

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

Índice

[Introdução](#)

[Antes de Começar](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Compreendendo EAFs](#)

[Configuração](#)

[Informações Relacionadas](#)

[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

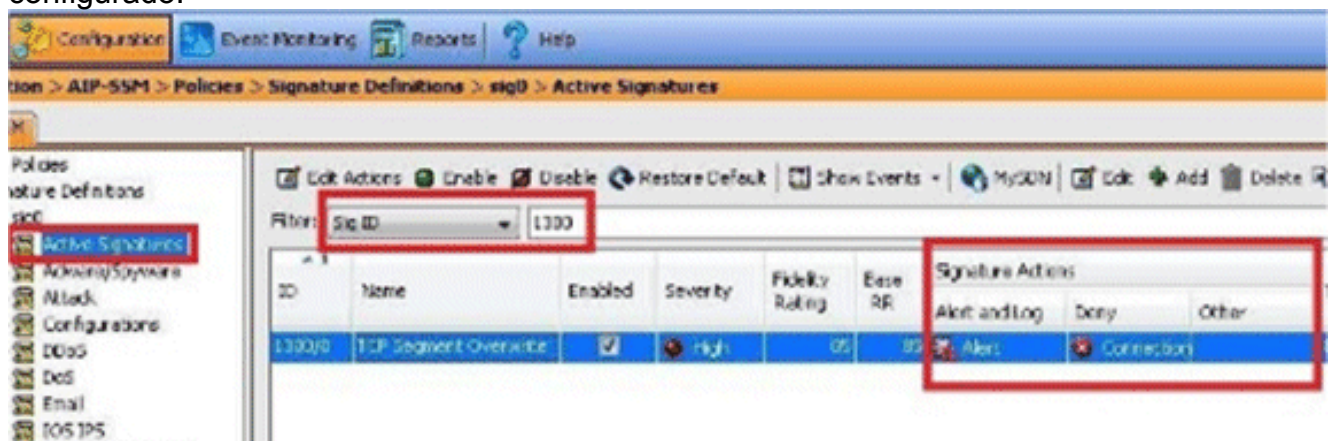
Exemplo: Evento do falso positivo: Disparadores da assinatura 1300 para o tráfego que vem e aos host confiável conhecidos.

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**.

Home Configuration Event Monitoring Reports Help

Configuration > AIP-SSM > Policies > IPS Policies

AIP-SSM

IPS Policies

Signature Definitions

- sig0
 - Active Signatures
 - Aware/Spyware
 - Attack
 - Configurations
 - DDoS
 - DoS
 - Email
 - IGMP IPS
 - Instant Messaging
 - L2/L3/L4 Protocol
 - Network Services
 - OS
 - Other Services
 - PGP
 - Reconnaissance
 - Releases
 - Specialty Licensed Signat...
 - TelePresence
 - UC Protection
 - Viruses/Worms/Trojans
 - Web Server
 - All Signatures
- Event Action Rules
- rules0
- Anomaly Detections
- ad0
- Global Correlation
- Inspection/Reputation
- Network Participation

Sensor Setup

Interfaces

Policies

Add Virtual Sensor Edit Delete

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Det Policy	
			Risk Rating	Actions to Add	Enabled		
vs0	GigabitEthernet0/1.0 (Backplane Interface)	sig0	rules0 (1 action overrides)	High-Risk	Deny Packet Tr...	Yes	ad0

Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters IPv4 Target Value Rating IPv6 Target Value Rating OS Identifications Event Variables Risk Category

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Add Edit Delete

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6) port
------	---------	--------	-----------	-----------------------------

Este indicador é

Add Event Action Filter

Name: Q00000

Enabled: Yes No

Signature ID: 900-65535

Subsignature ID: 0-255

Attacker IPv4 Address: 0.0.0.0-255.255.255.255

Attacker IPv6 Address: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF


Attacker Port: 0-65535


Victim IPv4 Address: 0.0.0.0-255.255.255.255

Victim IPv6 Address: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Victim Port: 0-65535

Risk Rating: 0 to 100

Actions to Subtract: 

More Options 

OK Cancel Help

indicado: configurar os vários campos tais como o IP do nome, do ID de assinatura, do atacante,

C

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

Actions to Subtract: 

More Options 

OK Cancel Help

etc.

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

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

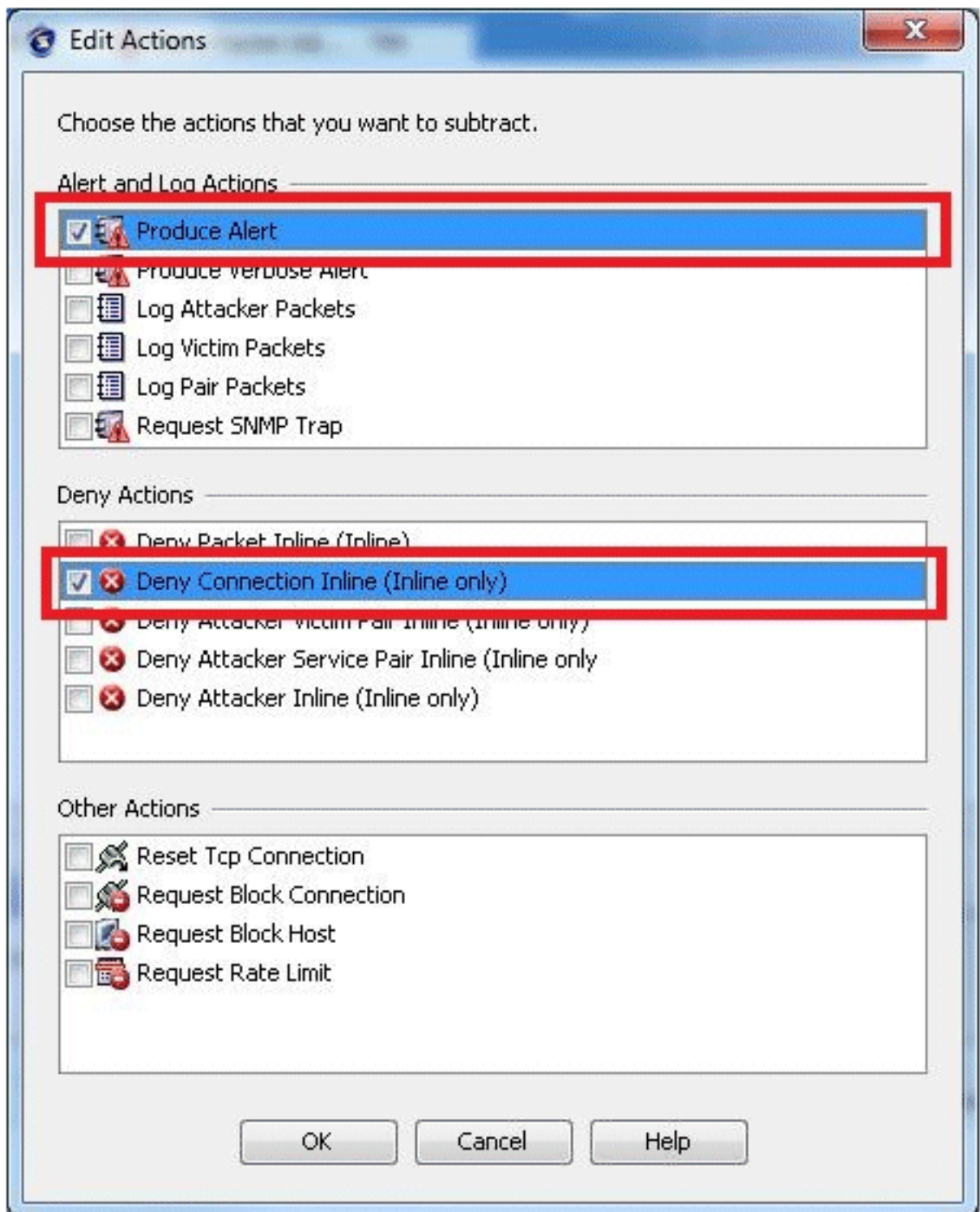
Actions to Subtract: 

More Options 

edição.

Nes

te 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

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

Actions to Subtract: 

More Options 

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

Cliqu

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description	
			Risk Rating	Actions to Add	Enabled			
vst0		sig0	rules0 (1 action override)	HIGH-RISK	Deny Packet 38...	Yes	add	default virtual se...

Event Action Rules "rules0" for virtual sensor "vst0"

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)
EAF_1000	Yes	1000	0	10.1.1.1-10.1.1.254 ip=10.1.1.1-10.1.1.254 p=80000

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](#)