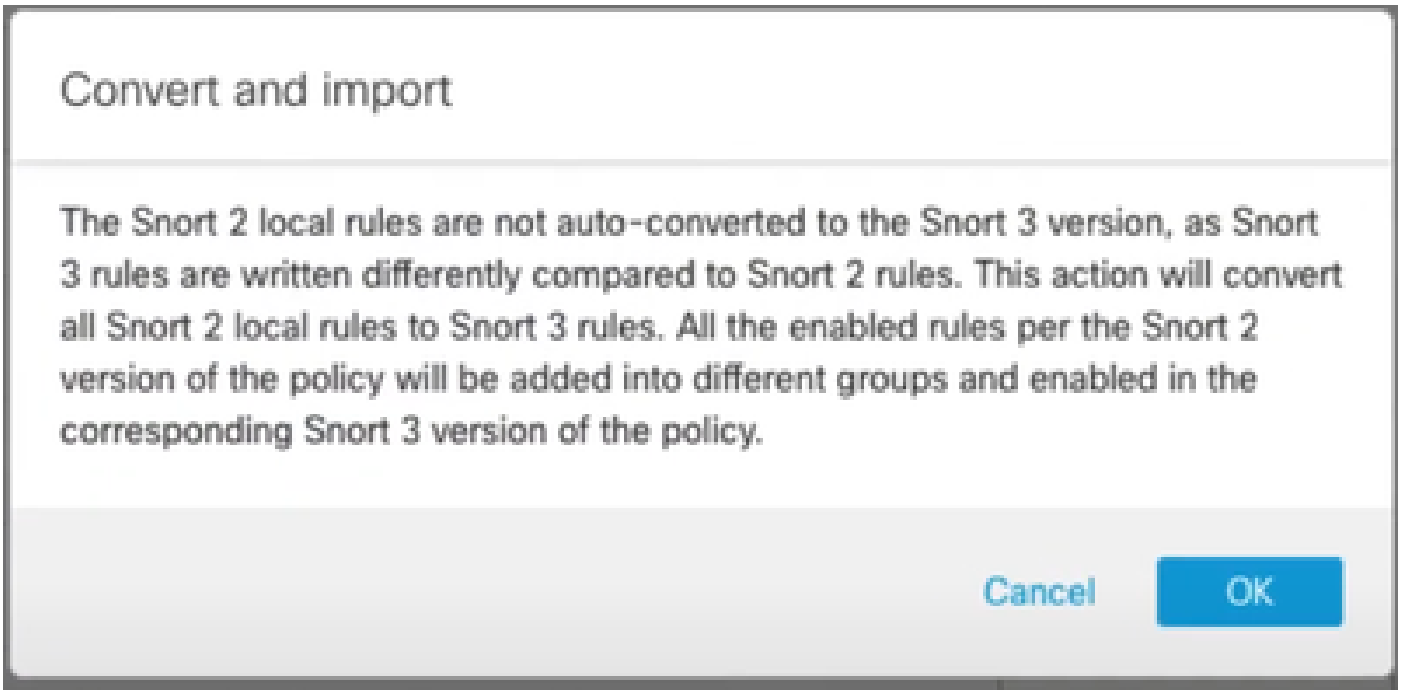
3. Haga clic en Snort 3 All Rules pestaña y asegúrese de que All Rules está seleccionado.



4.En el menú desplegable Task, seleccione Convert and import.



5. Haga clic en Aceptar en el mensaje de advertencia.

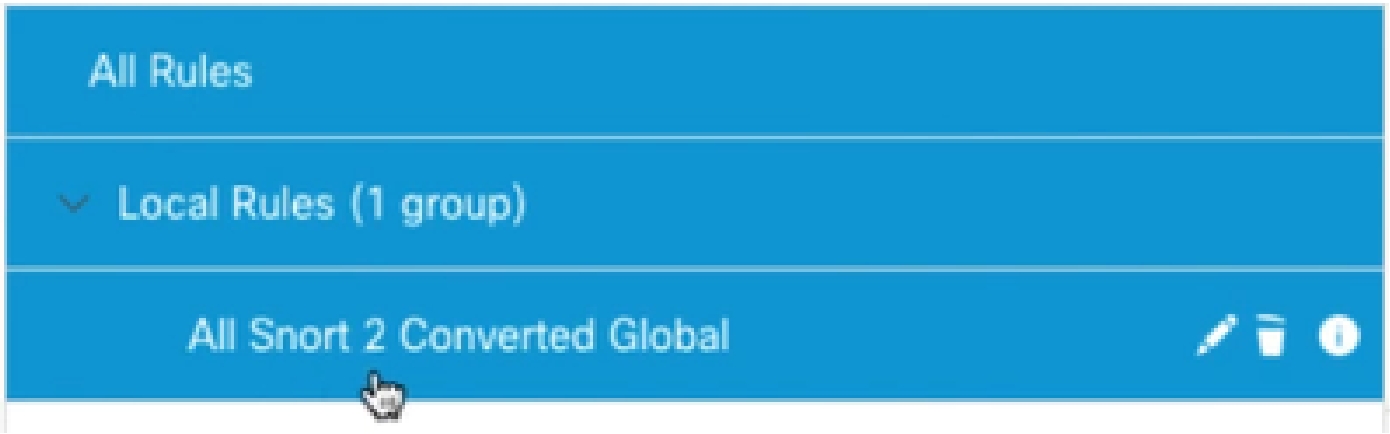


Verificación

La sección Motor de inspección muestra que la versión actual de Snort es Snort 3.

La conversión de la regla se realizó correctamente una vez que aparece este mensaje:

Por último, debe encontrar en el grupo Local Rules la sección All Snort 2 Converted Global, que contiene todas las reglas convertidas de Snort 2 a Snort 3.



Resolución de problemas

En caso de que la migración falle o falle, vuelva a Snort 2 e inténtelo de nuevo.

Información Relacionada

- Cómo migrar de Snort 2 a Snort 3
- Cisco Secure - Actualización de dispositivo Snort 3 (vídeo externo de YouTube)

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).