Contenido

Introducción

Una regla local de encargo en un sistema de FireSIGHT es una regla estándar de encargo del Snort que usted importa en un formato de archivo de texto de ASCII de una máquina local. Un sistema de FireSIGHT permite que usted importe las reglas locales usando la interfaz Web. Los pasos para importar las reglas locales son muy directos. Sin embargo, para escribir una regla local óptima, un usuario requiere el conocimiento en profundidad en los protocolos del Snort y de establecimiento de una red.

El propósito de este documento es proveer de usted ciertas extremidades y ayuda de escribir una regla local de encargo. Las instrucciones en crear las reglas locales están disponibles en el *manual de los usuarios del Snort,* que está disponible en snort.org. Cisco recomienda que usted descarga y lee a los usuarios manuales antes de que usted escriba una regla local de encargo.

> Nota: Las reglas proporcionadas en un paquete de la actualización de la regla de Sourcefire (SRU) son creadas y probadas por la inteligencia de Seguridad de Cisco Talos y el grupo de investigación, y soportadas por el Centro de Asistencia Técnica de Cisco (TAC). El TAC de Cisco no proporciona la ayuda en la escritura o ajustar una regla local de encargo, sin embargo si usted experimenta cualesquiera problemas con las funciones de la importación de la regla de su sistema de FireSIGHT, entre en contacto por favor el TAC de Cisco.

> Advertencia: Una aduana mal escrita regla local puede afectar el funcionamiento de un sistema de FireSIGHT que pueda llevar a la degradación del rendimiento del toda la red. Si usted está experimentando cualesquiera problemas de rendimiento en su red, y hay algunas reglas locales de encargo del Snort habilitadas en su sistema de FireSIGHT, Cisco le recomienda para inhabilitar esas reglas locales.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento en las reglas del Snort y el sistema de FireSIGHT.

Componentes Utilizados

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

- El centro de administración de FireSIGHT (también conocido como centro de la defensa)
- Versión de software 5.2 o más adelante

Trabajo con las reglas locales de encargo

Reglas del Local de la importación

Antes de que usted comience, usted debe aseegurarse que las reglas en el archivo no contienen ninguna caracteres de escape. El importador de la regla requiere todas las reglas de encargo ser importado usando la codificación ASCII o de UTF-8.

El siguiente procedimiento explica cómo importar las reglas estándar locales del texto de una máquina local:

1. Acceda la página del **editor de la regla** navegando a las **directivas > al editor de la intrusión > de la regla**.

2. Haga clic las **Reglas de importación**. La página de las **actualizaciones de la regla** aparece.

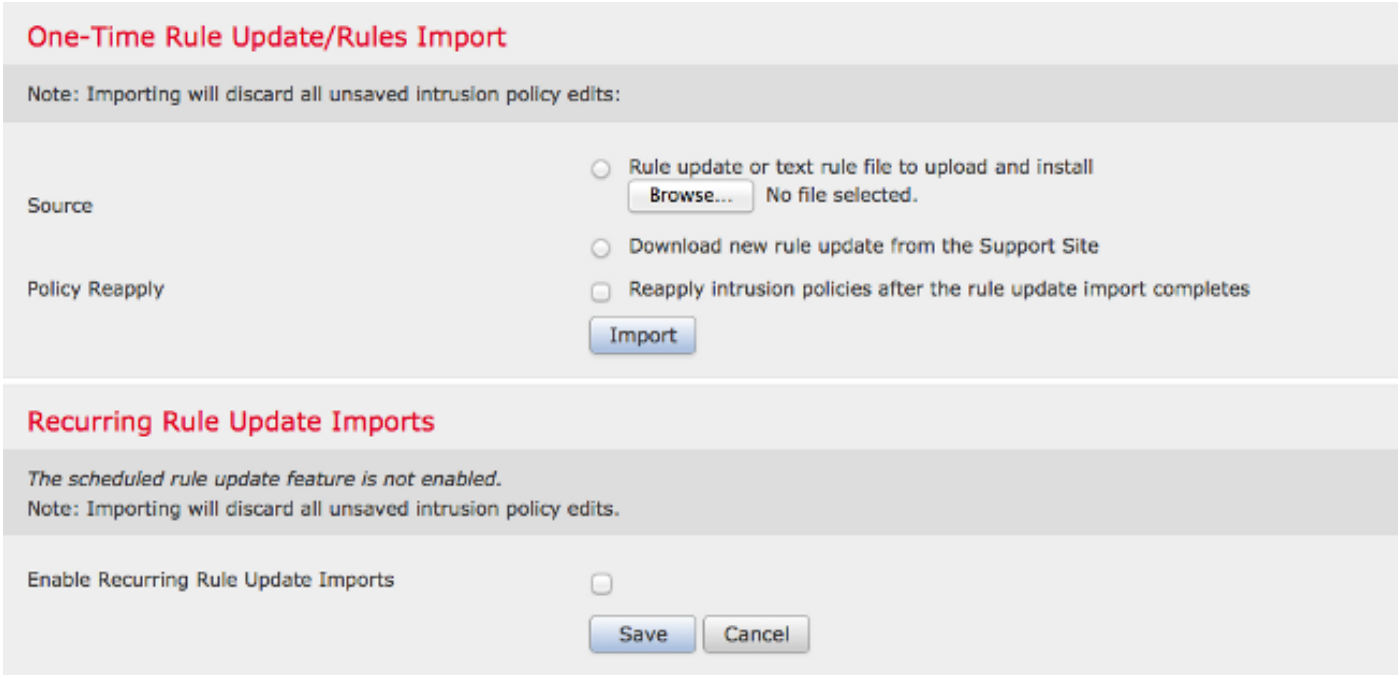


Figura: Un tiro de pantalla de la página de las actualizaciones de la regla

3. Seleccione la **actualización de la regla o el archivo de la regla del texto a cargar y a instalar** y el tecleo **hojean** para seleccionar el archivo de la regla.

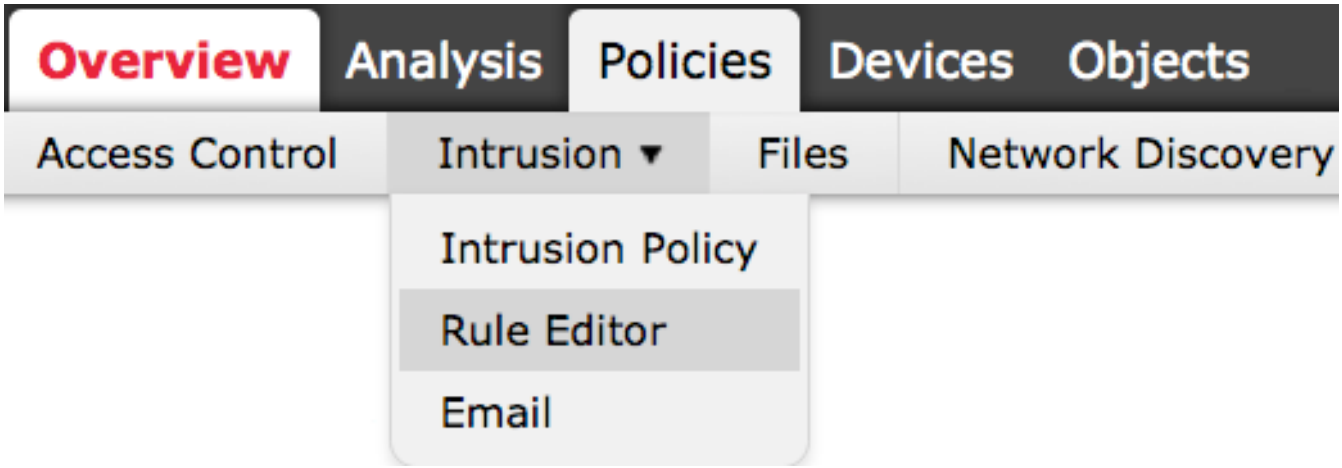
> Nota: Todas las reglas cargadas se guardan en la categoría **local de la regla**.

4. **Importación del** tecleo. Se importa el archivo de la regla.

> Precaución: Los sistemas de FireSIGHT no utilizan la nueva regla fijada para el examen. Para activar una regla local, usted necesita habilitarla en la directiva de la intrusión, y después aplica la directiva.

Reglas del Local de la visión

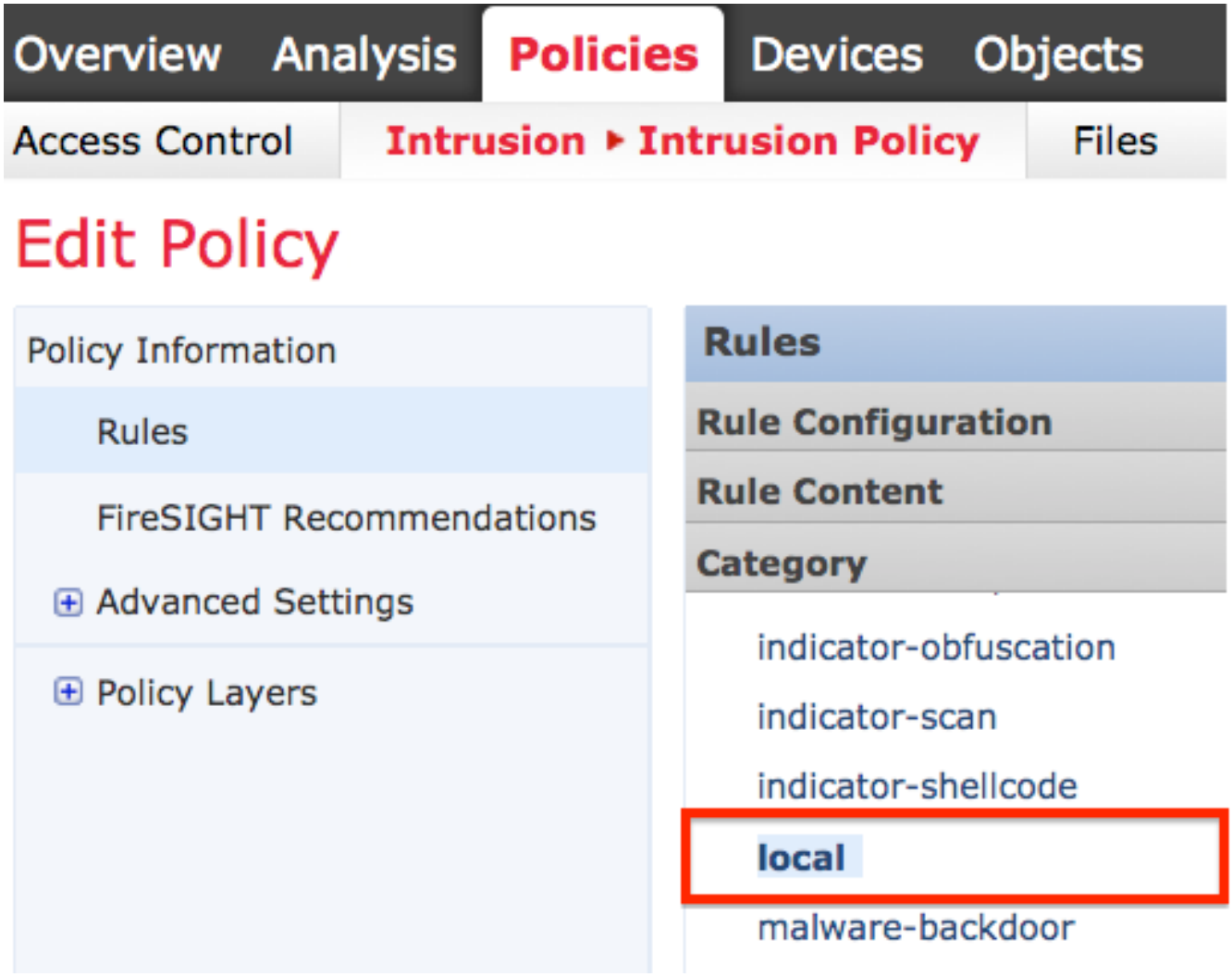
- Para ver el número de revisión para una regla local actual, navegue a la página del **editor de la regla** (**directivas > editor de la intrusión >** de la **regla**).



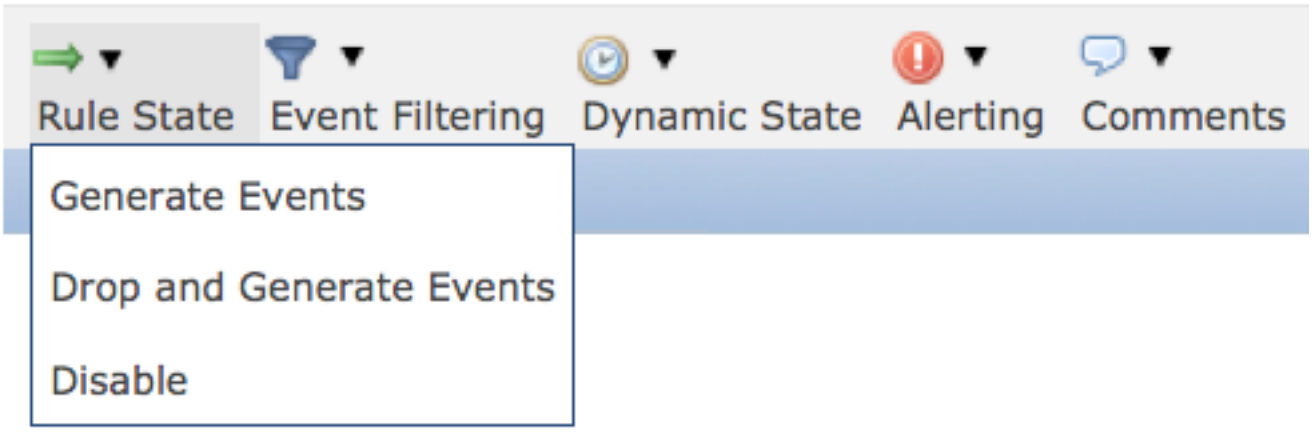
- En la página del editor de la regla, haga clic en la categoría **local de la regla** para ampliar la carpeta, después haga clic **editan** al lado de la regla.
- Todas las reglas locales importadas se guardan automáticamente en la categoría **local de la regla**.

Reglas del Local del permiso

- Por abandono, el sistema de FireSIGHT fija las reglas locales en un estado inhabilitado. Usted debe fijar manualmente el estado de las reglas locales antes de que usted pueda utilizarlas en su directiva de la intrusión.
- Para habilitar una regla local, navegue a la página del editor de políticas (**directivas > intrusión > directiva de la intrusión**). Seleccione las **reglas** en el panel izquierdo. Bajo **categoría**, seleccione el **local**. Todas las reglas locales deben aparecer, si están disponibles.



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



- Una vez que se selecciona el estado de la regla, haga clic en la opción de la **información de política** en el panel izquierdo. Seleccione el botón de los **cambios del cometer**. Se valida la directiva de la intrusión.

  Nota: La validación de la directiva falla si usted habilita una regla local importada que utilice la palabra clave desaprobada del umbral conjuntamente con la característica de la formación de umbrales del evento de la intrusión en una directiva de la intrusión.

Vea las reglas locales borradas

- Todas las reglas locales borradas se mueven desde la categoría local de la regla a la categoría borrada de la regla.
- Para ver el número de revisión de una regla local borrada, vaya a la página del **editor de la regla**, haga clic en la categoría **borrada** para ampliar la carpeta, después haga clic el icono del *lápiz* para ver el detalle de la regla en la página del **editor de la regla**.

Enumeración de las reglas locales

- Usted no tiene que especificar un generador (GID); si usted lo hace, usted puede especificar solamente GID 1 para una regla estándar del texto o 138 para los datos vulnerables gobiernan.
- No especifique un Snort ID (SID) o el número de revisión al importar una regla por primera vez; esto evita las colisiones con los SID de otras reglas, incluyendo las reglas borradas.
- El centro de administración de FireSIGHT asigna automáticamente la regla de encargo disponible siguiente SID de 1000000 o mayor, y un número de revisión de 1.
- Si usted intenta importar una regla de la intrusión con un SID mayor de 2147483647, un error de validación ocurrirá.
- Usted debe incluir el SID asignado por el IPS y un número de revisión mayor que el número de revisión actual al importar una versión actualizada de una regla local que usted ha importado previamente.
- Usted puede reinstalar una regla local que usted ha borrado importando la regla usando el SID asignado por el IPS y un número de revisión mayor que el número de revisión actual. Observe que el centro de administración de FireSIGHT incrementa automáticamente el número de revisión cuando usted borra una regla local; éste es un dispositivo que permite que usted reinstale las reglas locales.