Cisco IPS seguros - Excepto de alarmas falsamente positivas

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Alarmas falsa positivas y falsa negativas](#)
[Cisco IPS seguro excluye el mecanismo](#)
[Excluir un host](#)
[Excluir una red](#)
[Global inhabilite las firmas](#)
[Información Relacionada](#)

Introducción

Este documento describe la exclusión de alarmas positivas falsas en Cisco Secure Intrusion Prevention System (IPS).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión 7.0 segura del Sistema de prevención de intrusiones (IPS) de Cisco y el administrador del IPS de Cisco expresa 7.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Alarmas falsa positivas y falsa negativas

Cisco IPS seguro acciona una alarma cuando un paquete o una secuencia dado de paquetes hace juego las características de los perfiles del ataque conocido definidos en las firmas seguras de Cisco IPS. Un criterio de diseño crítico de la firma IPS es minimizar el acontecimiento del falso positivo y de las alarmas negativas falsas.

Los falsos positivos (activadores benignos) ocurren cuando el IPS señala cierta actividad benigna como malévola. Esto requiere la intervención humana diagnosticar el evento. Un gran número de falsos positivos pueden drenar perceptiblemente los recursos, y las habilidades especializadas requeridas analizarlos son costosas y difíciles de encontrar.

Las negativas falsas ocurren cuando el IPS no detecta y señala la actividad maliciosa real. La consecuencia de esto puede ser catastrófica y las firmas deben ser puestas al día continuamente mientras que se descubren los nuevos exploits y técnicas el cortar. Se le da una prioridad muy alta a la reducción de negativos falsos, a veces a expensas de más casos de positivos falsos.

Debido a la naturaleza de las firmas que los IPS utilizan para detectar la actividad maliciosa, es casi imposible eliminar totalmente los falsos positivos y las negativas sin seriamente la degradación de la eficacia del IPS o seriamente la interrupción de la infraestructura computacional de una organización (tal como host y redes). El ajustar personalizado cuando se despliega un IPS minimiza los falsos positivos. Se requieren nuevos ajustes periódicos cuando se modifica el entorno informático (por ejemplo, cuando se despliegan nuevos sistemas y aplicaciones). Cisco IPS seguro proporciona una capacidad de ajuste flexible que pueda minimizar los falsos positivos durante las operaciones de estado estacionario.

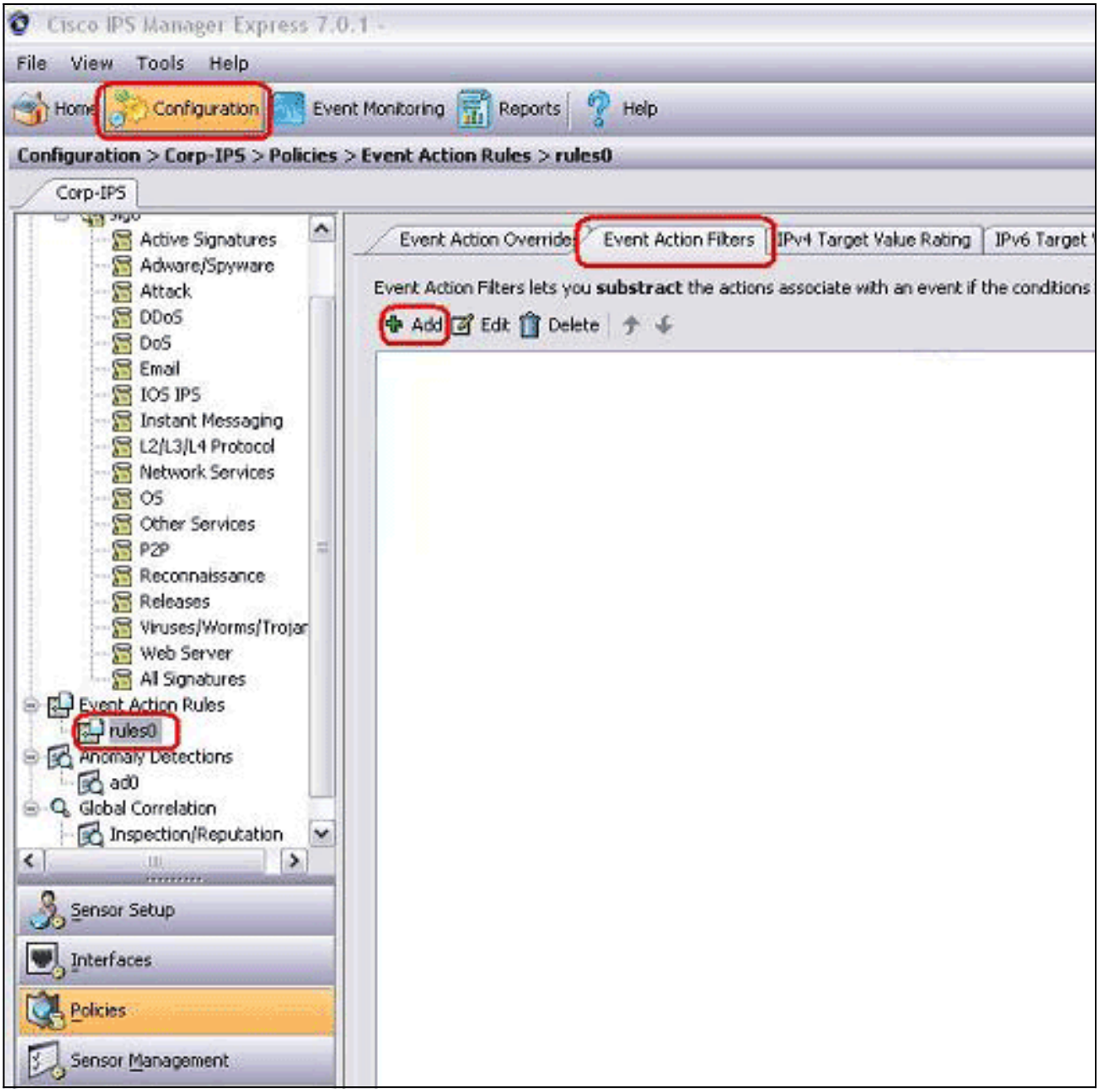
Cisco IPS seguro excluye el mecanismo

Cisco IPS seguro proporciona la capacidad para excluir una firma específica o a un host específico o a las direcciones de red. Las firmas excluidas no generan iconos de alarma o entradas en el registro cuando se activan desde los hosts o desde las redes que se excluyen específicamente a través de este mecanismo. Por ejemplo, una estación de administración de red pudo realizar la detección de red ejecutando los ping sweep, que accionan el barrido de red ICMP con la firma de la generación de eco (ID de la firma 2100). Si usted excluye la firma, usted no tiene que analizar la alarma y borrarla cada vez que el proceso para la detección de la red se ejecuta.

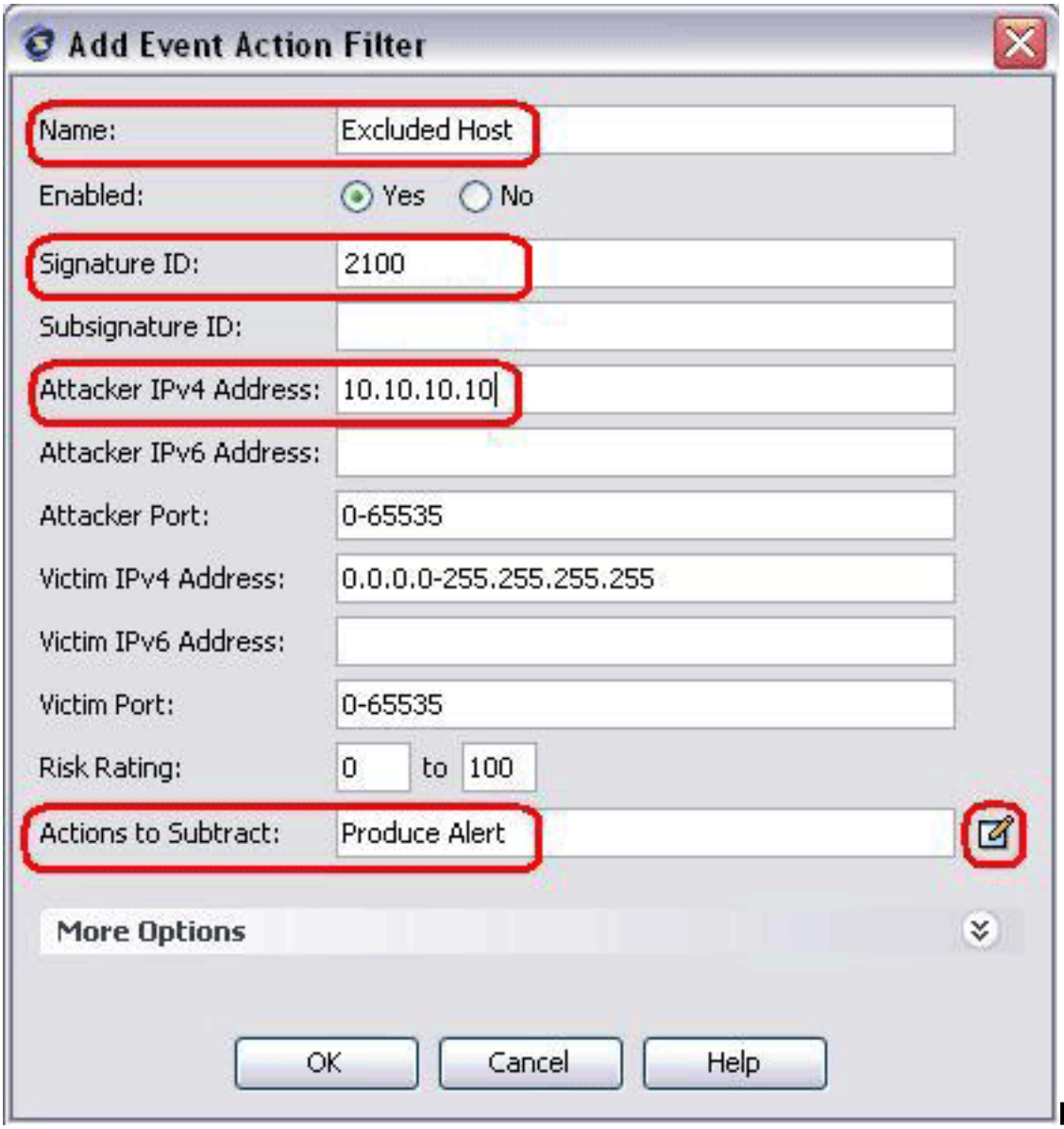
Excluir un host

Complete estos pasos para excluir un host específico (una dirección IP de origen) de generar una alarma de firma específica:

1. Elija la **configuración > el Corp-IPS > las directivas > las reglas de la acción del evento > rules0**, y haga clic la lengueta de los **filtros de la acción del evento**.



2. Haga clic en Add (Agregar).
3. Teclee el nombre del filtro, el ID de la firma, el direccionamiento del IPv4 del atacante, y la acción para restar en los campos adecuados, y después haga clic la AUTORIZACIÓN.



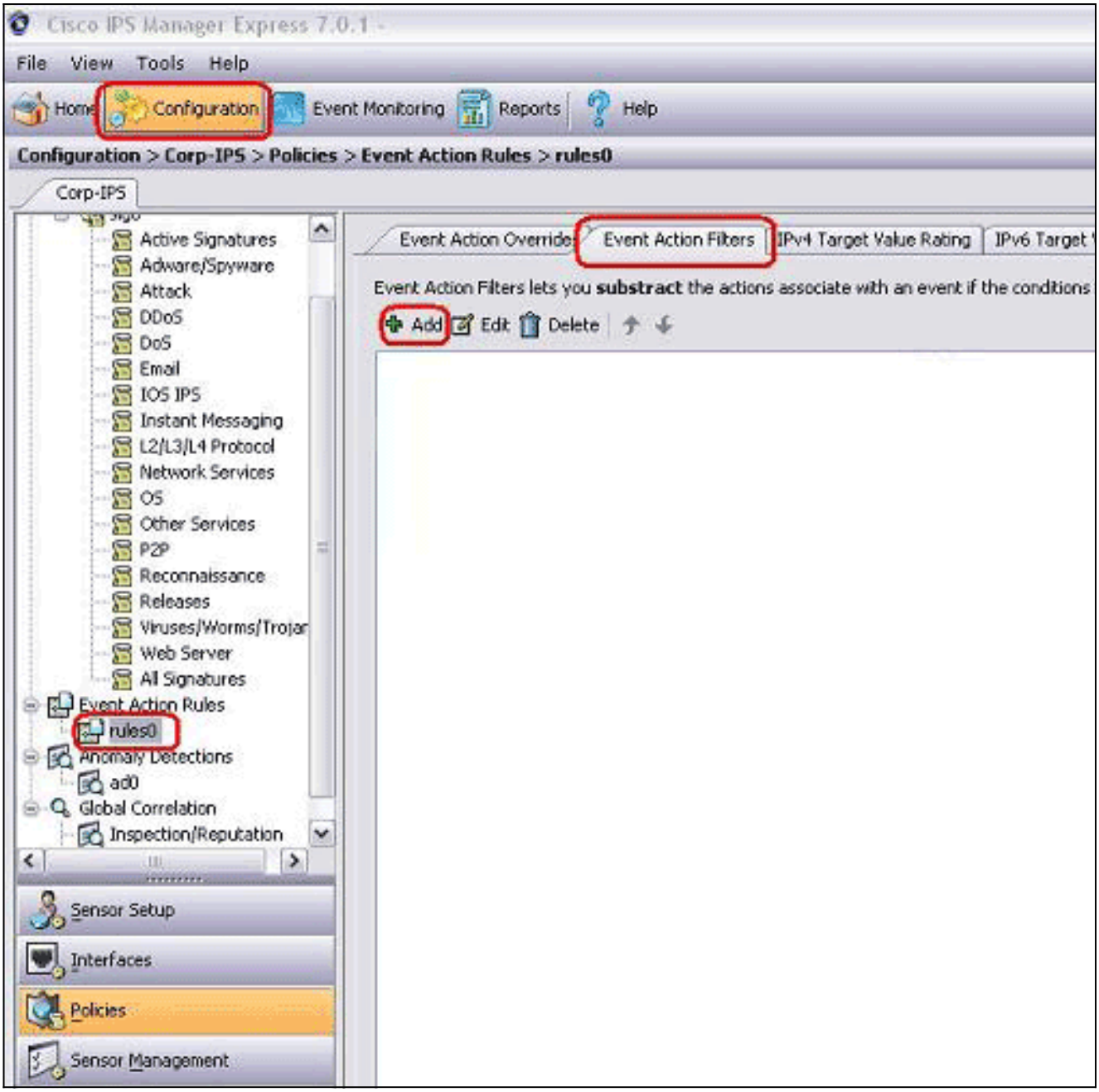
Nota: Si usted necesita excluir los IP Addresses múltiples de diversas redes, usted puede utilizar la coma como delimitador. Sin embargo, si usted utiliza una coma, evite el espacio final después de la coma; si no, usted puede ser que reciba un error.**Nota:** Además, usted puede utilizar las variables definidas en la lengueta de las variables de evento. Estas variables son útiles cuando el mismo valor se debe relanzar en los filtros de la acción de los eventos múltiples. Usted debe utilizar una muestra de dólar ($) como prefijo a la variable. La variable puede ser uno de estos formatos:Dirección IP completa; por ejemplo, 10.77.23.23.Rango de los IP Addresses; por ejemplo, 10.9.2.10-10.9.2.155.Conjunto de rango de los IP Addresses; por ejemplo, 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11.

Excluir una red

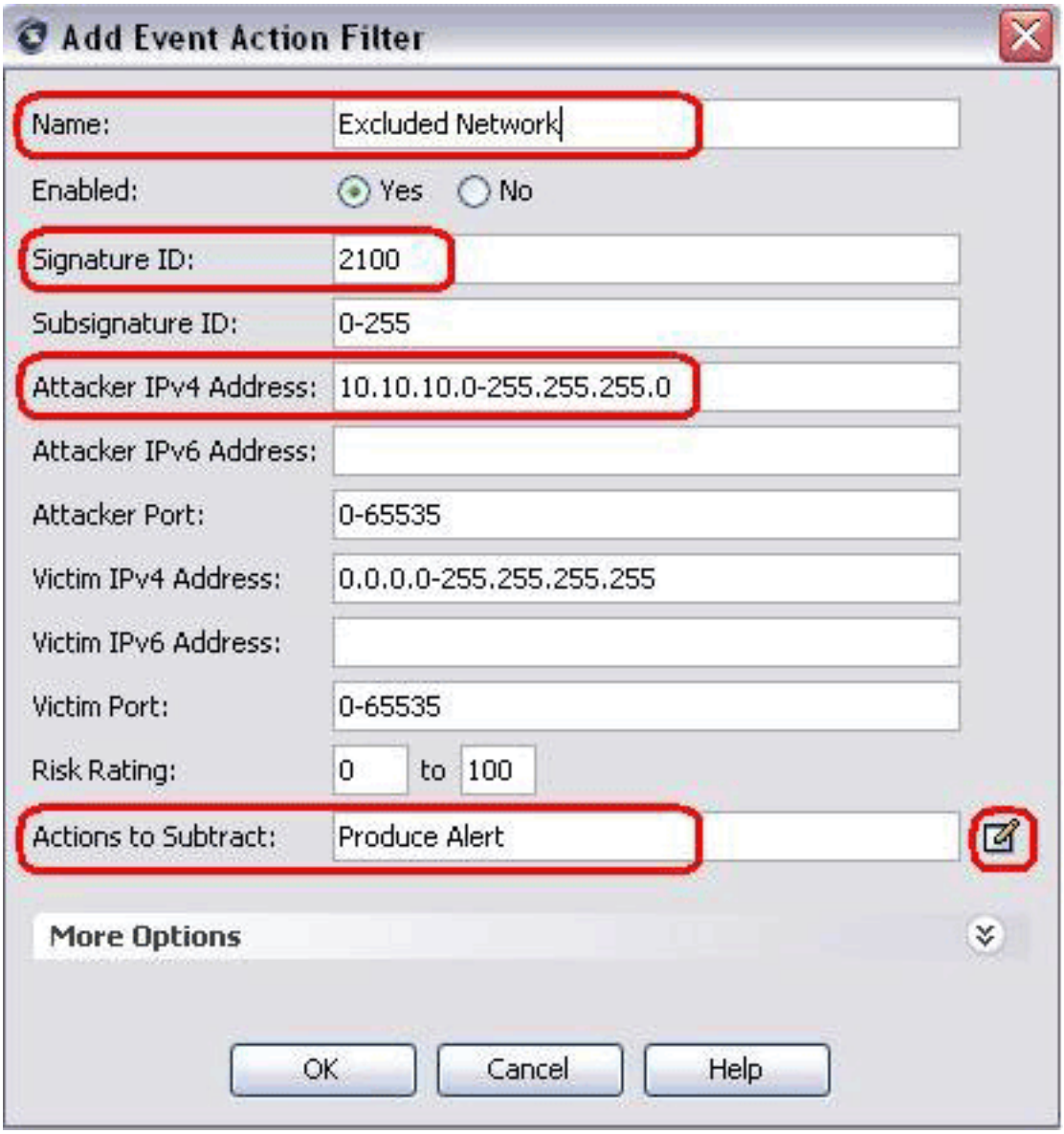
El filtro de la acción del evento también excluye las firmas específicas para encender una alarma basada en una dirección de red de origen o destino.

Complete estos pasos para excluir una red de generar una alarma de firma específica:

1. Haga clic la lengueta de los **filtros de la acción del evento**.



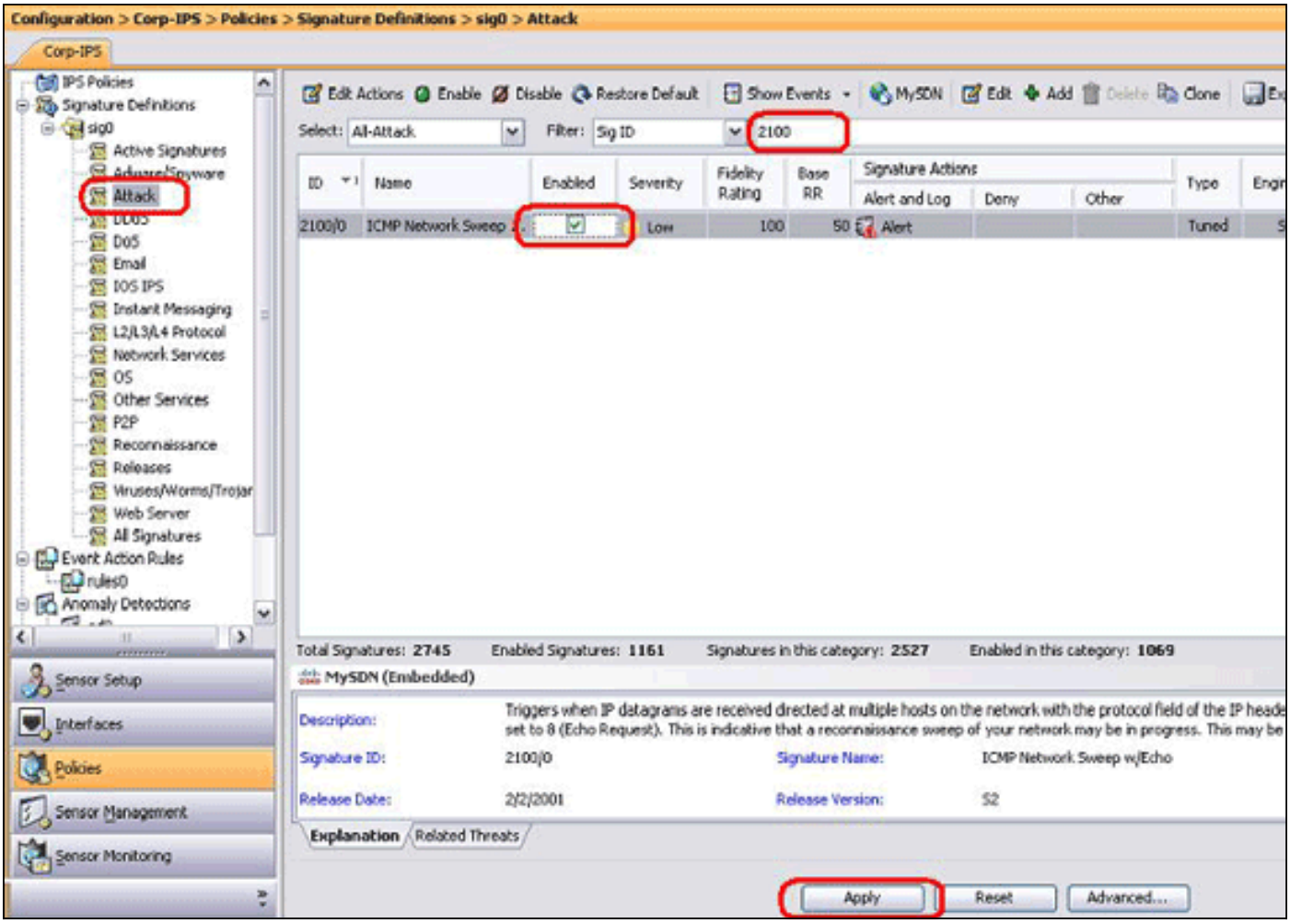
2. Haga clic en Add (Agregar).
3. Teclee el nombre, el ID de la firma, la dirección de red con la máscara de subred, y la acción del filtro para restar en los campos adecuados, y después haga clic la AUTORIZACIÓN.



Global inhabilite las firmas

Usted puede ser que quiera inhabilitar una firma de alarmar en cualquier momento. Para habilitar, inhabilitar, y retirar las firmas, complete estos pasos:

1. Inicie sesión a IME usando una cuenta con los privilegios del administrador o del operador.
2. Elija la **configuración** > el **sensor_name** > las **directivas** > las **definiciones de la firma** > **sig0** > **todas las firmas**.
3. Para localizar una firma, elija una opción de clasificación de la lista desplegable del filtro. Por ejemplo, si usted está buscando para una firma del barrido de red ICMP, elija **todas las firmas** bajo sig0, después busque por el ID de la firma o nómbrelas. El cristal sig0 restaura y visualiza solamente esas firmas que hagan juego sus criterios de clasificación.
4. Para habilitar o inhabilitar una firma existente, elija la firma, y complete estos pasos:Vea la columna habilitada para determinar el estatus de la firma. Una firma se habilita que tiene la casilla de verificación marcada.Para habilitar una firma se inhabilite que, marque la casilla de verificación **habilitada**.Para inhabilitar una firma se habilite que, desmarque la casilla de verificación **habilitada**.Para retirar una o más firmas, elija las firmas, haga clic con el botón derecho del ratón, y después haga clic el **estatus del cambio a > retirado**.
5. El tecleo **se aplica** para aplicar sus cambios y salvar la configuración revisada.



Información Relacionada

- Final de la venta para el director del Cisco Secure IDS
- Página de soporte de Cisco Secure Intrusion Detection
- Soporte Técnico y Documentación - Cisco Systems