Ajuste el IPS para la prevención del falso positivo usando el filtro de la acción del evento

Contenido

Introducción

Este documento proporciona los pasos requeridos para ajustar el Sistema de prevención de intrusiones (IPS) para la prevención del falso positivo usando el administrador de dispositivo IPS (IDM) o el administrador IPS expreso (IME). El falso positivo que ajusta en el IPS es alcanzado por una característica llamada filtro de Event Action (EAF).

Antes de comenzar

Requisitos

Los Quien lea este documento deben tener conocimiento del IPS de Cisco.

Componentes Utilizados

La información en este documento no se basa en las versiones de software y hardware específicas.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Comprensión de EAFs

EAFs se configura sobre todo para ajustar del falso positivo. EAF proporciona la capacidad de hacer que una firma determinada no tome las acciones deseadas para un subconjunto de tráfico.

EAFs es útil en las situaciones donde se requiere para satisfacer las condiciones múltiples, por ejemplo:

- La firma x no toma medidas y para una subred deseada del tráfico.
- La firma x toma medidas y para el resto del tráfico.

EAFs es útil haciendo frente a accionar benigno de una firma.

Configuración

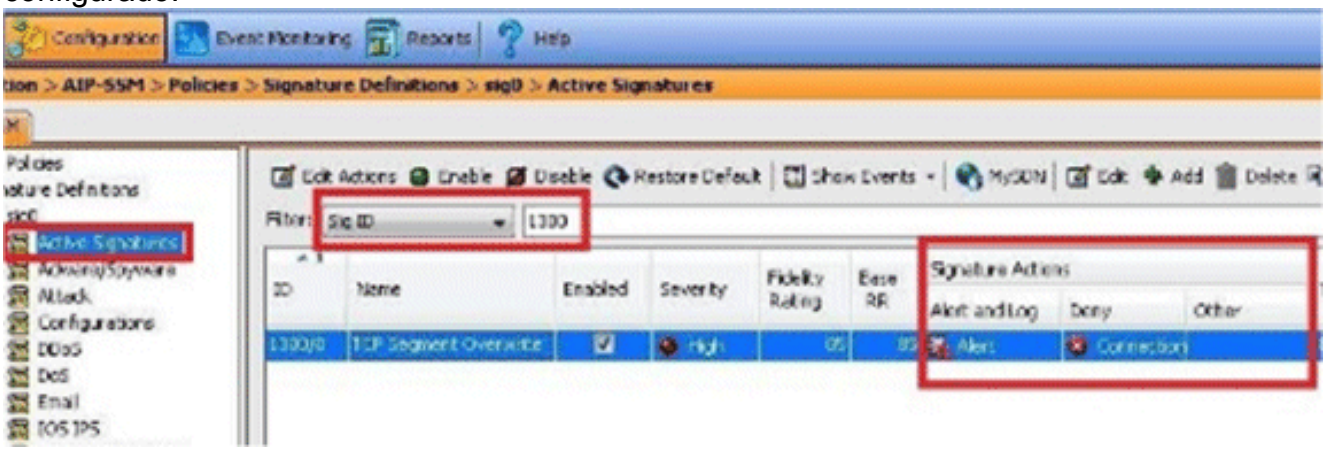
Ejemplo: Evento del falso positivo: Activadores de la firma 1300 para el tráfico que viene y a los host confiables sabidos.

Nota: Éste es apenas propósitos de un ejemplo para demostración solamente. Si usted es inseguro si un evento determinado debido al activador de la firma es benigno o no, entre en contacto el Soporte técnico de Cisco para el análisis adicional.

Nota: Refiera a las firmas del Cisco Intrusion Prevention System para más información sobre las firmas IPS.

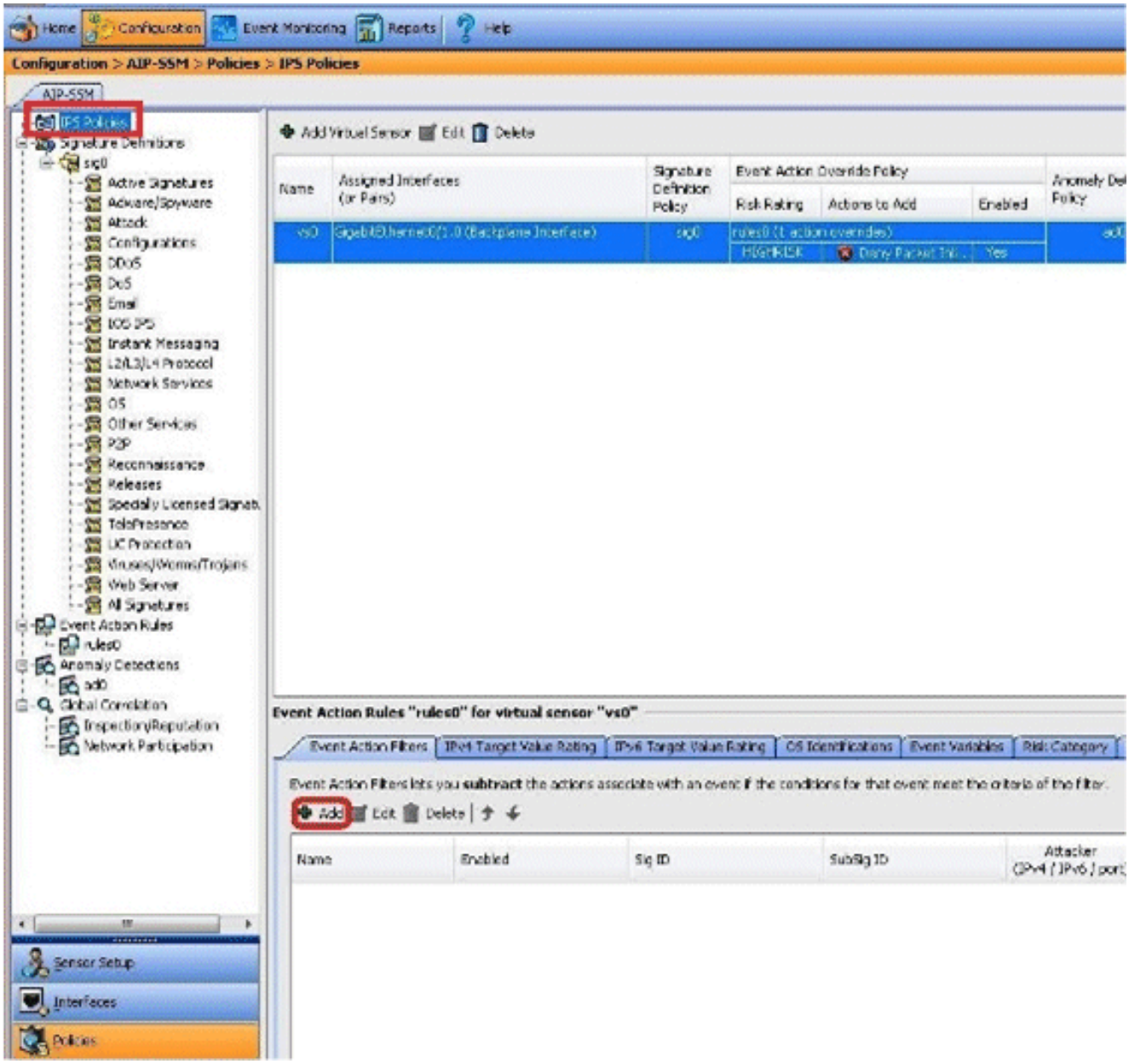
Complete estos pasos:

1. Marque las acciones predeterminadas para la firma (1300, en este ejemplo) para saber si hay la cual EAF las necesidades de ser configurado.

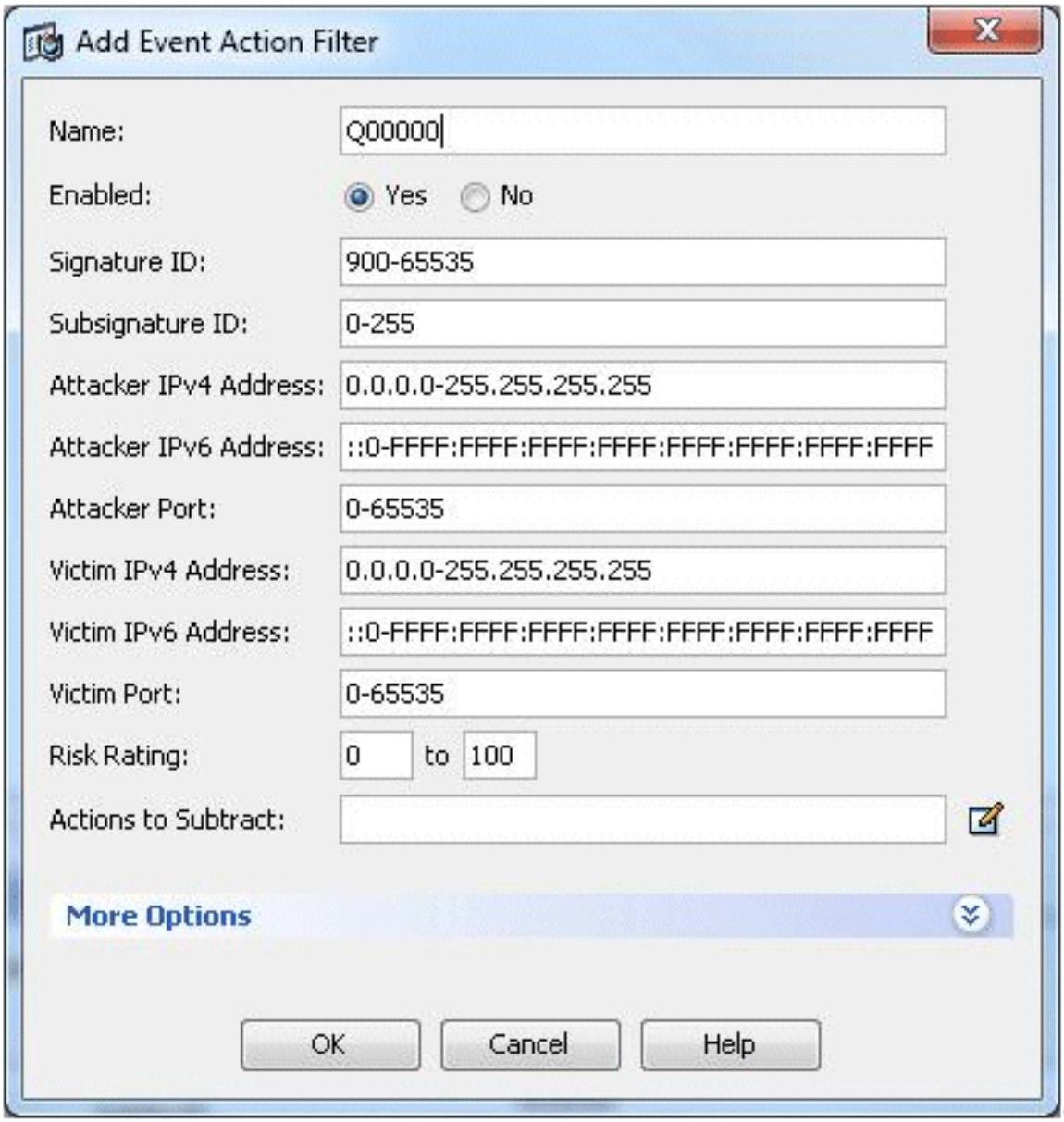


Las acciones predeterminadas de la firma 1300 incluyen la **alerta de la producción** y **niegan la conexión en línea**.

2. Identifique los host para los cuales esta firma no debe encender. Por ejemplo, usted no quisiera que la firma encendiera para el tráfico que viene de una subred de confianza, tal como 10.1.1.1-10.1.1.254.
3. Cree EAF para los criterios descritos en el paso 2:De IDM/IME, vaya a la **configuración** > a las **directivas** > a las **directivas IPS**. Haga clic la lengueta de los **filtros de la acción del evento**. Bajo esta lengueta, haga click en Add

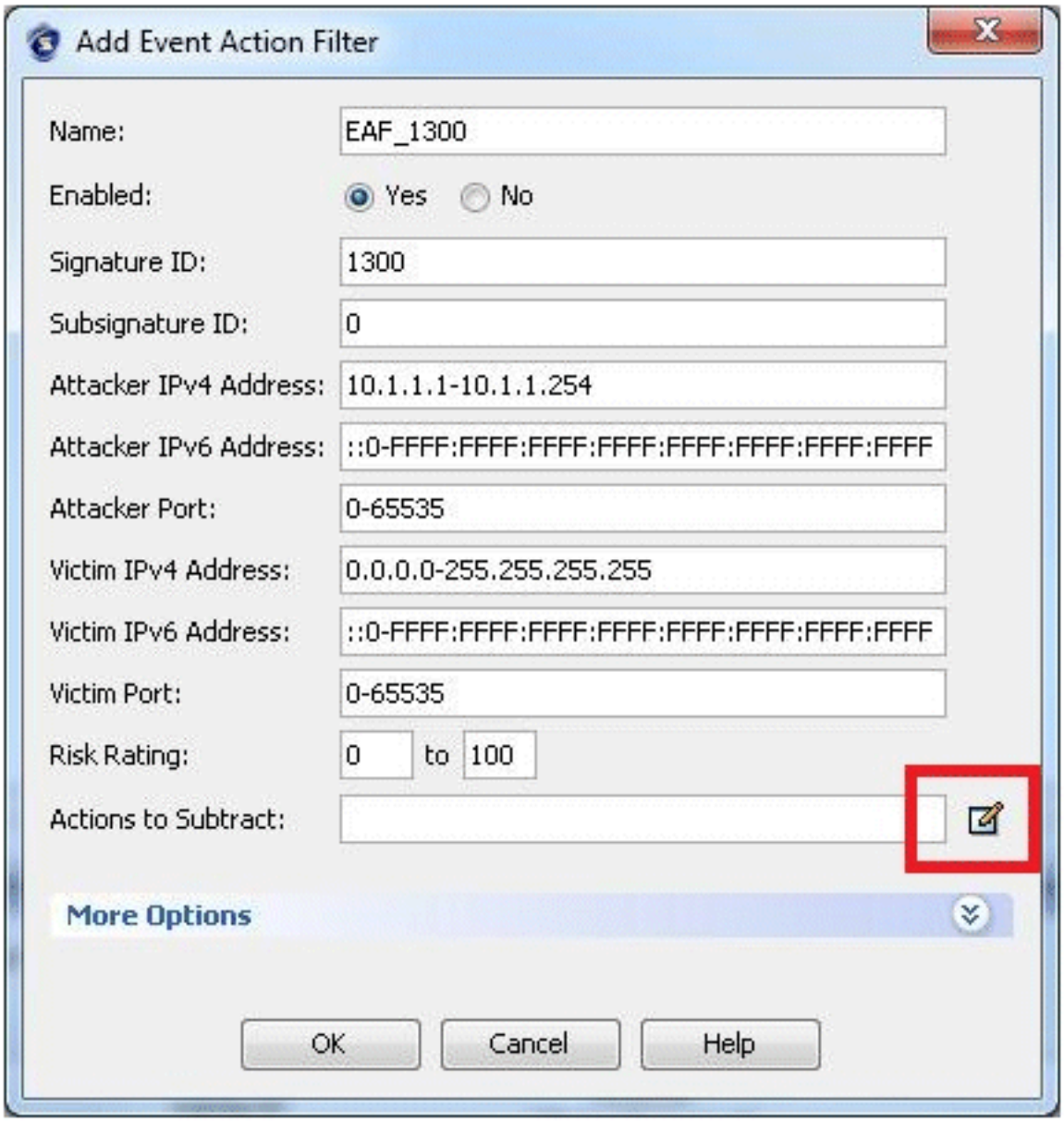


Se visualiza esta

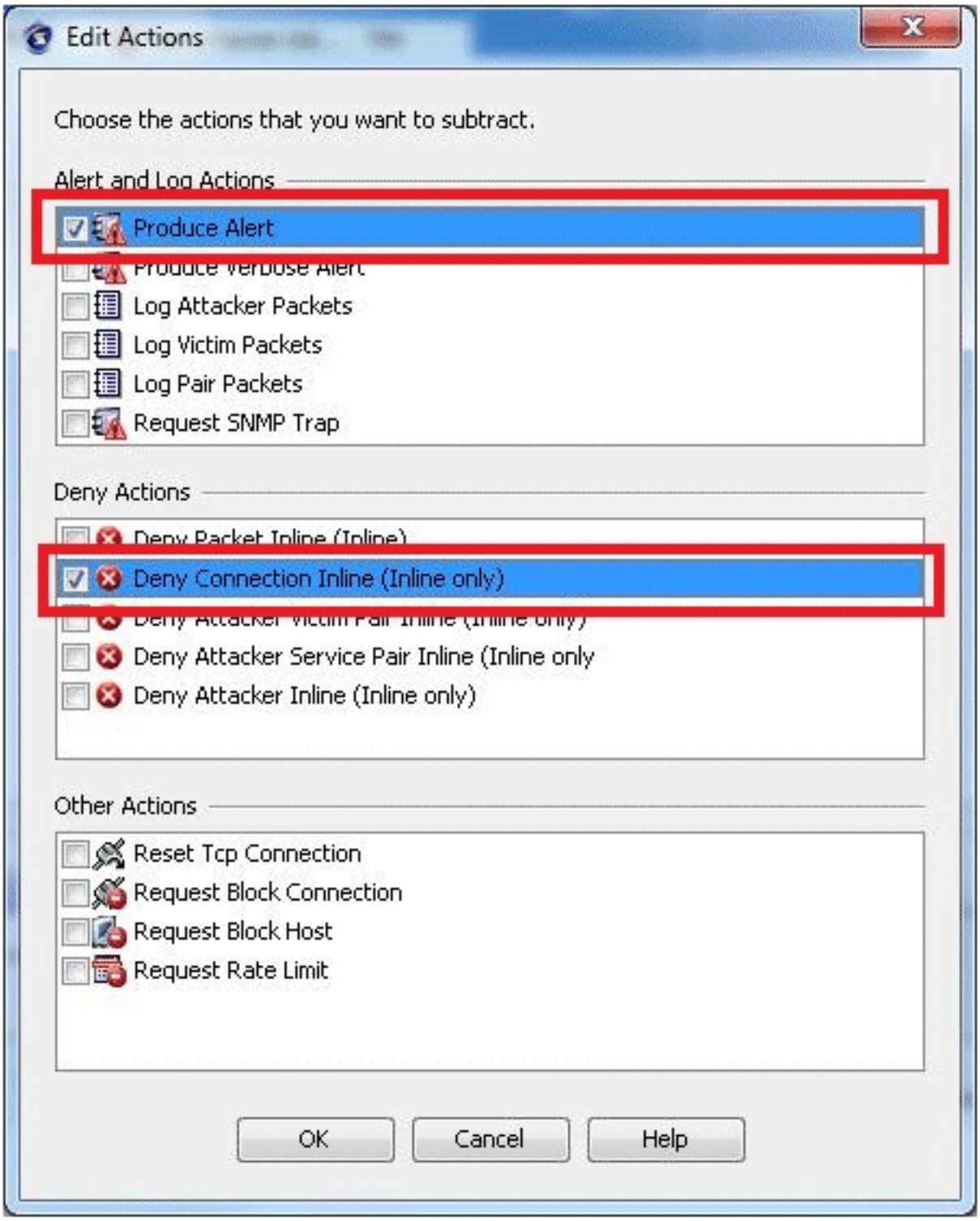


ventana: Configure los diversos campos tales como **IP del nombre**, del **ID de la firma**, del **atacante**,

etc. Haga clic el icono a la derecha de las **acciones para restar el** campo para abrir el cuadro de diálogo de las acciones del



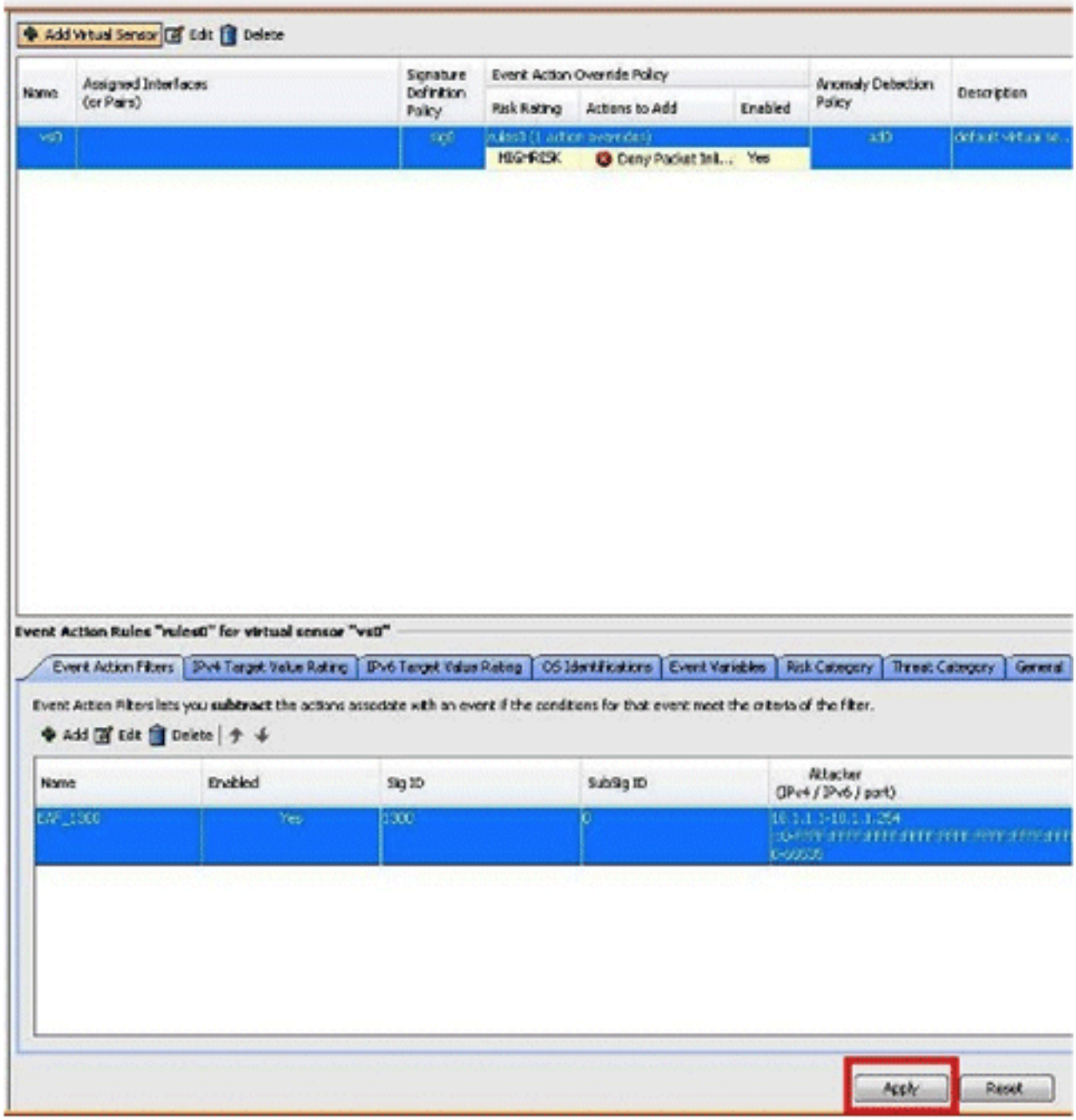
editar. En esta ventana, usted puede especificar las acciones de la firma que usted no quisiera que el IPS ejecutara.**Nota:** Para seleccionar correctamente las acciones de la firma que usted quiere restar, usted necesite entender las acciones predeterminadas de las firmas según lo descrito en el paso 1.En este ejemplo, elegimos la **alerta de la producción** y **negamos la conexión en**



línea. El IPS no tomará estas medidas si los 1300 activadores de la firma para el tráfico que viene a partir del 10.1.1.1-10.1.1.254.Para el resto del tráfico, la acción de la firma predeterminada de la **alerta de la producción** y **niega la conexión en línea** todavía se aplicará.Después de que usted elija la alerta de la producción y niegue el paquete en línea, usted verá estas acciones poblar en la parte inferior EAF de la

pantalla: El

Haga Click en OK, y entonces **se aplica** para salvar los cambios.



Para la configuración del filtro de la acción del evento usando el CLI, refiera a la sección de la interfaz de línea de comando IPS en la página de las guías de configuración. De la guía de configuración apropiada, haga clic **configurar las reglas de la acción del evento**, y busque para “configurar los filtros de la acción del evento”.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems