Ajuste o IPS para a prevenção do falso positivo usando o filtro da ação do evento

Índice

Introdução

Este documento fornece as etapas exigidas a fim ajustar o Intrusion Prevention System (IPS) para a prevenção do falso positivo usando o gerenciador de dispositivo IPS (IDM) ou o gerente IPS expresso (IME). O falso positivo que ajusta no IPS é conseguido por uma característica chamada o filtro de Evento Ação (CES).

Antes de Começar

Requisitos

Os leitores deste documento devem ter o conhecimento do ips Cisco.

Componentes Utilizados

A informação neste documento não é baseada na versão de hardware e software específica.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Compreendendo EAFs

EAFs é configurado primeiramente para o ajustamento do falso positivo. O CES fornece a capacidade para mandar uma assinatura particular não tomar ações desejadas para um subconjunto do tráfego.

EAFs é útil nas situações onde se exige para satisfazer circunstâncias múltiplas, como:

- A assinatura x não toma as ações y para uma sub-rede desejada do tráfego.
- A assinatura x toma as ações y para todo tráfego restante.

EAFs é útil ao lidar com a provocação benigna de uma assinatura.

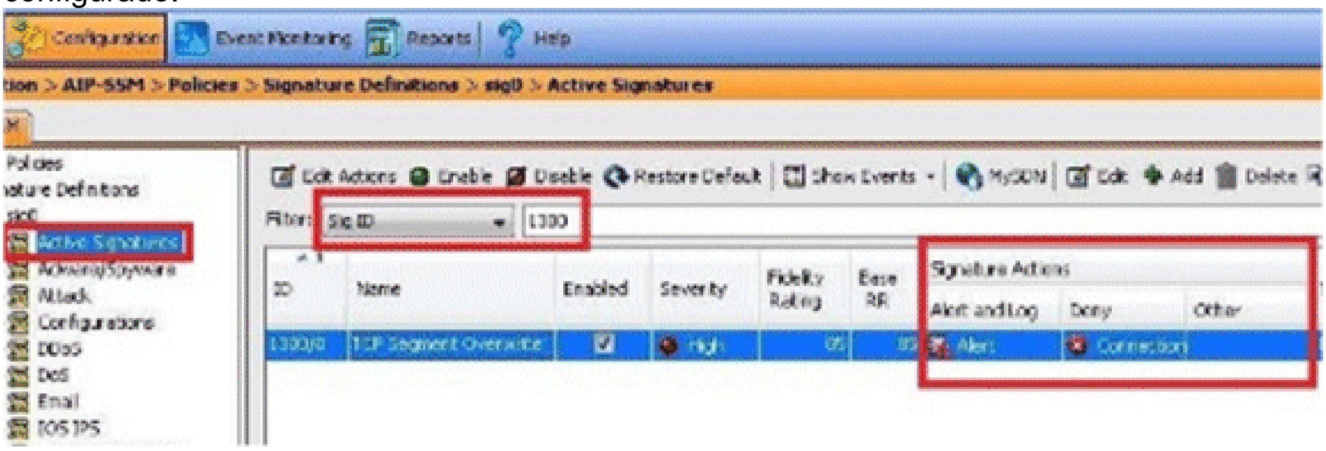
Configuração

Exemplo: Evento do falso positivo: Disparadores da assinatura 1300 para o tráfego que vem e aos host confiável conhecidos.

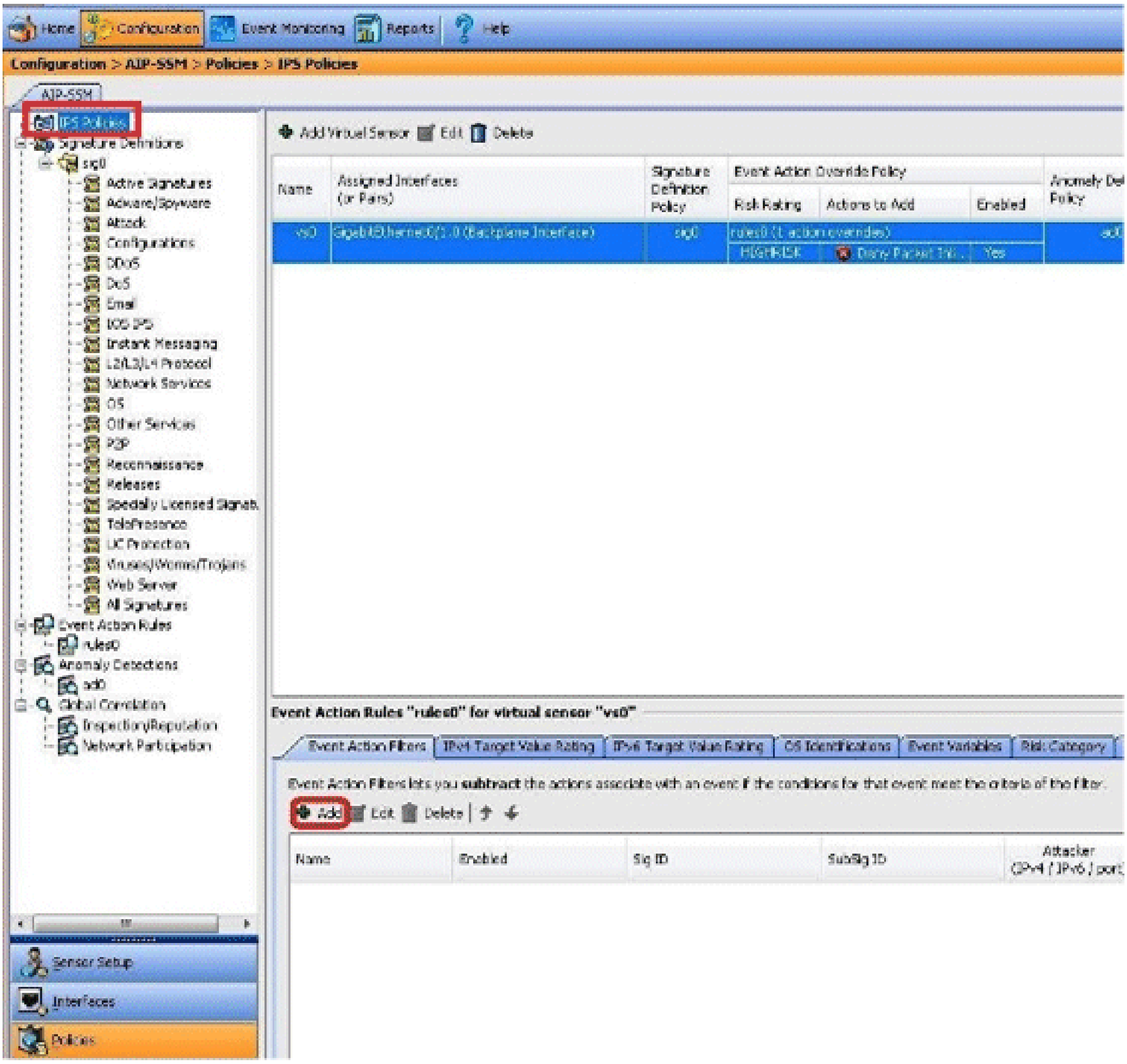
Nota: Esta é apenas finalidades de um exemplo para demonstração somente. Se você é incerto se um evento particular devido ao disparador da assinatura é benigno ou não, contacte o Suporte técnico de Cisco para a análise mais aprofundada.

Nota: Refira [assinaturas do Sistema de prevenção de intrusões da Cisco]() para obter informações adicionais sobre das assinaturas IPS.

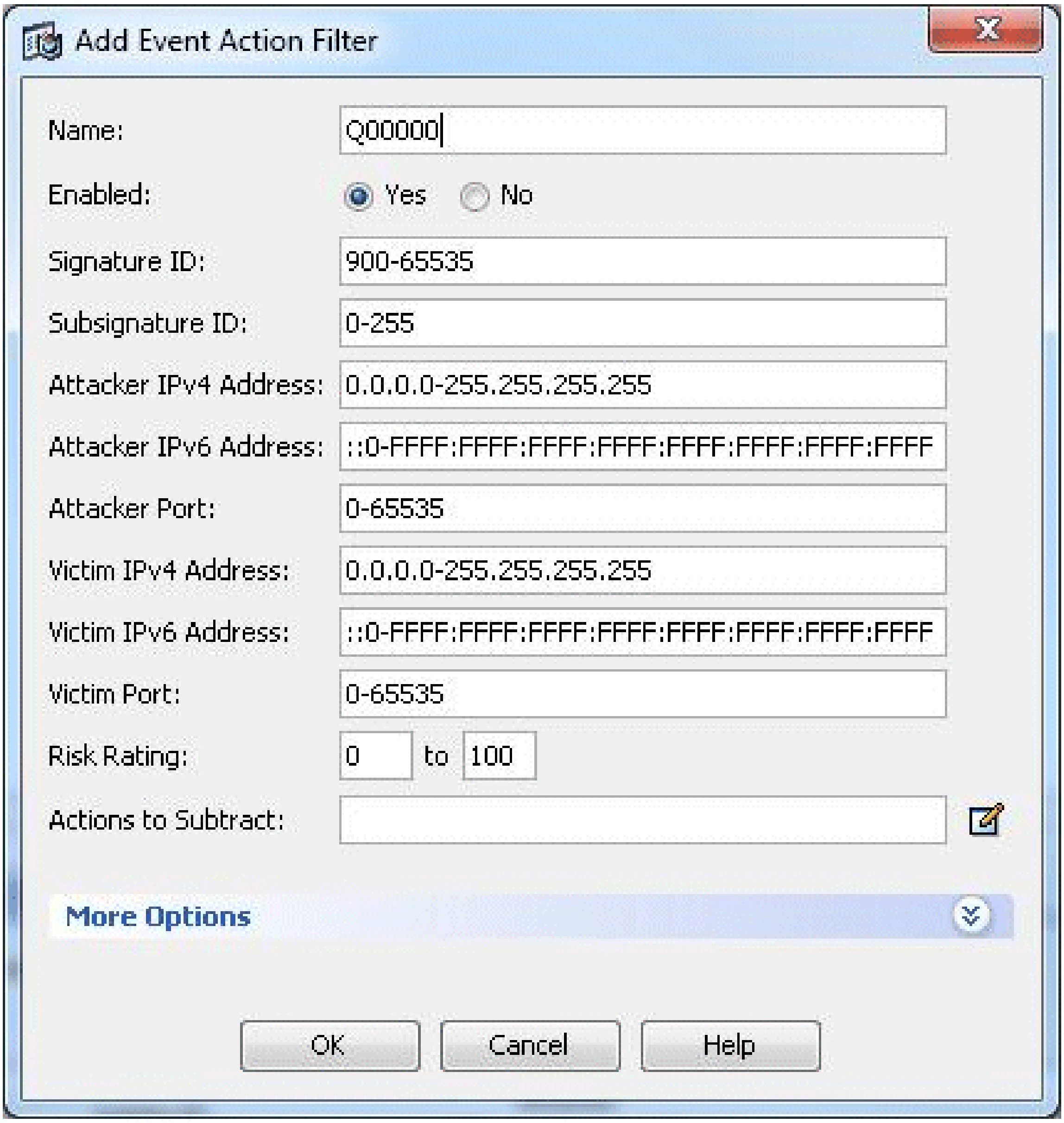
Conclua estes passos:

1. Verifique as ações padrão para ver se há a assinatura (1300, neste exemplo) para que o CES precisa de ser configurado.


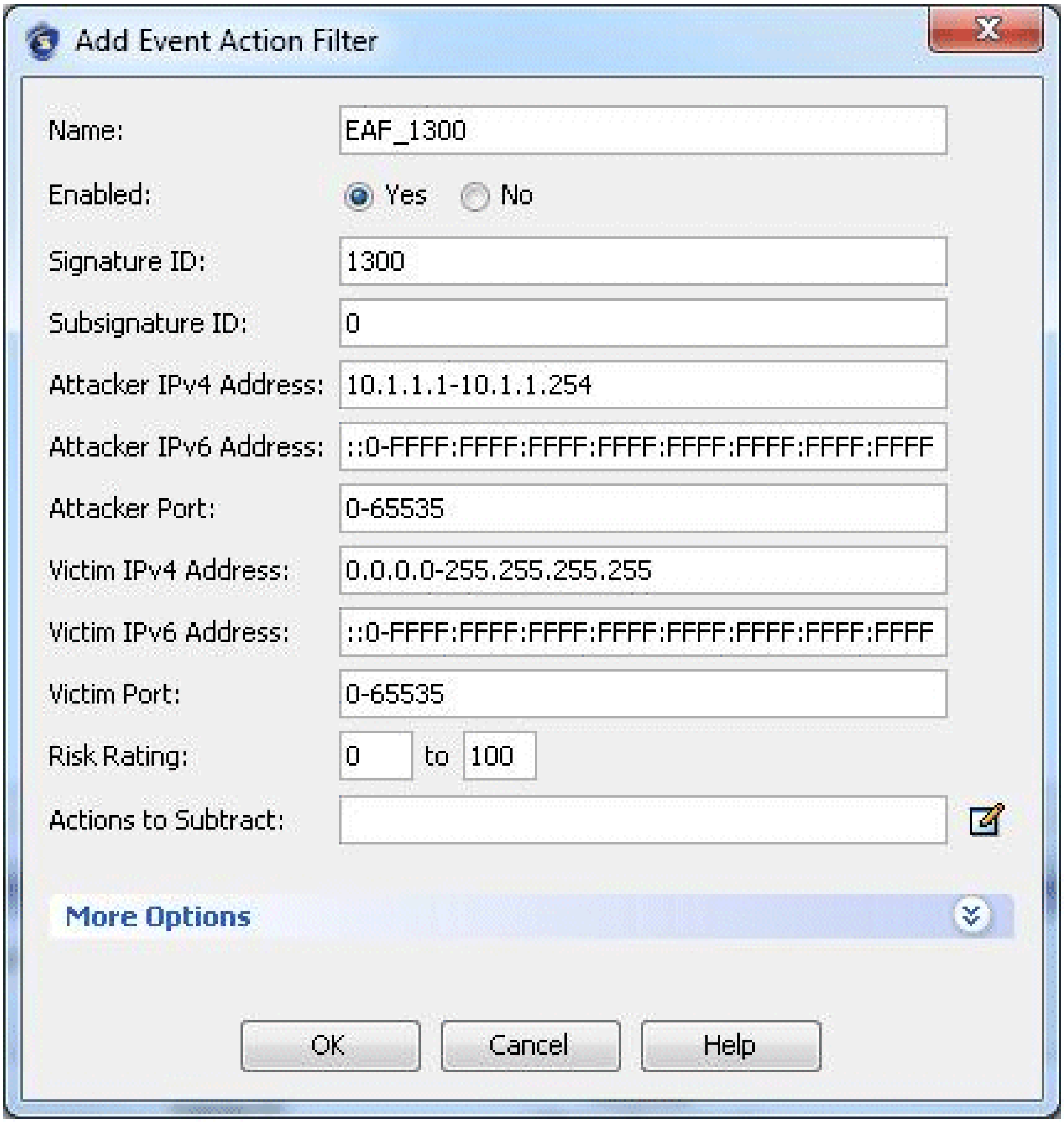
As ações padrão da assinatura 1300 incluem o **alerta do produto** e **negam a conexão Inline**.
2. Identifique os anfitriões para que esta assinatura não deve atear fogo. Por exemplo, você não quer a assinatura atear fogo para o tráfego que vem de uma sub-rede confiada, tal como 10.1.1.1-10.1.1.254.
3. Crie um CES para os critérios descritos em etapa 2:De IDM/IME, vá à **configuração** > às **políticas** > às **políticas IPS**. Clique a aba dos **filtros da ação do evento**. Sob esta aba, o clique **adiciona**.

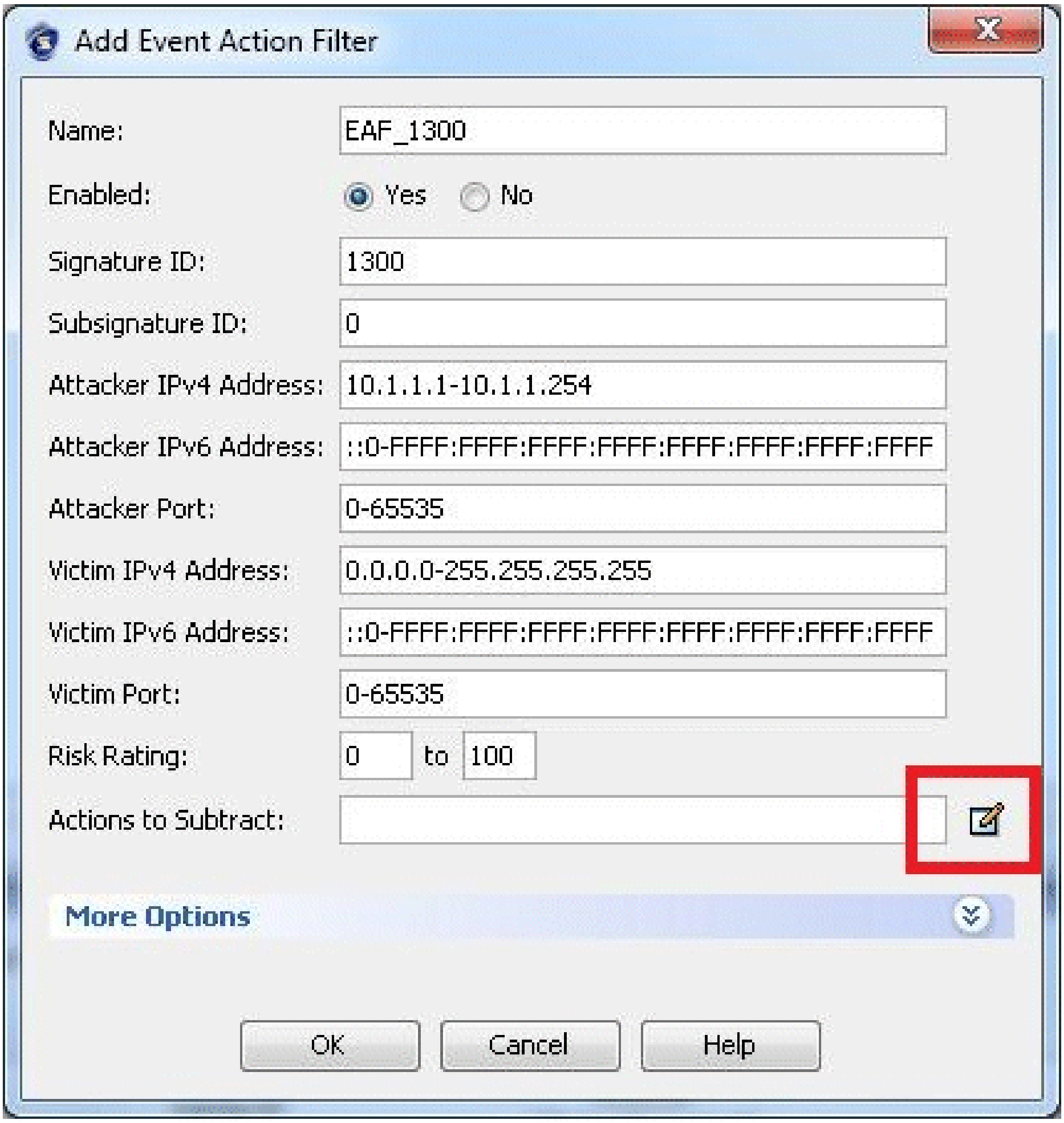


Este indicador é

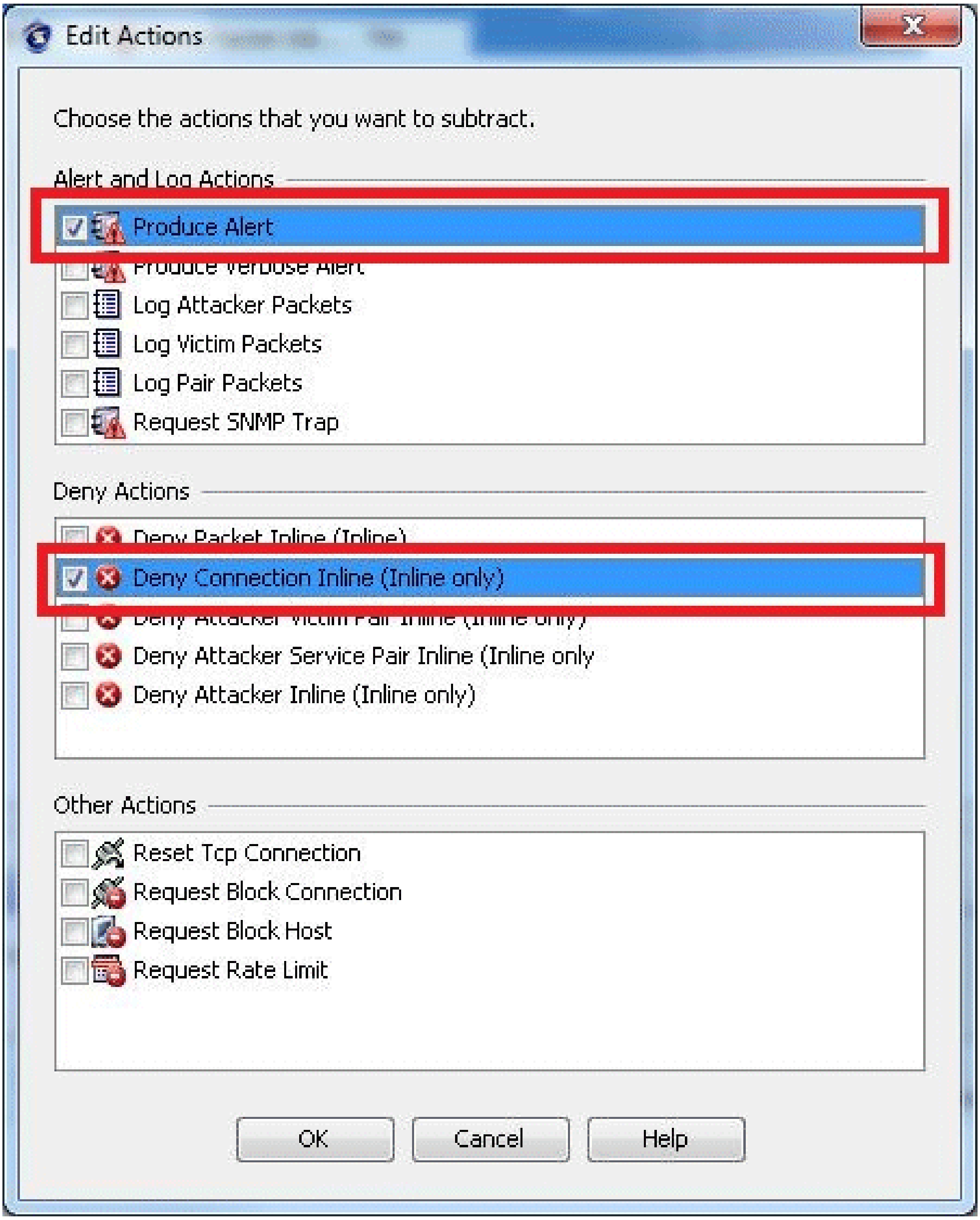
indicado: 

C
onfigurar os vários campos tais como o **IP do nome**, do **ID de assinatura**, do **atacante**,

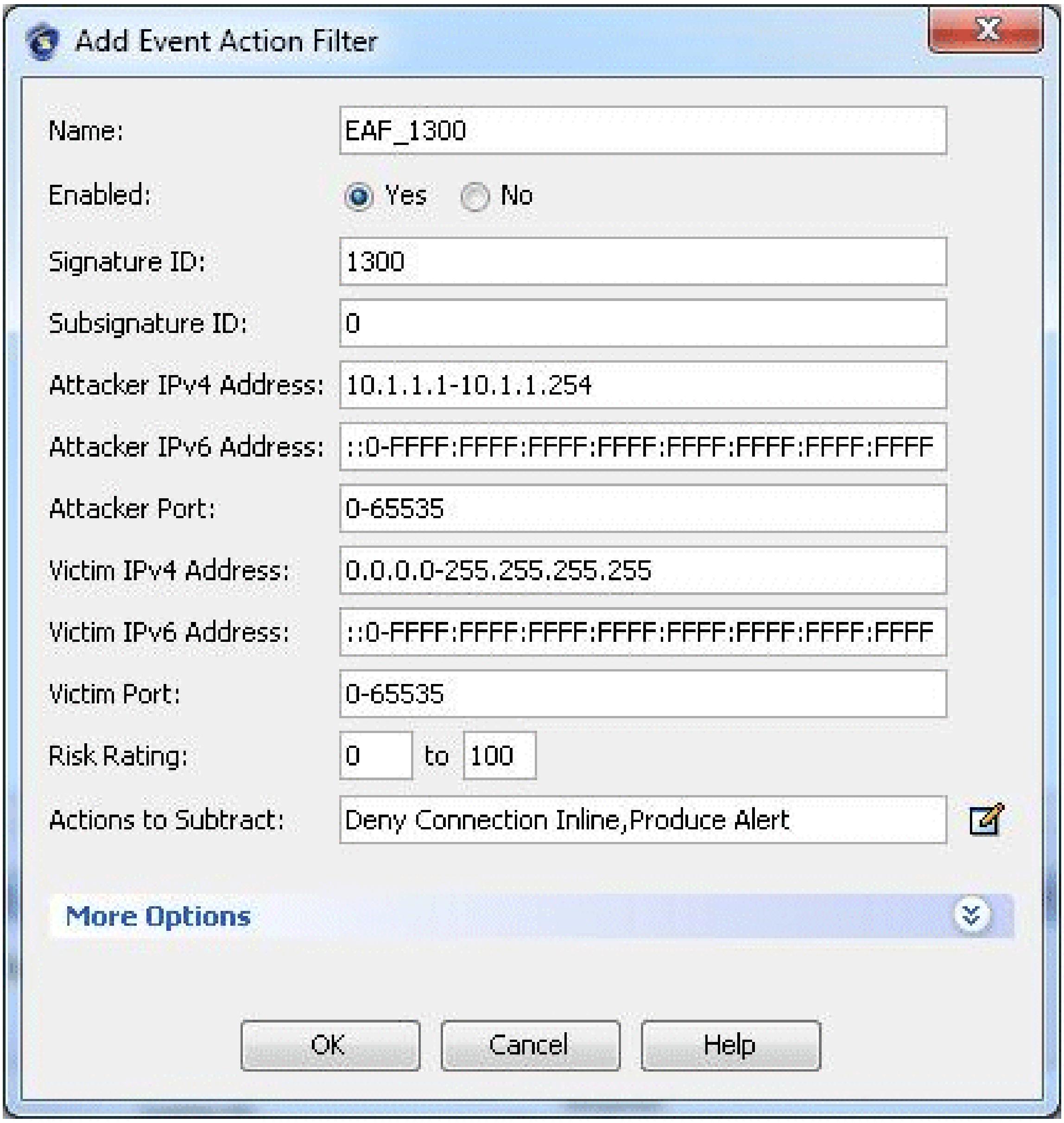
etc. 

Clique o ícone à direita das **ações para subtrair o** campo a fim abrir a caixa de diálogo das ações da edição. 

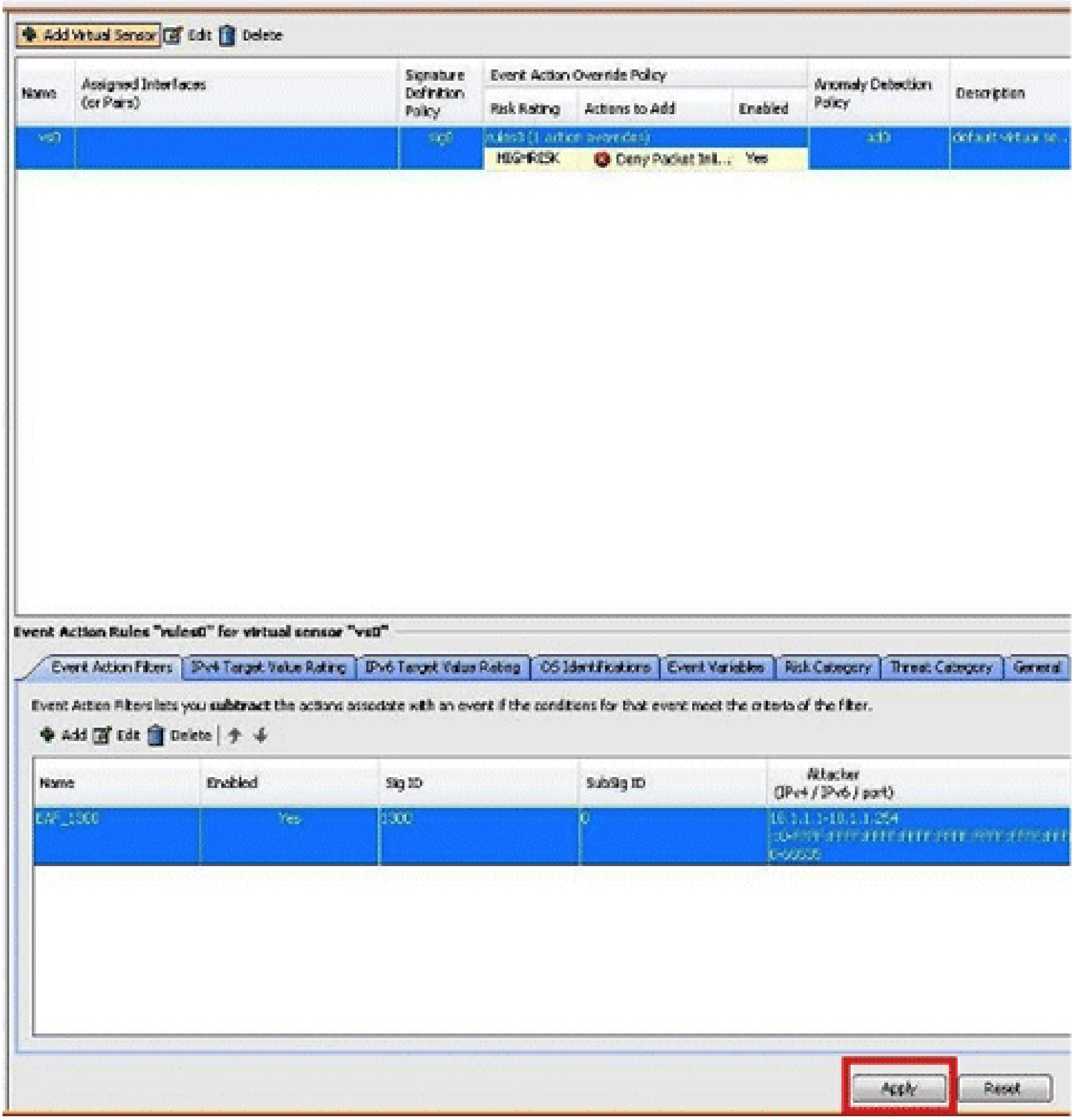
Neste indicador, você pode especificar as ações de assinatura que você não quer o IPS executar.**Nota:** A fim selecionar corretamente ações de assinatura que você quer subtrair, você precise de compreender as ações das assinaturas do padrão como descrito em etapa 1.Neste exemplo, nós escolhemos o **alerta do produto** e **negamos a conexão**



Inline.
O IPS não tomará estas ações se os 1300 disparadores da assinatura para o tráfego que vem de 10.1.1.1-10.1.1.254.Para todo tráfego restante, a ação de assinatura do padrão do **alerta do produto** e **nega a conexão Inline** ainda aplicar-se-á.Depois que você escolhe o alerta do produto e nega o pacote Inline, você verá estas ações povoar na parte inferior da tela

CES: 

Cliqu e a **APROVAÇÃO**, e **aplique-a** então a fim salvar as mudanças.



Para a configuração do filtro da ação do evento usando o CLI, refira a seção da interface da linha de comando IPS na [página dos manuais de configuração](). Do manual de configuração apropriado, clique **configurar regras da ação do evento**, e procure-o “configurando filtros da ação do evento”.

[Informações Relacionadas]()

- [Suporte Técnico e Documentação - Cisco Systems]()