IPS 5.x y posterior: Ajustar la firma con el filtro de la acción del evento usando el CLI y el IDM

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Filtros de la acción del evento](#)
[Comprensión de los filtros de la acción del evento](#)
[Configuración de filtros de la acción del evento usando el CLI](#)
[Configuración de filtros de la acción del evento usando el IDM](#)
[Configuración variable del evento](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo ajustar la firma con el filtro de la acción del evento en el (IPS) del Cisco Intrusion Prevention System con el comando line interface(cli) y el IDS Device Manager (IDM).

prerrequisitos

Requisitos

Este documento asume que el IPS de Cisco está instalado y trabaja correctamente.

Componentes Utilizados

La información en este documento se basa en el dispositivo de las Cisco 4200 Series IDS/IPS que funciona con la versión de software 5.0 y posterior.

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.

Filtros de la acción del evento

Comprensión de los filtros de la acción del evento

Se procesan los filtros de la acción del evento mientras que una lista ordenada y usted pueden mover los filtros hacia arriba o hacia abajo en la lista.

Los filtros dejaron el sensor realizar ciertas acciones en respuesta al evento sin requerir el sensor realizar todas las acciones o quitar el evento entero. Los filtros funcionan por el retiro de las acciones de un evento. Un filtro que quita todas las acciones de un evento con eficacia consume el evento.

Note: Cuando usted filtra las firmas del barrido, Cisco recomienda que usted no filtra a las direcciones destino. Si hay direcciones de destino múltiple, sólo el direccionamiento más reciente se utiliza para hacer juego el filtro.

Usted puede configurar los filtros de la acción del evento para quitar las acciones específicas de un evento o para desechar un evento entero y para prevenir el procesamiento adicional por el sensor. Usted puede utilizar las variables de acción del evento que usted definió a los grupos de dirección para sus filtros. Para el procedimiento en cómo configurar las variables de acción del evento, vea agregar, editar, y borrar la sección de las variables de acción del evento.

Note: Usted debe introducir la variable con una muestra de dólar ($) para indicar que usted utiliza una variable bastante que una cadena. Si no, usted recibe la `malos fuente y error del destino.`

Configuración de filtros de la acción del evento usando el CLI

Complete estos pasos para configurar los filtros de la acción del evento:

1. Inicie sesión al CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese el submode de las reglas de la acción del evento:
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. Cree el nombre del filtro:
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   Utilice **name1, name2**, y así sucesivamente para nombrar sus filtros de la acción del evento. Utilice el **comenzar | Finalizar | desactivado | antes | después de que** palabras claves para especificar donde usted quiere insertar el filtro.
4. Especifique los valores para este filtro:Especifique el rango del ID de la firma:
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   El valor por defecto es 900 a 65535.Especifique el rango del subsignature ID:
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

   El valor por defecto es 0 a 255.Especifique el intervalo de direcciones del atacante:
   ```
   sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
   ```

El valor por defecto es 0.0.0.0 a 255.255.255.255.Especifique el intervalo de direcciones de la víctima:
```
sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
```

El valor por defecto es 0.0.0.0 a 255.255.255.255.Especifique el rango de puertos de la víctima:
```
sensor(config-eve-fil)#victim-port-range 0-434
```

El valor por defecto es 0 a 65535.Especifique la importancia OS:
```
sensor(config-eve-fil)#os-relevance relevant
```

El valor por defecto es 0 a 100.Especifique el rango del grado de riesgo.
```
sensor(config-eve-fil)#risk-rating-range 85-100
```

El valor por defecto es 0 a 100.Especifique las acciones para quitar:
```
sensor(config-eve-fil)#actions-to-remove reset-tcp-connection
```

Si usted filtra una acción de la negación, fije el porcentaje de niegan las acciones que usted quiere:
```
sensor(config-eve-fil)#deny-attacker-percentage 90
```

El valor por defecto es 100.Especifique el estatus del filtro a inhabilitado o a habilitado.
```
sensor(config-eve-fil)#filter-item-status {enabled | disabled}
```

Se habilita el valor por defecto.Especifique la parada en el parámetro de la coincidencia.
```
sensor(config-eve-fil)#stop-on-match {true | false}
```

Verdad dice el sensor parar el procesar de los filtros si este elemento hace juego. Falso dice el sensor continuar procesando los filtros incluso si este elemento hace juego.Agregue los algunos comentarios que usted quiere utilizar para explicar este filtro:
```
sensor(config-eve-fil)#user-comment NEW FILTER
```

5. Verifique las configuraciones para el filtro:
```
sensor(config-eve-fil)#show settings
 NAME: name1

   ----------------------------------------------

      signature-id-range: 1000-10005 default: 900-65535

      subsignature-id-range: 1-5 default: 0-255

      attacker-address-range: 10.89.10.10-10.89.10.23 default: 0.0.0.0-255.255.255.255

      victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255

      attacker-port-range: 0-65535 <defaulted>

      victim-port-range: 1-343 default: 0-65535

      risk-rating-range: 85-100 default: 0-100

      actions-to-remove: reset-tcp-connection default:

      deny-attacker-percentage: 90 default: 100
```

```
      filter-item-status: Enabled default: Enabled

      stop-on-match: True default: False

      user-comment: NEW FILTER default:

      os-relevance: relevant default: relevant|not-relevant|unknown

   ------------------------------------------------

senor(config-eve-fil)#
```

6. Para editar un filtro existente:

```
sensor(config-eve)#filters edit name1
```

7. Edite los parámetros y vea los pasos 4a con 4l para más información.
8. Para mover un filtro hacia arriba o hacia abajo en la lista de filtros:

```
sensor(config-eve-fil)#exit
sensor(config-eve)#filters move name5 before name1
```

9. Verifique que usted haya movido los filtros:

```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

 ------------------------------------------------

   filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)

   ------------------------------------------------

   ACTIVE list-contents

   ------------------------------------------------

      NAME: name5

      ------------------------------------------------

         signature-id-range: 900-65535 <defaulted>

         subsignature-id-range: 0-255 <defaulted>

         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

         attacker-port-range: 0-65535 <defaulted>

         victim-port-range: 0-65535 <defaulted>

         risk-rating-range: 0-100 <defaulted>

         actions-to-remove: <defaulted>

         filter-item-status: Enabled <defaulted>

         stop-on-match: False <defaulted>

         user-comment: <defaulted>

      ------------------------------------------------

      ------------------------------------------------
```

```
   NAME: name1
   ------------------------------------------------
      signature-id-range: 900-65535 <defaulted>
      subsignature-id-range: 0-255 <defaulted>
      attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 0-65535 <defaulted>
      risk-rating-range: 0-100 <defaulted>
      actions-to-remove: <defaulted>
      filter-item-status: Enabled <defaulted>
      stop-on-match: False <defaulted>
      user-comment: <defaulted>
   ------------------------------------------------
   ------------------------------------------------
   NAME: name2
   ------------------------------------------------
      signature-id-range: 900-65535 <defaulted>
      subsignature-id-range: 0-255 <defaulted>
      attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 0-65535 <defaulted>
      risk-rating-range: 0-100 <defaulted>
      actions-to-remove: <defaulted>
      filter-item-status: Enabled <defaulted>
      stop-on-match: False <defaulted>
      user-comment: <defaulted>
   ------------------------------------------------
   ------------------------------------------------
-----------------------------------------------
INACTIVE list-contents
```

```
    ------------------------------------------

  ----------------------------------------

  sensor(config-eve)#
```

10. Para mover un filtro a la lista inactiva:
```
sensor(config-eve)#filters move name1 inactive
```

11. Verifique que el filtro se haya movido a la lista inactiva:
```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

    ------------------------------------------

    INACTIVE list-contents

    ------------------------------------------

        ------------------------------------------

        NAME: name1

        ------------------------------------------

            signature-id-range: 900-65535 <defaulted>

            subsignature-id-range: 0-255 <defaulted>

            attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>

            victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>

            attacker-port-range: 0-65535 <defaulted>

            victim-port-range: 0-65535 <defaulted>

            risk-rating-range: 0-100 <defaulted>

            actions-to-remove: <defaulted>

            filter-item-status: Enabled <defaulted>

            stop-on-match: False <defaulted>

            user-comment: <defaulted>

        ------------------------------------------

        ------------------------------------------

sensor(config-eve)#
```

12. Salga el submode de las reglas de la acción del evento:
```
sensor(config-eve)#exit
Apply Changes:?[yes]:
```

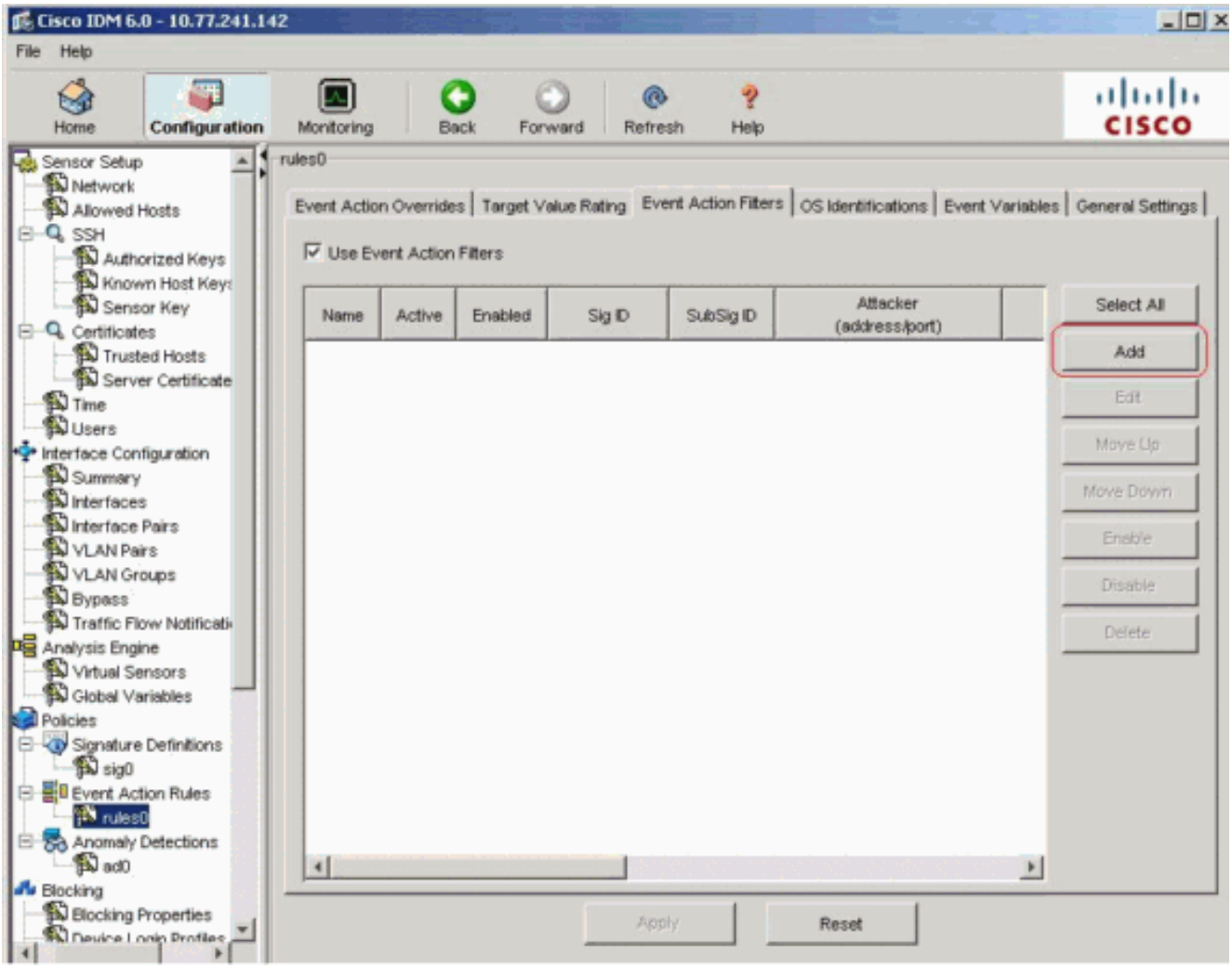
13. Presione ENTER para aplicar sus cambios o ingresar **ningún** para desecharlos.

Configuración de filtros de la acción del evento usando el IDM

Complete estos pasos para agregar, editar, borrar, habilitar, inhabilitar, y mover los filtros de la

acción del evento:

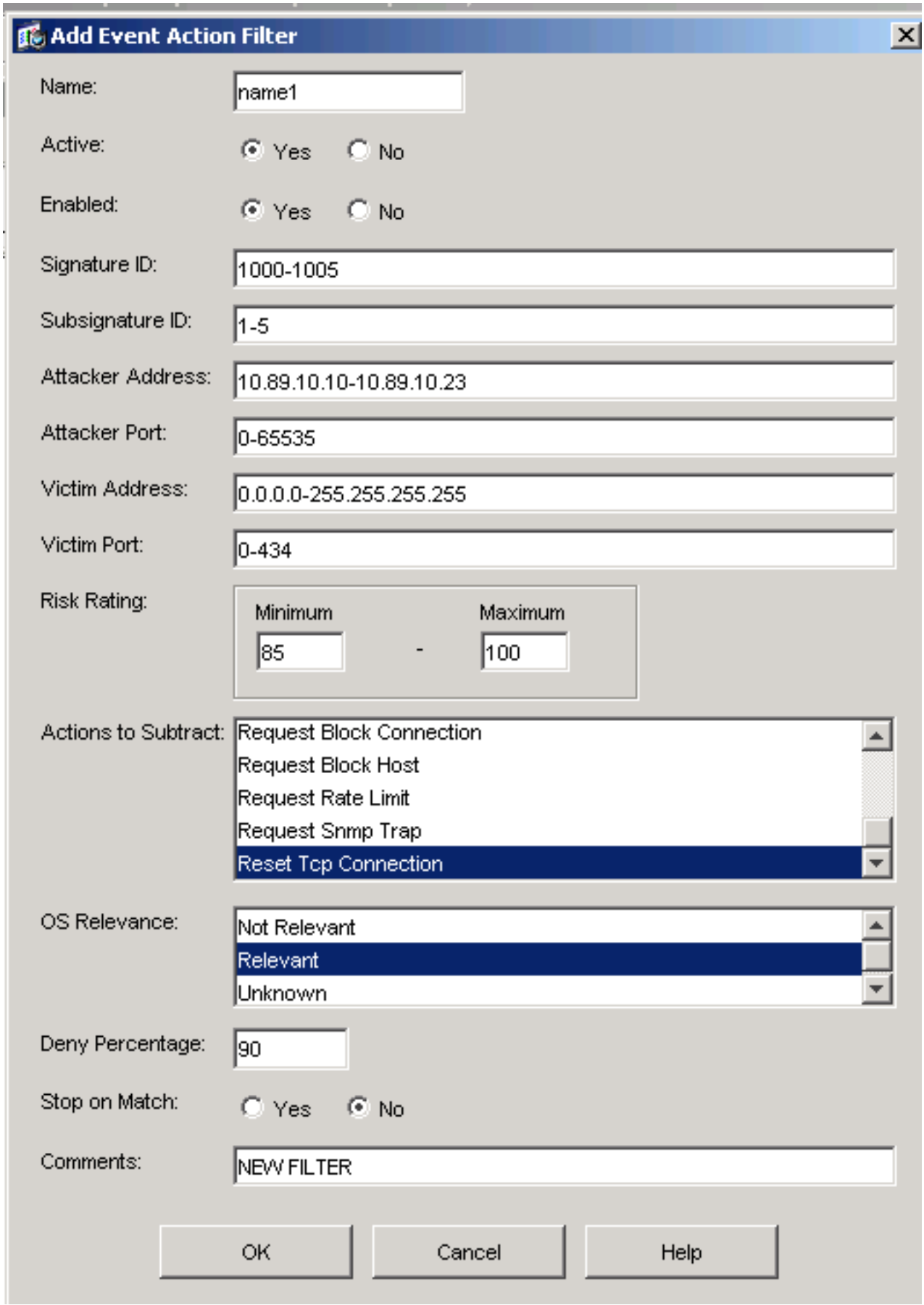
1. Inicie sesión al IDM con una cuenta que tenga privilegios del administrador o del operador.
2. Elija la **configuración > las directivas > las reglas de la acción del evento > rules0 > los filtros de la acción del evento** si la versión de software es 6.x. Para la versión de software 5.x, elija los **filtros de la acción de las reglas > del evento de la configuración > de la acción del evento.**La lengueta de los filtros de la acción del evento aparece como se muestra.



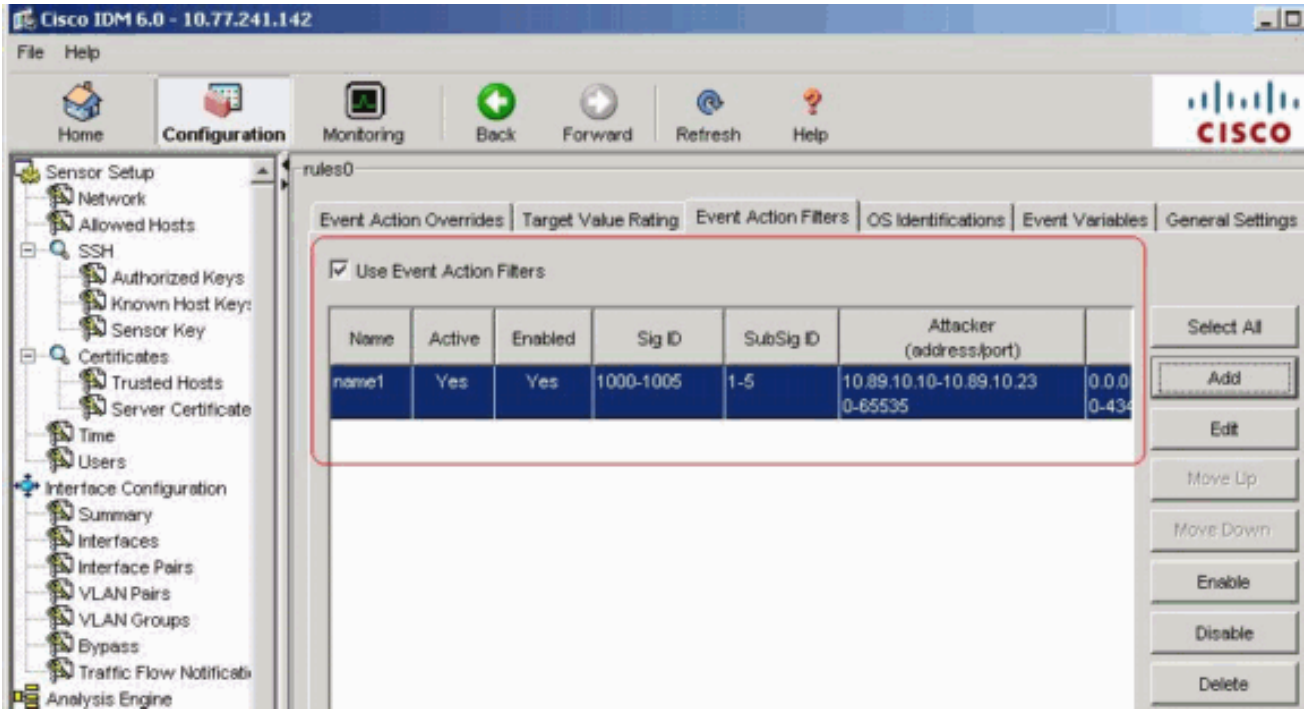
3. El tecleo **agrega** para agregar un filtro de la acción del evento.El cuadro de diálogo del filtro de la acción del evento del agregar aparece.
4. En el campo de nombre, ingrese un nombre como **name1** para el filtro de la acción del evento.Se suministra un nombre predeterminado, pero usted puede cambiarlo a un nombre más significativo.
5. En el campo activo, haga clic el **botón Yes Radio Button** para agregar este filtro a la lista de modo que tome el efecto sobre los eventos de filtración.
6. En el campo habilitado, haga clic el **botón Yes Radio Button** para habilitar el filtro.**Note**: Usted debe también marcar la casilla de verificación de los **filtros de la acción del evento del uso** en la lengueta de los filtros de la acción del evento o ningunos de los filtros de la acción del evento llegan a ser habilitados sin importar si usted marca la casilla de verificación del **sí** en el cuadro de diálogo del filtro de la acción del evento del agregar.
7. En el campo del ID de la firma, ingrese los ID de la firma de todas las firmas a las cuales este filtro deba ser aplicado.Usted puede utilizar una lista, por ejemplo, 1000, 1005, o un rango, por ejemplo, **1000-1005** o una de las variables SIG si usted las definió en el prefacio

de cuadro de las variables de evento la variable con $.

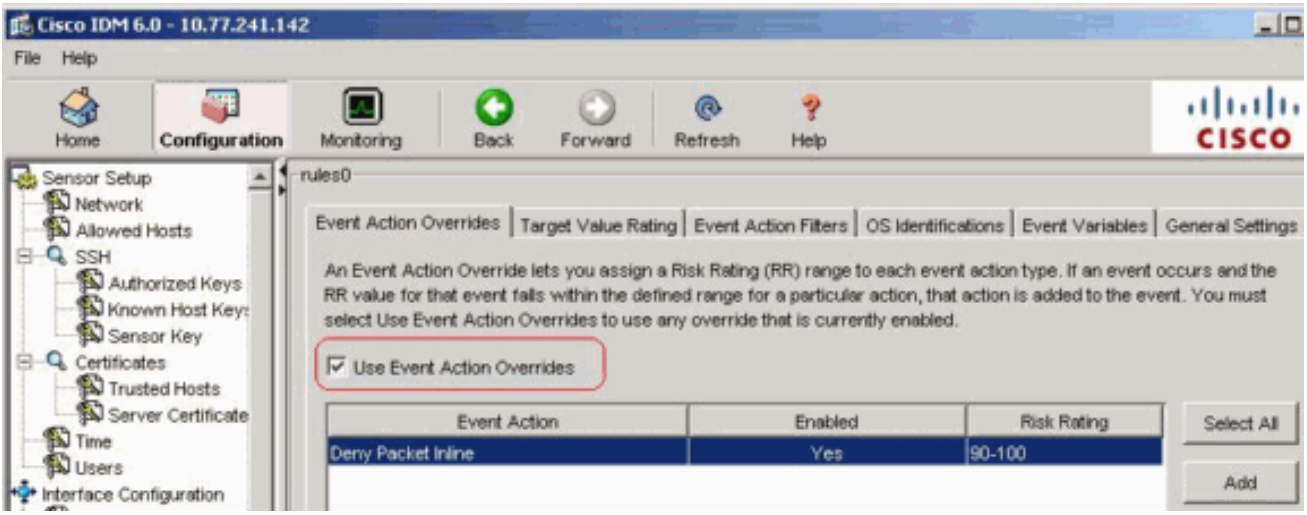
8. En el campo de SubSignature ID, ingrese el subsignature ID de los subsignatures a los cuales este filtro debe ser aplicado. Por ejemplo, **1-5**.
9. En el campo de dirección del atacante, ingrese el IP Address del host de origen.Usted puede utilizar una de las variables si usted las definió en el prefacio de cuadro de las variables de evento la variable con $. Usted puede también ingresar un rango de direcciones, por ejemplo, **10.89.10.10-10.89.10.23**. El valor por defecto es 0.0.0.0-255.255.255.255.
10. En el campo de puerto del atacante, ingrese el número del puerto usado por el atacante para enviar el paquete que ofende.
11. En el campo de dirección de la víctima, ingrese el IP Address del host receptor.Usted puede utilizar una de las variables si usted las definió en el prefacio de cuadro de las variables de evento la variable con $. Usted puede también ingresar un rango de direcciones, por ejemplo, **192.56.10.1-192.56.10.255**. El valor por defecto es 0.0.0.0-255.255.255.255.
12. En el campo de puerto de la víctima, ingrese el número del puerto usado por el host víctima para recibir el paquete que ofende. Por ejemplo, **0-434**.
13. En el campo del grado de riesgo, ingrese un rango RR para este filtro. Por ejemplo, **85-100**.Si el RR para un evento baja dentro del rango que usted especifica, el evento se procesa contra los criterios de este filtro.
14. De las acciones para restar la lista desplegable, elija las acciones que usted quisiera que este filtro quitara del evento. Por ejemplo, elija la **conexión TCP de la restauración**.**Consejo:** Mantenga la clave del **Ctrl** para elegir más de una acción del evento en la lista.
15. En la lista desplegable de la importancia OS, elija si usted quiere saber si la alerta es relevante al OS que se ha identificado para la víctima. Por ejemplo, elija **relevante**.
16. En el campo del porcentaje de la negación, ingrese el porcentaje de paquetes para negar para niegan las características del atacante. Por ejemplo, **90**.El valor por defecto es el 100 por ciento.
17. En la parada en el campo de la coincidencia, elija uno de estos botones de radio:**Sí** — Si usted quiere la acción del evento filtra el componente para parar el procesar después de que las acciones de este filtro determinado se quitenNinguna filtros que permanecen no se procesan; por lo tanto, ningunas acciones adicionales se pueden quitar del evento.**No** — Si usted quiere continuar procesando los filtros adicionales
18. En el campo de comentarios, ingrese los algunos comentarios que usted quiere salvar con este filtro, tal como el propósito de este filtro o porqué usted ha configurado este filtro de una manera determinada. Por ejemplo, **NUEVO FILTRO**.**Consejo:** Haga clic la **cancelación** para deshacer sus cambios y cerrar el cuadro de diálogo del filtro de la acción del evento del
agregar.



19. Click OK.El filtro de la acción del nuevo evento ahora aparece en la lista en la lengueta de los filtros de la acción del evento como se muestra.

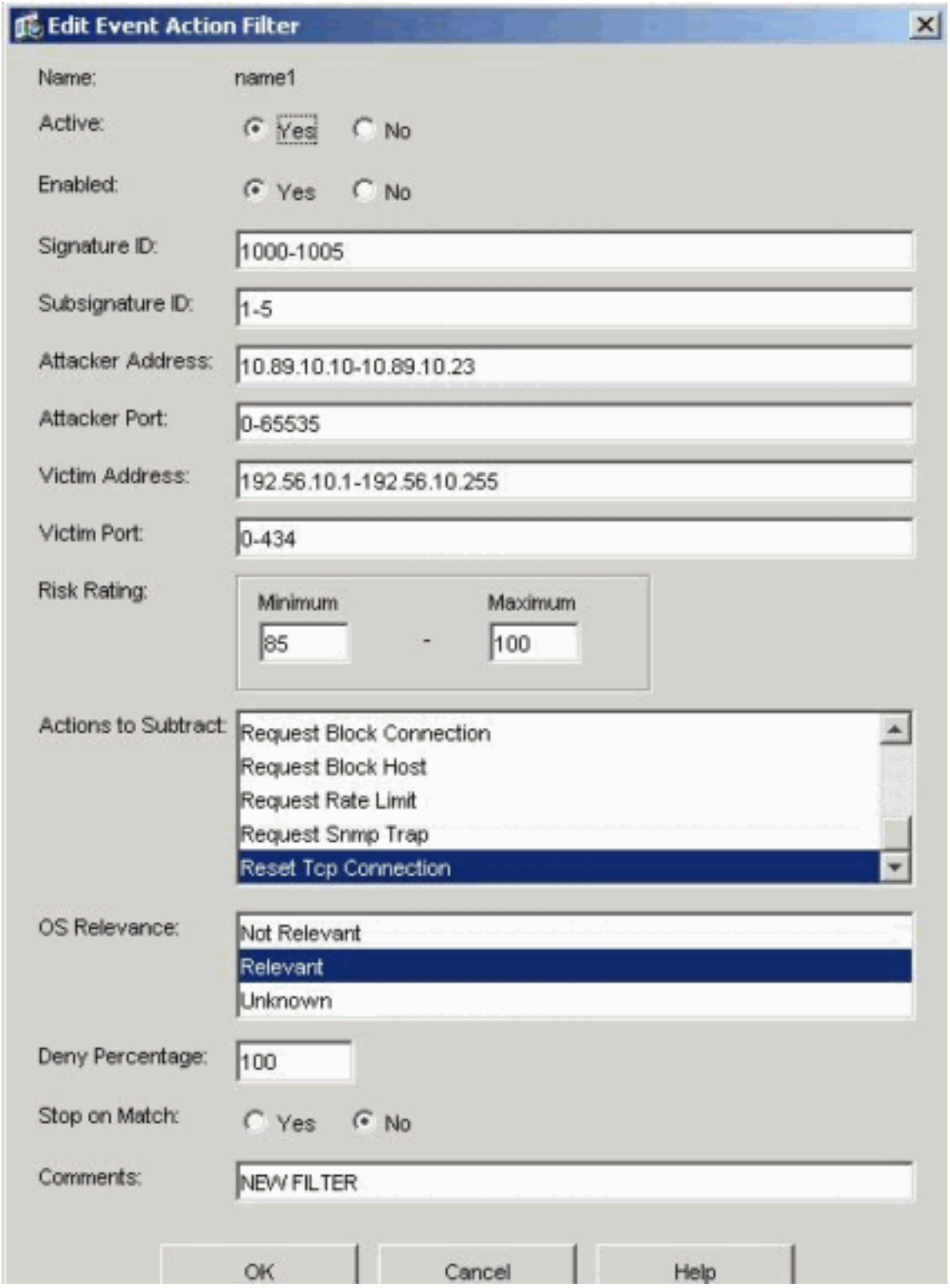


20. Marque la **acción del evento del uso reemplaza la** casilla de verificación como se muestra.



Note: Usted debe marcar la **acción del evento del uso reemplaza la** casilla de verificación en la acción del evento reemplaza la lengueta o ninguna de la acción del evento reemplaza llegado a ser habilitada sin importar el valor que usted fija en el cuadro de diálogo del filtro de la acción del evento del agregar.

21. Elija un filtro existente de la acción del evento en la lista para editarla, y después haga clic **editan**.El cuadro de diálogo del filtro de la acción del evento del editar



aparece.

22. Cambie cualquier valor en los campos que usted necesita alterar.Vea los pasos 4 a 18 para la información sobre cómo completar los campos.**Consejo:** Haga clic la **cancelación** para deshacer sus cambios y cerrar el cuadro de diálogo del filtro de la acción del evento del editar.
23. Click OK.El filtro editado de la acción del evento ahora aparece en la lista en la lengueta de los filtros de la acción del evento.
24. Marque la **acción del evento del uso reemplaza la** casilla de verificación.**Note**: Usted debe marcar la **acción del evento del uso reemplaza la** casilla de verificación en la acción del evento reemplaza la lengueta o ninguna de la acción del evento reemplaza se habilita sin importar el valor que usted fija en el cuadro de diálogo del filtro de la acción del evento del editar.
25. Elija un filtro de la acción del evento en la lista para borrarla, y después haga clic la

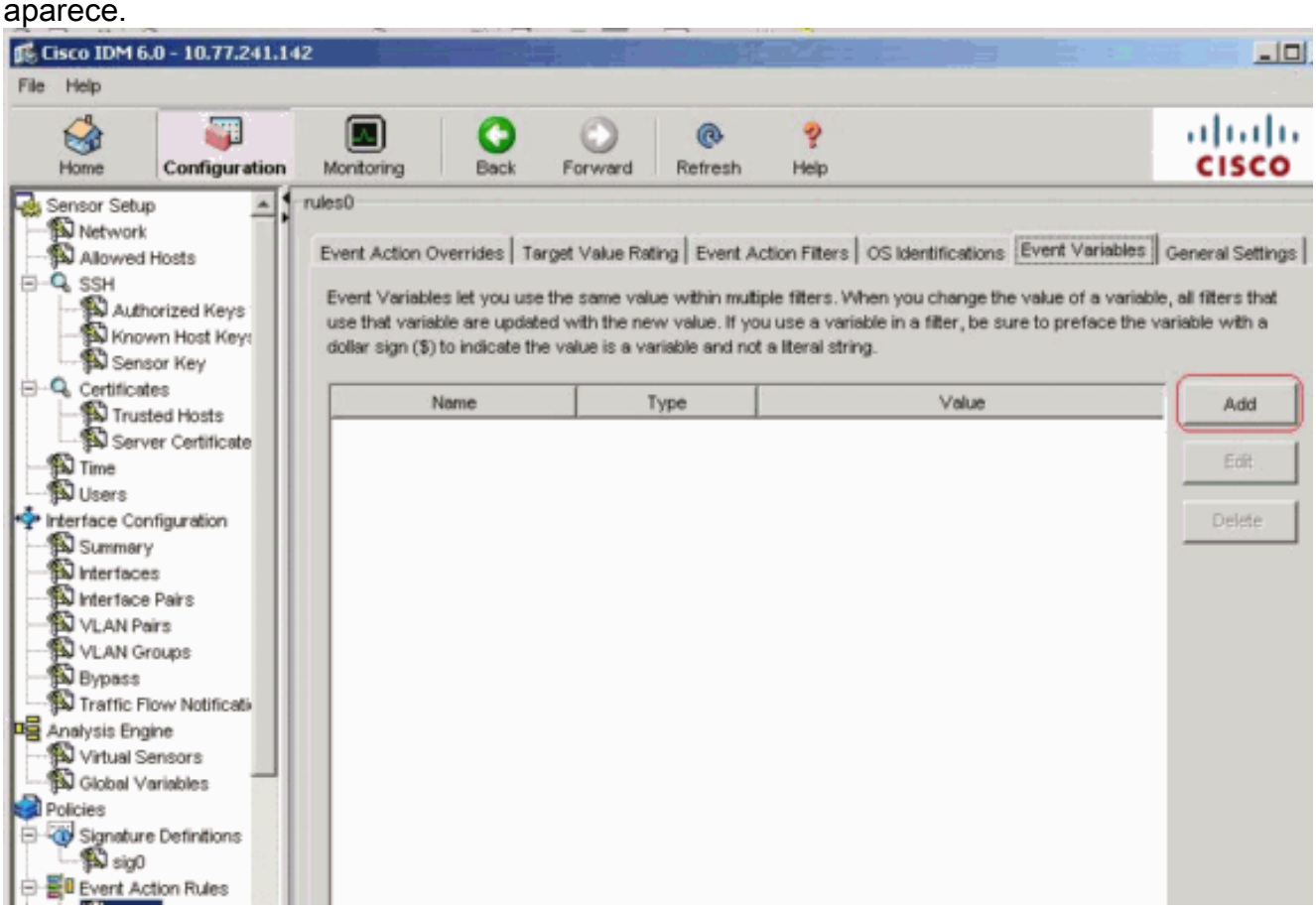
cancelación.El filtro de la acción del evento aparece no más en la lista en la lengueta de los filtros de la acción del evento.

26. Filtre hacia arriba o hacia abajo en la lista para mover una acción del evento, elíjala, y después haga clic **se levantan** o **se bajan**.**Consejo:** Tecleo **reajustado** para quitar sus cambios.
27. Haga clic **se aplican** para aplicar sus cambios y salvar la configuración revisada.

Configuración variable del evento

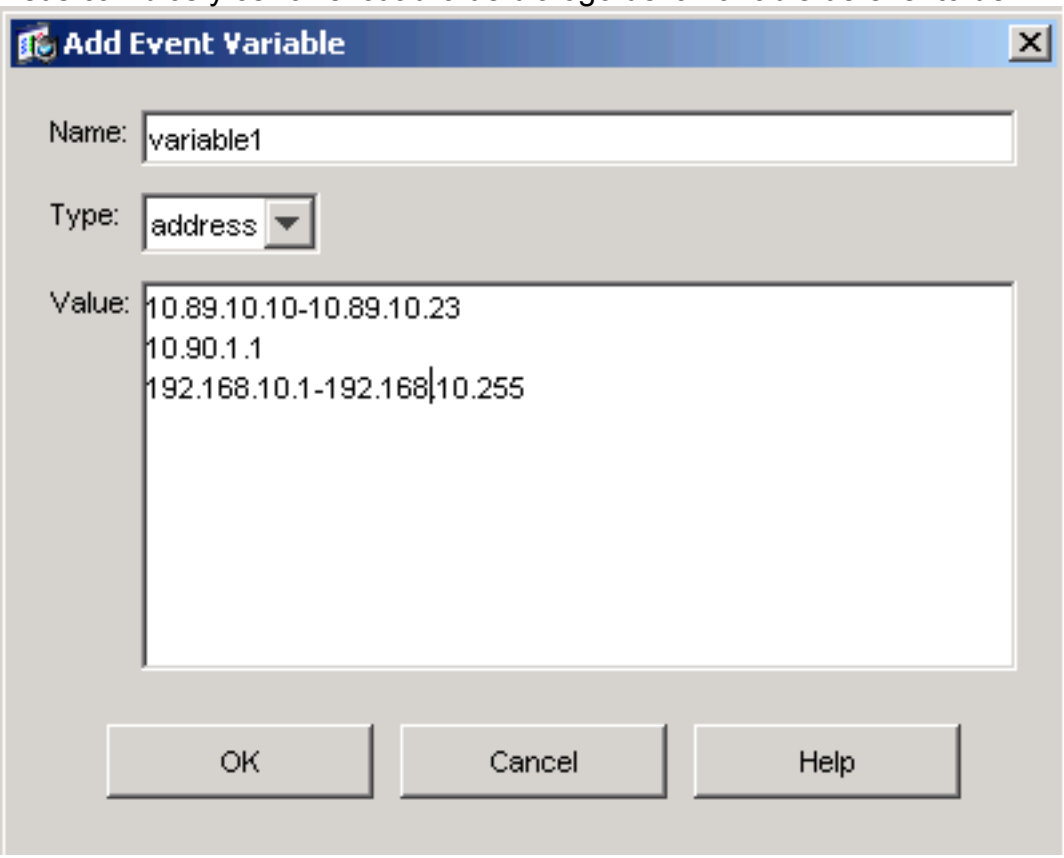
Complete estos pasos para agregar, editar, y borrar las variables de evento:

1. Login. Por ejemplo, utilice una cuenta con los privilegios del administrador o del operador.
2. Elija la **configuración > las directivas > las reglas de la acción del evento > rules0 > las variables de evento** si la versión de software es 6.x. Para la versión de software 5.x, elija las **reglas de la configuración > de la acción del evento > las variables de evento**.La lengueta de las variables de evento
   aparece.

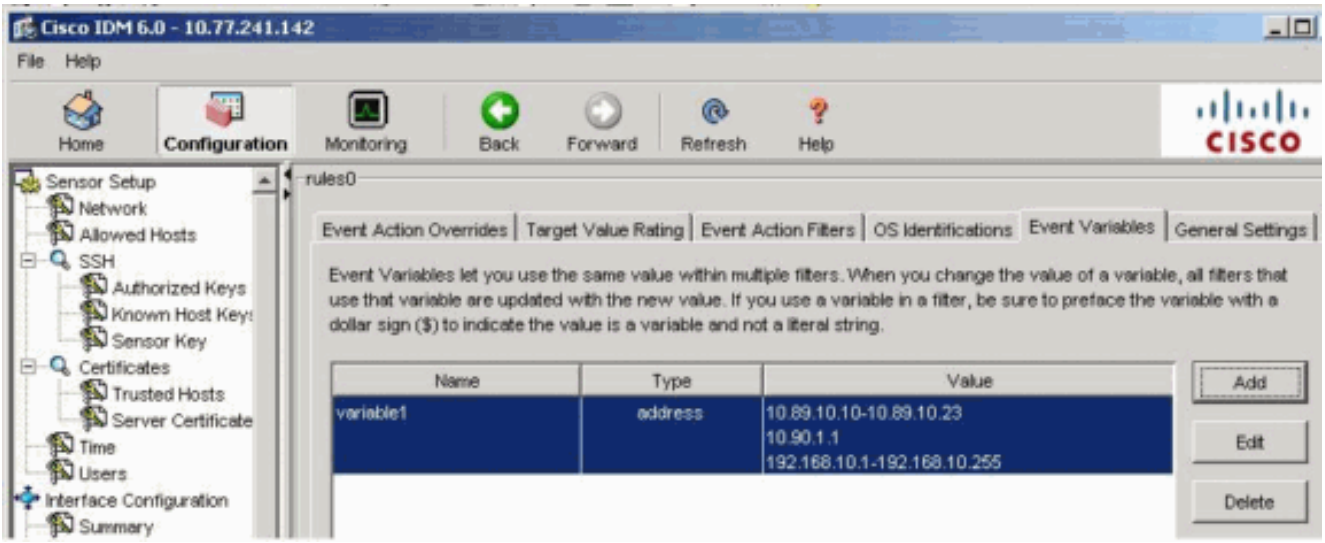


3. El tecleo **agrega** para crear una variable.El cuadro de diálogo variable del agregar aparece.
4. En el campo de nombre, ingrese un nombre para esta variable.**Note**: El nombre válido puede contener solamente los números o las cartas. Usted puede también utilizar un guión (-) o un caracter de subrayado (_).
5. En el campo de valor, ingrese los valores para esta variable.Especifique la dirección IP o los rangos o el conjunto completos de los rangos. Por ejemplo:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**Note**: Usted puede utilizar las comas como delimitadores. Aseegurese allí no son ningún espacio final después de la coma. Si no, usted recibe un mensaje de error `fallado validación`.**Consejo:** Haga clic la **cancelación** para

deshacer sus cambios y cerrar el cuadro de diálogo de la variable de evento del agregar.



6. Click OK.La nueva variable aparece en la lista en la lengueta de las variables de evento.



7. Elija la variable existente en la lista para editarla, y después haga clic **editan**.El cuadro de diálogo de la variable de evento del editar aparece.
8. En el campo de valor, ingrese sus cambios al valor.
9. Click OK.La variable de evento editada ahora aparece en la lista en la lengueta de las variables de evento.**Consejo:** Elija la **restauración** para quitar sus cambios.
10. El tecleo **se aplica** para aplicar sus cambios y salvar la configuración revisada.

Información Relacionada

- Página de soporte del Cisco Intrusion Prevention System
- Soporte Técnico y Documentación - Cisco Systems