Reglas de Snort locales personalizadas en un sistema Cisco FireSIGHT

Contenido

Introducción

Una regla local personalizada en un sistema FireSIGHT es una regla Snort estándar personalizada que se importa en un formato de archivo de texto ASCII desde un equipo local. Un sistema FireSIGHT permite importar reglas locales mediante la interfaz web. Los pasos para importar reglas locales son muy sencillos. Sin embargo, para escribir una regla local óptima, un usuario necesita un conocimiento profundo de los protocolos de red y Snort.

El propósito de este documento es proporcionarle algunas sugerencias y ayuda para escribir una regla local personalizada. Las instrucciones para crear reglas locales están disponibles en el *Manual del usuario de Snort,* que está disponible en snort.org. Cisco recomienda descargar y leer el Manual del usuario antes de escribir una regla local personalizada.

> **Nota:** Las reglas proporcionadas en un paquete de actualización de reglas de Sourcefire (SRU) son creadas y probadas por el Cisco Talos Security Intelligence and Research Group, y cuentan con el respaldo del Cisco Technical Assistance Center (TAC). El Cisco TAC no proporciona asistencia para escribir o ajustar una regla local personalizada. Sin embargo, si experimenta algún problema con la funcionalidad de importación de reglas de su sistema FireSIGHT, póngase en contacto con el Cisco TAC.

> **Advertencia:** Una regla local personalizada mal escrita puede afectar al rendimiento de un sistema FireSIGHT, lo que puede reducir el rendimiento de toda la red. Si experimenta algún problema de rendimiento en la red y hay algunas reglas de Snort locales personalizadas activadas en el sistema FireSIGHT, Cisco recomienda que desactive dichas reglas locales.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre las reglas de Snort y el sistema FireSIGHT.

Componentes Utilizados

La información de este documento se basa en estas versiones de hardware y software:

- FireSIGHT Management Center (también conocido como Defense Center)
- Software versión 5.2 o posterior

Trabajo con reglas locales personalizadas

Importar reglas locales

Antes de comenzar, debe asegurarse de que las reglas del archivo no contienen caracteres de escape. El importador de reglas requiere que todas las reglas personalizadas se importen mediante codificación ASCII o UTF-8.

El siguiente procedimiento explica cómo importar reglas de texto estándar locales desde un equipo local:

1. Acceda a la página **Editor de Reglas** navegando hasta **Políticas > Intrusión > Editor de Reglas**.

2. Haga clic en **Reglas de importación**. Aparecerá la página **Actualización de Reglas**.

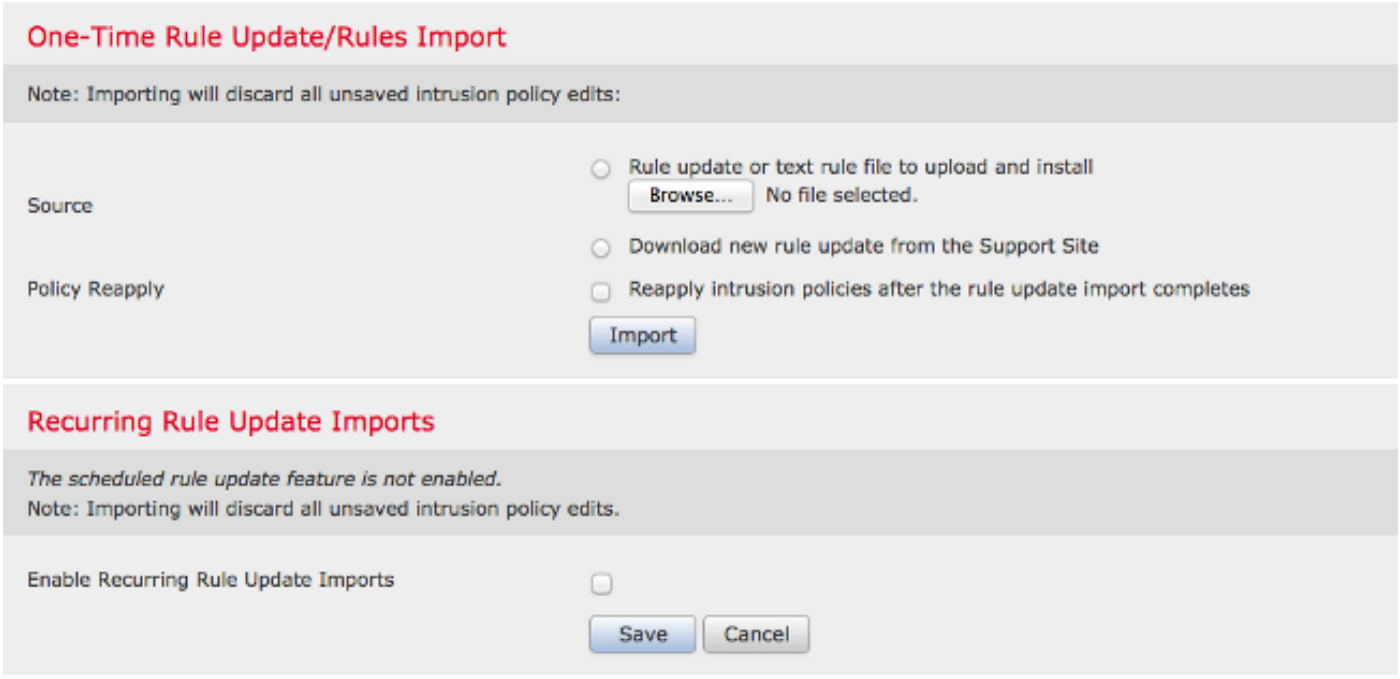


Figura: Captura de pantalla de la página Actualización de reglas

3. Seleccione **Actualización de reglas o archivo de reglas de texto para cargar e instalar** y haga clic en **Examinar** para seleccionar el archivo de reglas.

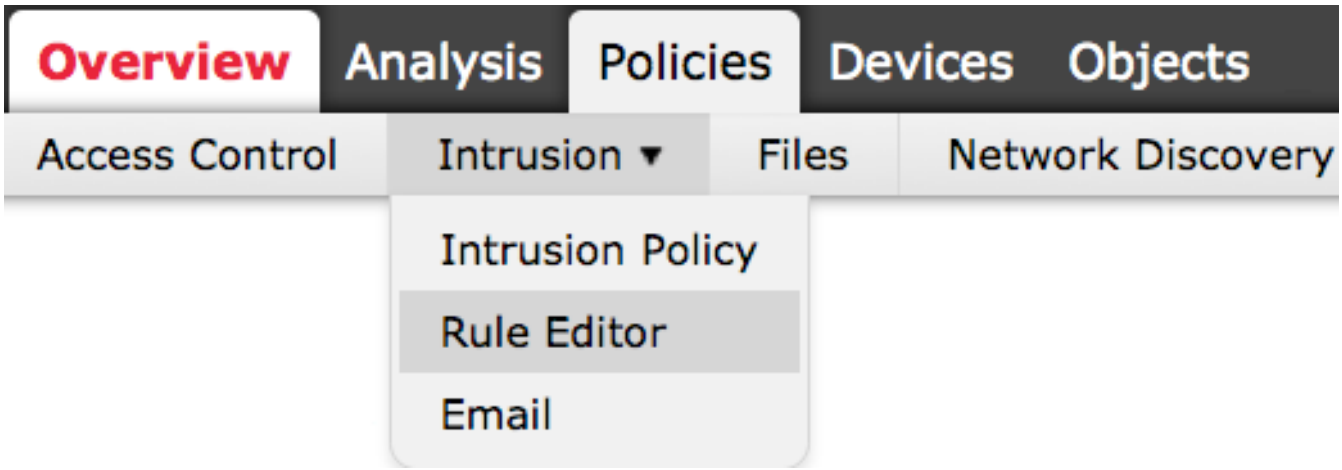
> **Nota:** Todas las reglas cargadas se guardan en la categoría **regla local**.

4. Haga clic en **Importar**. Se importa el archivo de reglas.

> **Precaución:** Los sistemas FireSIGHT no utilizan el nuevo conjunto de reglas para la inspección. Para activar una regla local, debe habilitarla en la directiva de intrusiones y, a continuación, aplicar la directiva.

Ver reglas locales

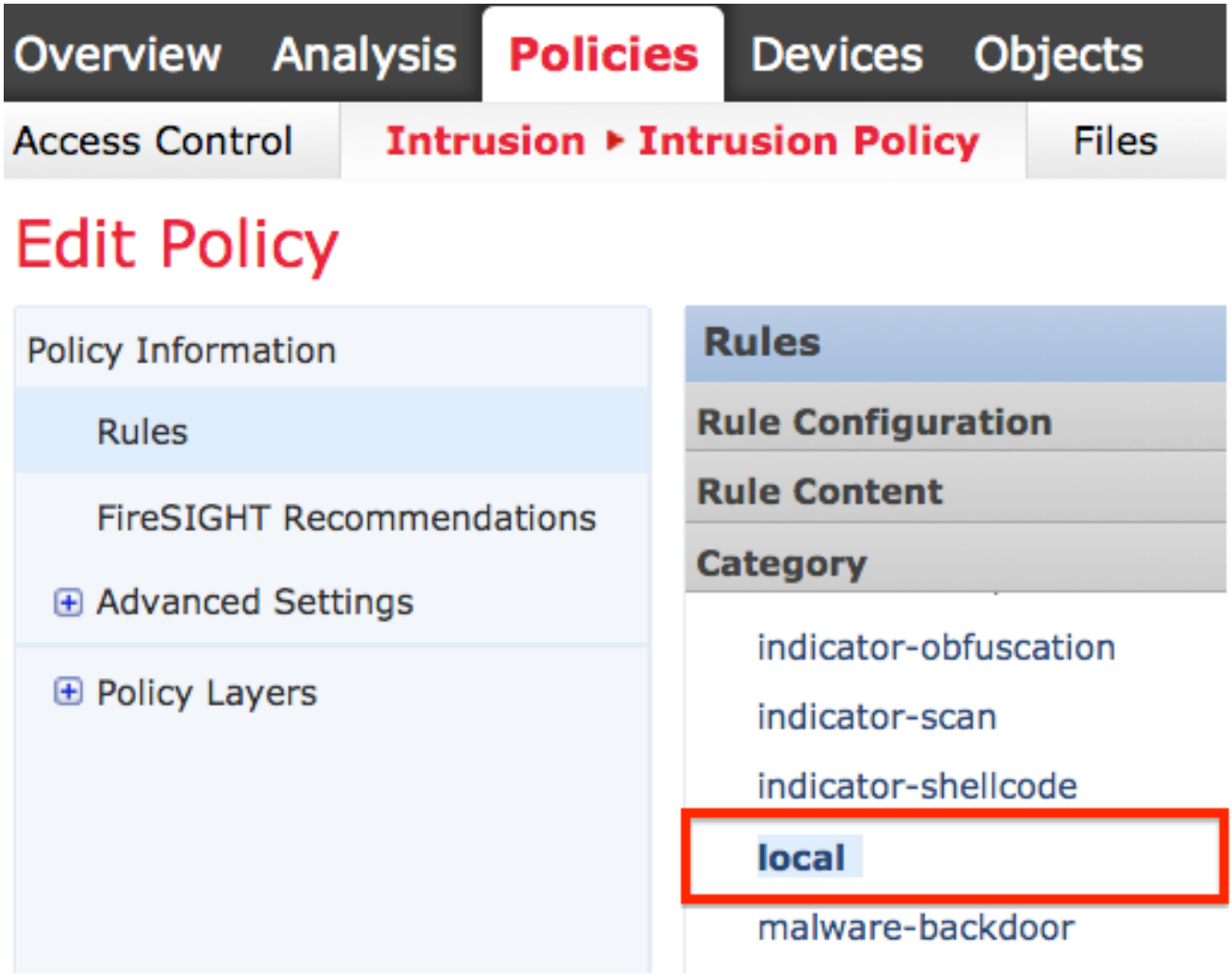
- Para ver el número de revisión de una regla local actual, acceda a la página **Editor de reglas** (**Políticas** > **Intrusión** > **Editor de reglas**).



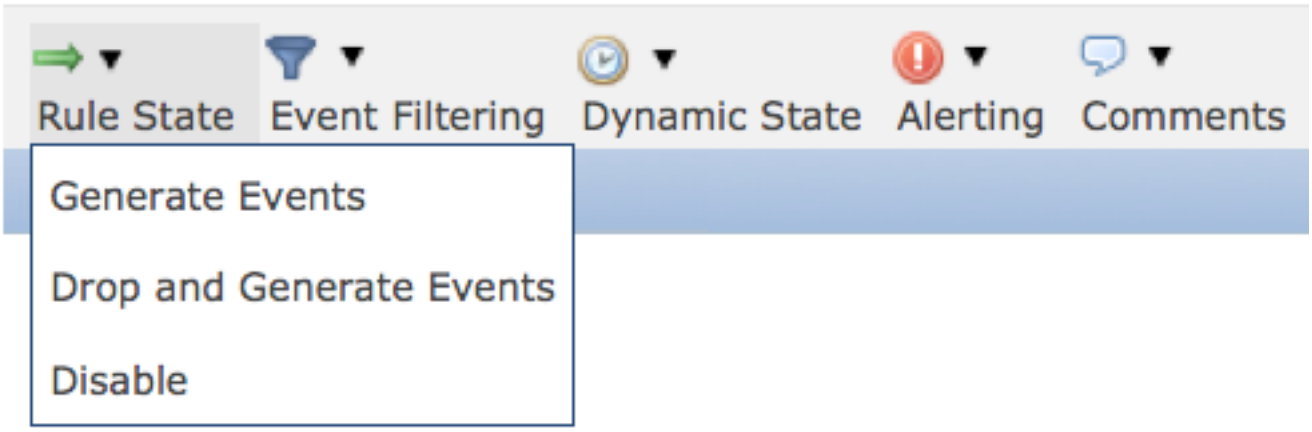
- En la página Editor de reglas, haga clic en la categoría **Regla local** para expandir la carpeta y, a continuación, haga clic en **Editar** junto a la regla.
- Todas las reglas locales importadas se guardan automáticamente en la categoría **regla local**.

Habilitar reglas locales

- De forma predeterminada, el sistema FireSIGHT establece las reglas locales en un estado deshabilitado. Debe establecer manualmente el estado de las reglas locales antes de poder utilizarlas en la directiva de intrusiones.
- Para habilitar una regla local, navegue hasta la página Policy Editor (**Políticas** > **Intrusión** > **Política de intrusión**). Seleccione **Reglas** en el panel izquierdo. En la **Categoría**, seleccione **local**. Deben aparecer todas las reglas locales, si están disponibles.



- Después de seleccionar las reglas locales deseadas, seleccione un estado para las reglas.



- Una vez seleccionado el estado de regla, haga clic en la opción **Información de directiva** en el panel izquierdo. Seleccione el botón **Registrar cambios**. Se valida la directiva de intrusiones.

  Nota: La validación de la política falla si habilita una regla local importada que utiliza la palabra clave threshold desaprobada en combinación con la función de umbral de eventos de intrusión en una política de intrusiones.

Ver las reglas locales eliminadas

- Todas las reglas locales eliminadas se mueven de la categoría de regla local a la categoría de regla eliminada.
- Para ver el número de revisión de una regla local eliminada, vaya a la página **Editor de reglas**, haga clic en la categoría **eliminada** para expandir la carpeta y, a continuación, haga clic en el icono de *lápiz* para ver los detalles de la regla en la página **Editor de reglas**.

Numeración de las reglas locales

- No es necesario especificar un generador (GID); si lo hace, puede especificar sólo GID 1 para una regla de texto estándar o 138 para una regla de datos confidenciales.
- No especifique un identificador de Snort (SID) o un número de revisión al importar una regla por primera vez; esto evita colisiones con SID de otras reglas, incluidas las eliminadas.
- FireSIGHT Management Center asigna automáticamente el siguiente SID de regla personalizada disponible igual o superior a 1000000 y un número de revisión de 1.
- Si intenta importar una regla de intrusión con un SID mayor que 2147483647, se producirá un error de validación.
- Debe incluir el SID asignado por IPS y un número de revisión mayor que el número de revisión actual al importar una versión actualizada de una regla local que haya importado previamente.
- Puede restablecer una regla local que haya eliminado importándola mediante el SID asignado por IPS y un número de revisión mayor que el número de revisión actual. Tenga en cuenta que FireSIGHT Management Center incrementa automáticamente el número de revisión cuando se elimina una regla local; se trata de un dispositivo que permite restablecer las reglas locales.

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).

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).