IPS 5.x e mais tarde: Ajustando a assinatura com o filtro da ação do evento usando o CLI e o IDM

Índice

Introdução

Este documento descreve como ajustar a assinatura com o filtro da ação do evento no Sistema de prevenção de intrusões da Cisco (IPS) com o comando line interface(cli) e gerenciador de dispositivo ids (IDM).

Pré-requisitos

Requisitos

Este documento supõe que o ips Cisco está instalado e trabalha corretamente.

Componentes Utilizados

A informação neste documento é baseada no dispositivo do Cisco 4200 Series IDS/IPS que executa a versão de software 5.0 e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Filtros da ação do evento

Compreendendo filtros da ação do evento

Os filtros da ação do evento são processados enquanto uma lista requisitada e você podem mover filtros para cima ou para baixo na lista.

Os filtros deixaram o sensor executar determinadas ações em resposta ao evento sem exigir o sensor executar todas as ações ou remover o evento inteiro. Os filtros funcionam pela remoção das ações de um evento. Um filtro que remova todas as ações de um evento eficazmente consome o evento.

Note: Quando você filtra assinaturas da varredura, Cisco recomenda que você não filtra os endereços de destino. Se há uns endereços de destino múltiplo, simplesmente o último endereço está usado para combinar o filtro.

Você pode configurar filtros da ação do evento para remover as ações específicas de um evento ou para rejeitar um evento inteiro e para impedir o processamento adicional pelo sensor. Você pode usar as variáveis de ação do evento que você definiu aos endereços de grupo para seus filtros. Para o procedimento em como configurar variáveis de ação do evento, veja adicionar, editar, e suprimir da seção das variáveis de ação do evento.

Note: Você deve prefaciar a variável com um sinal de dólar ($) a fim indicar que você usa uma variável um pouco do que uma corda. Se não, você recebe a `fonte e o erro ruins do destino`.

Configuração de filtros da ação do evento usando o CLI

Termine estas etapas a fim configurar filtros da ação do evento:

1. Entre ao CLI com uma conta que tenha privilégios do administrado.
2. Incorpore o submode das regras da ação do evento:
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. Crie o nome do filtro:
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   Use **name1, name2**, e assim por diante a fim nomear seus filtros da ação do evento. Use o **começo | fim | inativo | antes | depois que** palavras-chaves a fim especificar onde você quer introduzir o filtro.
4. Especifique os valores para este filtro:Especifique a escala do ID de assinatura:
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   O padrão é 900 a 65535.Especifique a escala do subsignature ID:
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

   O padrão é 0 a 255.Especifique a escala de endereço do atacante:
   ```
   sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
   ```

O padrão é 0.0.0.0 a 255.255.255.255.Especifique a escala de endereço da vítima:
```
sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
```

O padrão é 0.0.0.0 a 255.255.255.255.Especifique o intervalo de porta da vítima:
```
sensor(config-eve-fil)#victim-port-range 0-434
```

O padrão é 0 a 65535.Especifique a importância do OS:
```
sensor(config-eve-fil)#os-relevance relevant
```

O padrão é 0 a 100.Especifique a escala da avaliação de risco.
```
sensor(config-eve-fil)#risk-rating-range 85-100
```

O padrão é 0 a 100.Especifique as ações para remover:
```
sensor(config-eve-fil)#actions-to-remove reset-tcp-connection
```

Se você filtra uma ação da negação, ajuste a porcentagem de negam ações que você quer:
```
sensor(config-eve-fil)#deny-attacker-percentage 90
```

O padrão é 100.Especifique o estado do filtro ao desabilitação ou ao permitido.
```
sensor(config-eve-fil)#filter-item-status {enabled | disabled}
```

O padrão é permitido.Especifique a parada no parâmetro do fósforo.
```
sensor(config-eve-fil)#stop-on-match {true | false}
```

Verdadeiro diz o sensor para parar de processar filtros se este artigo combina. Falso diz o sensor para continuar a processar filtros mesmo se este artigo combina.Adicionar qualquer comentários que você quer se usar a fim explicar este filtro:
```
sensor(config-eve-fil)#user-comment NEW FILTER
```

5. Verifique os ajustes para o 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. A fim editar um filtro existente:

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

7. Edite os parâmetros e veja as etapas 4a com 4l para mais informação.
8. A fim mover para cima ou para baixo um filtro na lista de filtro:

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

9. Verifique que você moveu os 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. A fim mover um filtro para a lista inativa:
```
    sensor(config-eve)#filters move name1 inactive
```

11. Verifique que o filtro se moveu para a lista inativa:
```
    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)#
```

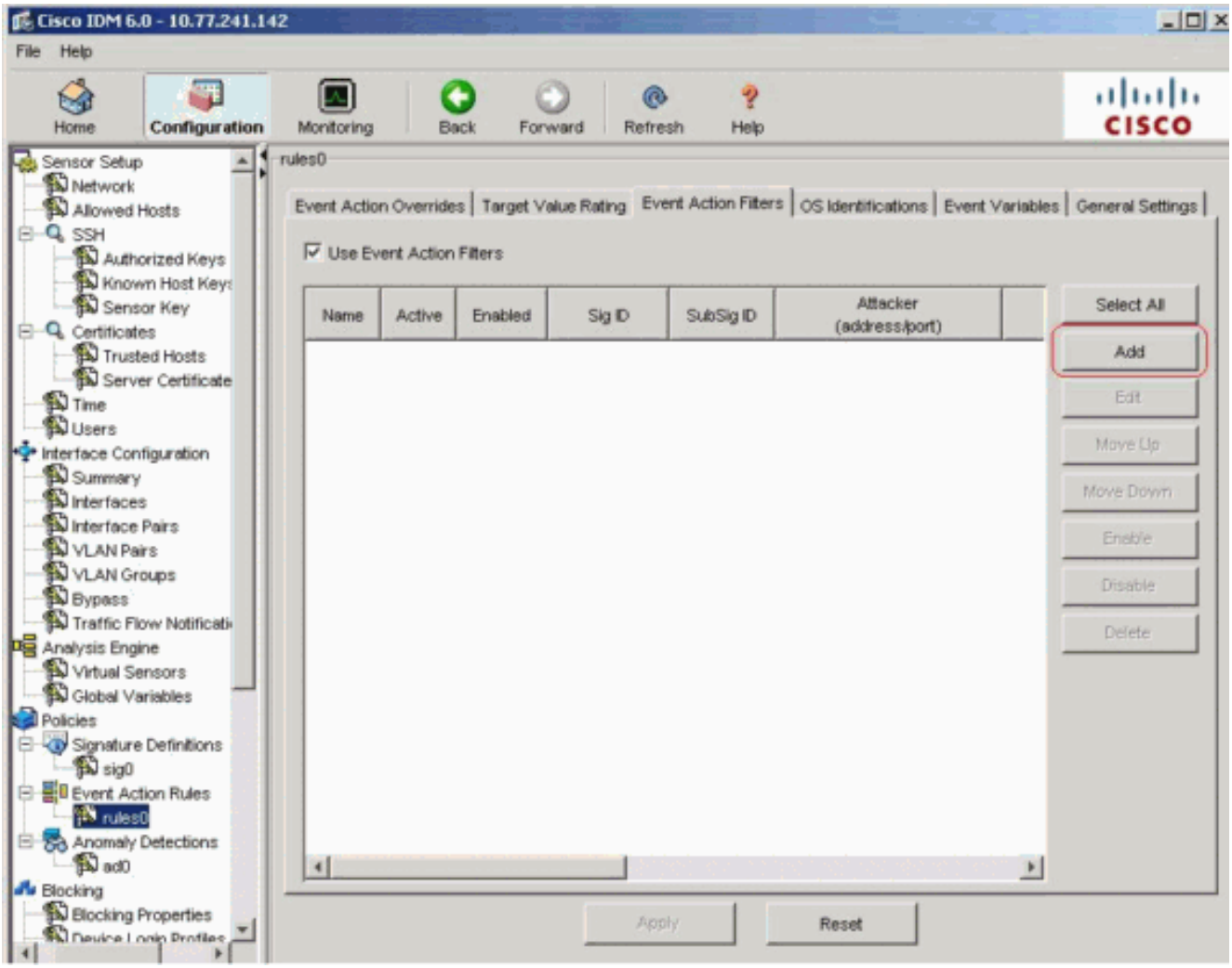
12. Retire o submode das regras da ação do evento:
```
    sensor(config-eve)#exit
    Apply Changes:?[yes]:
```

13. A imprensa **entra** a fim aplicar suas mudanças ou entrá-las **nenhum** a fim rejeitá-las.

Configuração de filtros da ação do evento usando o IDM

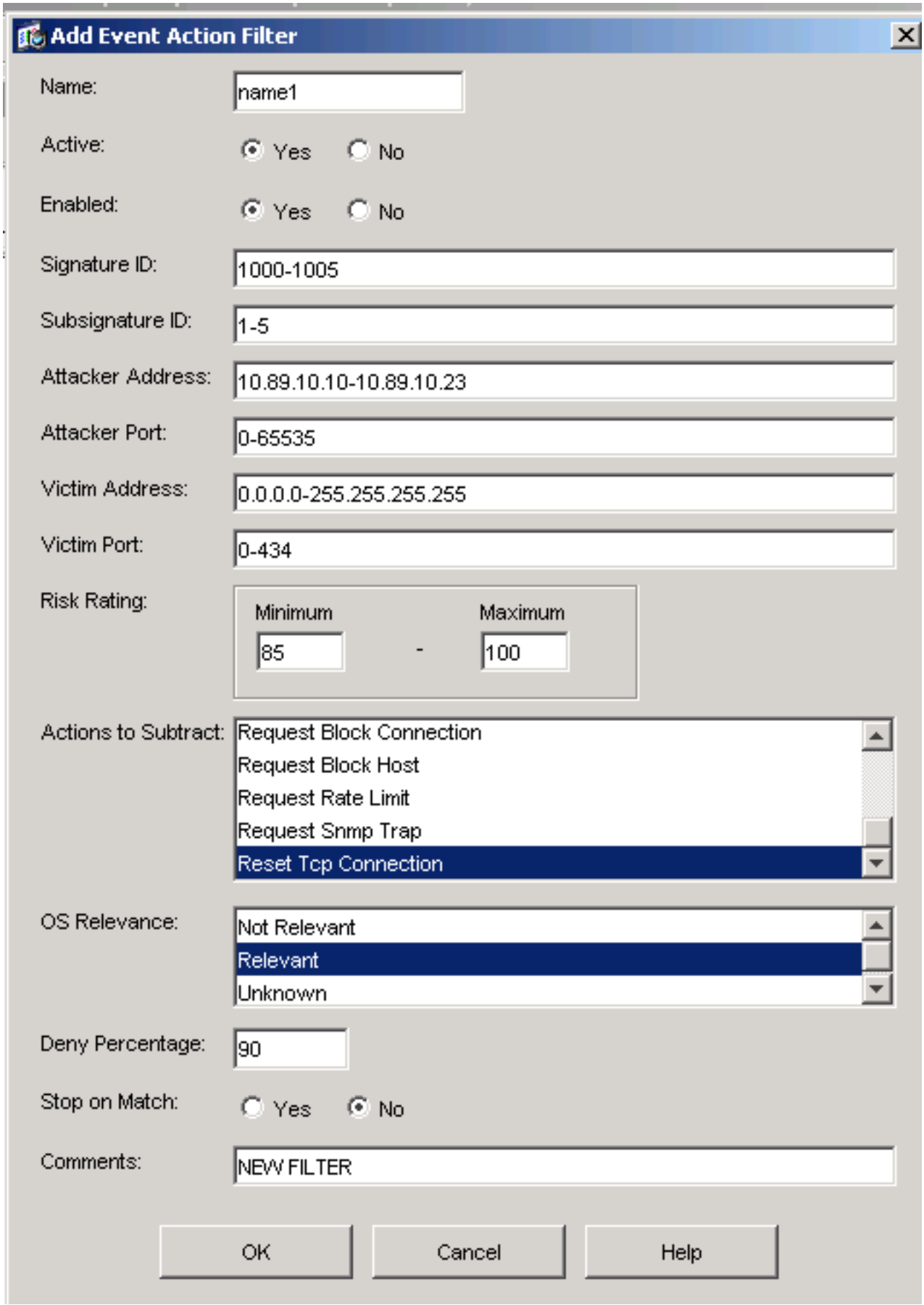
Termine estas etapas a fim adicionar, editar, suprimir, permitir, desabilitar, e mover de filtros da ação do evento:

1. Entre ao IDM com uma conta que tenha privilégios do administrador ou do operador.
2. Escolha a **configuração > as políticas > as regras da ação do evento > o rules0 > os filtros da ação do evento** se a versão de software é 6.x. Para a versão de software 5.x, escolha **filtros da ação das regras > do evento da configuração > da ação do evento.**A aba dos filtros da ação do evento aparece como
mostrado.

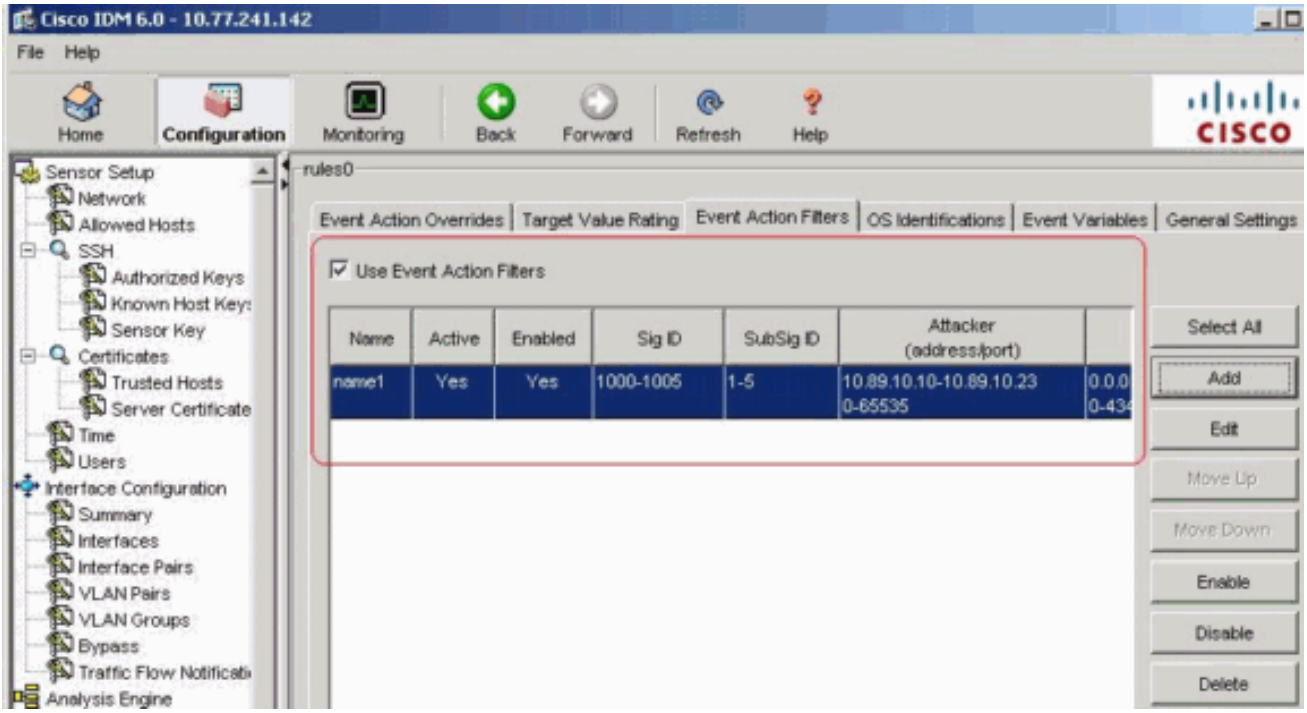


3. O clique **adiciona** a fim adicionar um filtro da ação do evento.A caixa de diálogo do filtro da ação do evento adicionar aparece.
4. No campo de nome, dê entrada com um nome como **name1** para o filtro da ação do evento.Um nome padrão é fornecido, mas você pode mudá-lo a um nome mais significativo.
5. No campo ativo, clique o **botão Yes Radio Button** a fim adicionar este filtro à lista de modo que tome o efeito em eventos de filtração.
6. No campo permitido, clique o **botão Yes Radio Button** a fim permitir o filtro.**Note**: Você deve igualmente verificar a caixa de verificação dos **filtros da ação do evento do uso na** aba dos filtros da ação do evento ou nenhuns dos filtros da ação do evento tornam-se permitidos apesar de se você verifica a caixa de verificação do **Yes na** caixa de diálogo do filtro da ação do evento adicionar.
7. No campo do ID de assinatura, entre na assinatura ID de todas as assinaturas a que este filtro deve ser aplicado.Você pode usar uma lista, por exemplo, 1000, 1005, ou uma escala, por exemplo, **1000-1005** ou uma das variáveis SIG se você as definiu na aba das variáveis de evento. Prefácio a variável com $.
8. No campo de SubSignature ID, entre no subsignature ID dos subsignatures a que este filtro deve ser aplicado. Por exemplo, **1-5**.

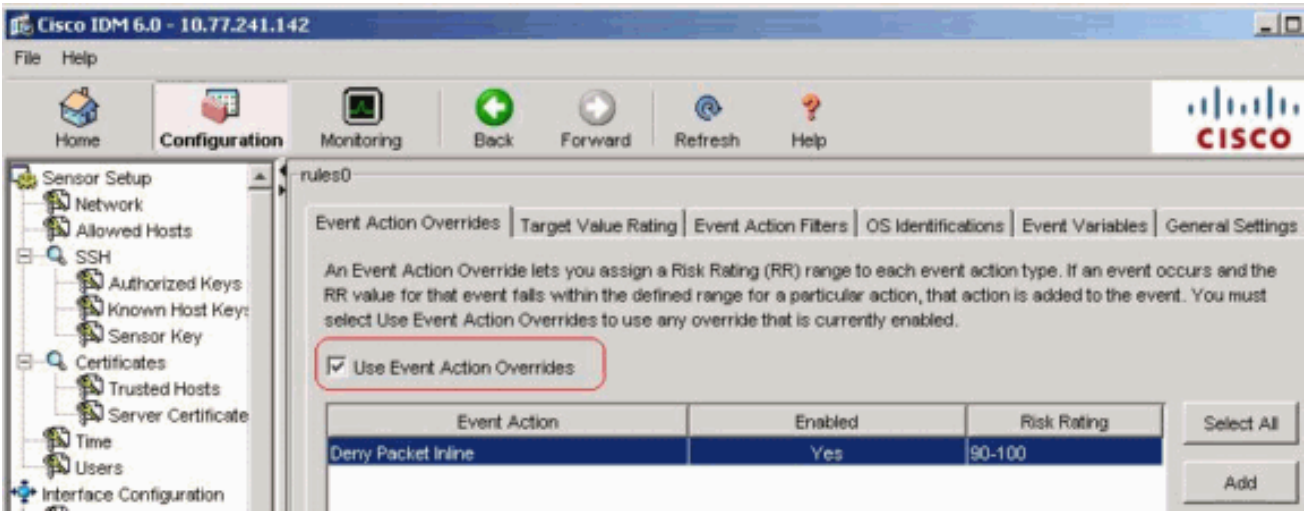
9. No campo de endereço do atacante, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do host de origem.Você pode usar uma das variáveis se você as definiu na aba das variáveis de evento. Prefácio a variável com $. Você pode igualmente incorporar um intervalo de endereço, por exemplo, **10.89.10.10-10.89.10.23**. O padrão é 0.0.0.0-255.255.255.255.
10. No campo de porta do atacante, entre no número de porta usado pelo atacante a fim enviar o pacote de ofensa.
11. No campo de endereço da vítima, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do host destinatário.Você pode usar uma das variáveis se você as definiu na aba das variáveis de evento. Prefácio a variável com $. Você pode igualmente incorporar um intervalo de endereço, por exemplo, **192.56.10.1-192.56.10.255**. O padrão é 0.0.0.0-255.255.255.255.
12. No campo de porta da vítima, entre no número de porta usado pelo host de vítima a fim receber o pacote de ofensa. Por exemplo, **0-434**.
13. No campo da avaliação de risco, incorpore uma escala RR para este filtro. Por exemplo, **85-100**.Se o RR para um evento cai dentro da escala que você especifica, o evento é processado contra os critérios deste filtro.
14. Das ações para subtrair a lista de drop-down, escolha as ações que você quer este filtro remover do evento. Por exemplo, escolha a **conexão de TCP da restauração**.**Tip**: Mantenha a chave **CTRL** a fim escolher mais de uma ação do evento na lista.
15. Na lista de drop-down da importância do OS, escolha se você quer saber se o alerta é relevante ao OS que esteve identificado para a vítima. Por exemplo, escolha **relevante**.
16. No campo da porcentagem da negação, incorpore o porcentagem de pacotes a fim negar para negam características do atacante. Por exemplo, **90**.O padrão é 100 por cento.
17. Na parada no campo do fósforo, escolha um destes botões de rádio:**Sim** — Se você quer a ação do evento filtra o componente para parar de processar depois que as ações deste filtro particular são removidasNenhuns filtros que permanecem não são processados; consequentemente, nenhuma ação adicional pode ser removida do evento.**Não** — Se você quer continuar a processar filtros adicionais
18. No campo de comentários, entre nos qualquer comentários que você quer armazenar com este filtro, tal como a finalidade deste filtro ou em porque você configurou este filtro em uma maneira particular. Por exemplo, **FILTRO NOVO**.**Tip**: Clique o **cancelamento** a fim desabotoar suas mudanças e fechar a caixa de diálogo do filtro da ação do evento adicionar.



19. Click **OK**.O filtro novo da ação do evento aparece agora na lista na aba dos filtros da ação do evento como
mostrado.

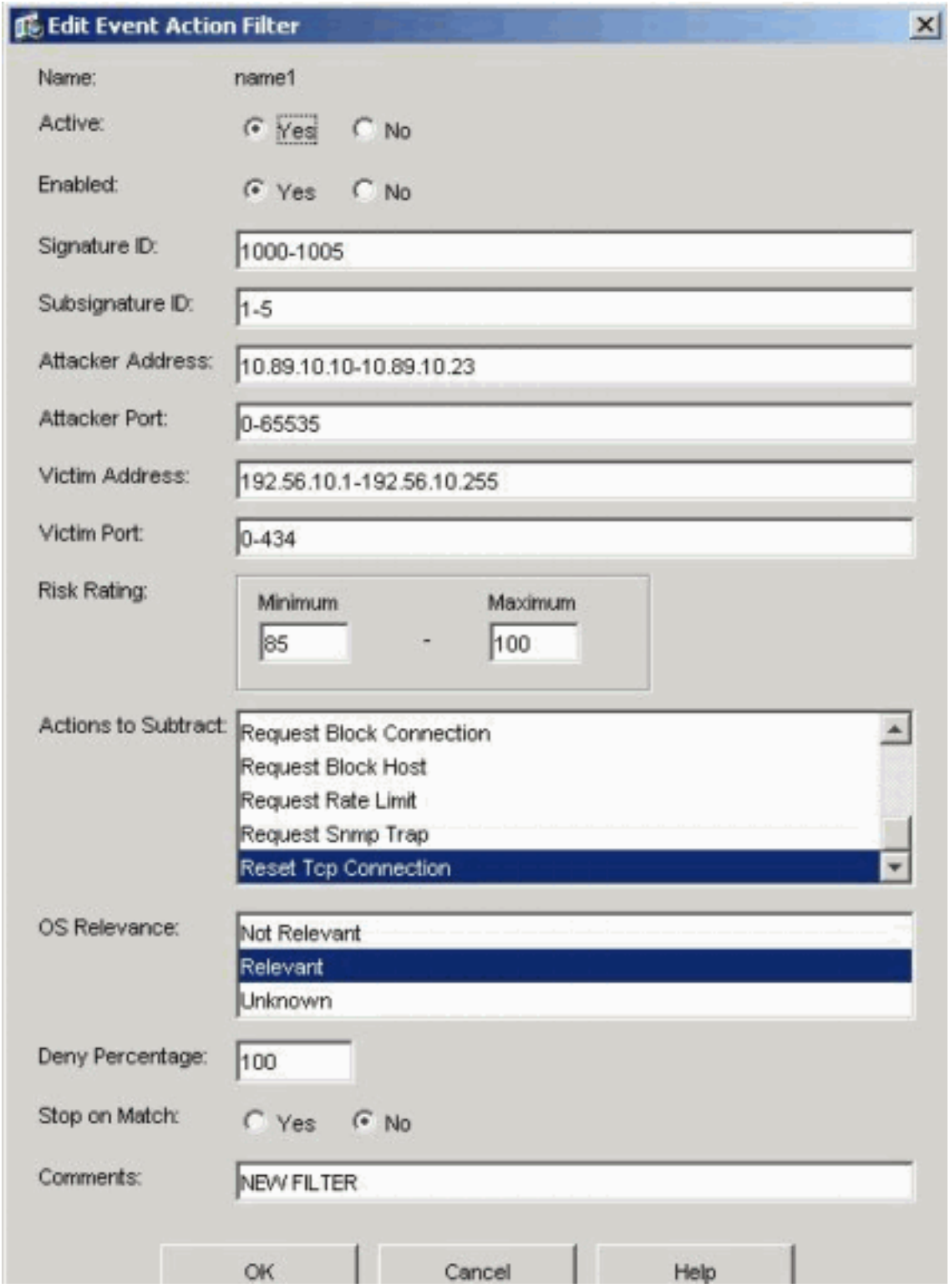


20. Verifique a **ação do evento do uso cancela a** caixa de verificação como mostrado.



Note: Você deve verificar a **ação do evento do uso cancela a** caixa de verificação na ação do evento cancela a aba ou nenhuma da ação do evento cancela tornado permitida apesar do valor que você se ajusta na caixa de diálogo do filtro da ação do evento adicionar.

21. Escolha um filtro existente da ação do evento na lista a fim editá-la, e clique-o então **editam**.A caixa de diálogo do filtro da ação do evento da edição



aparece.

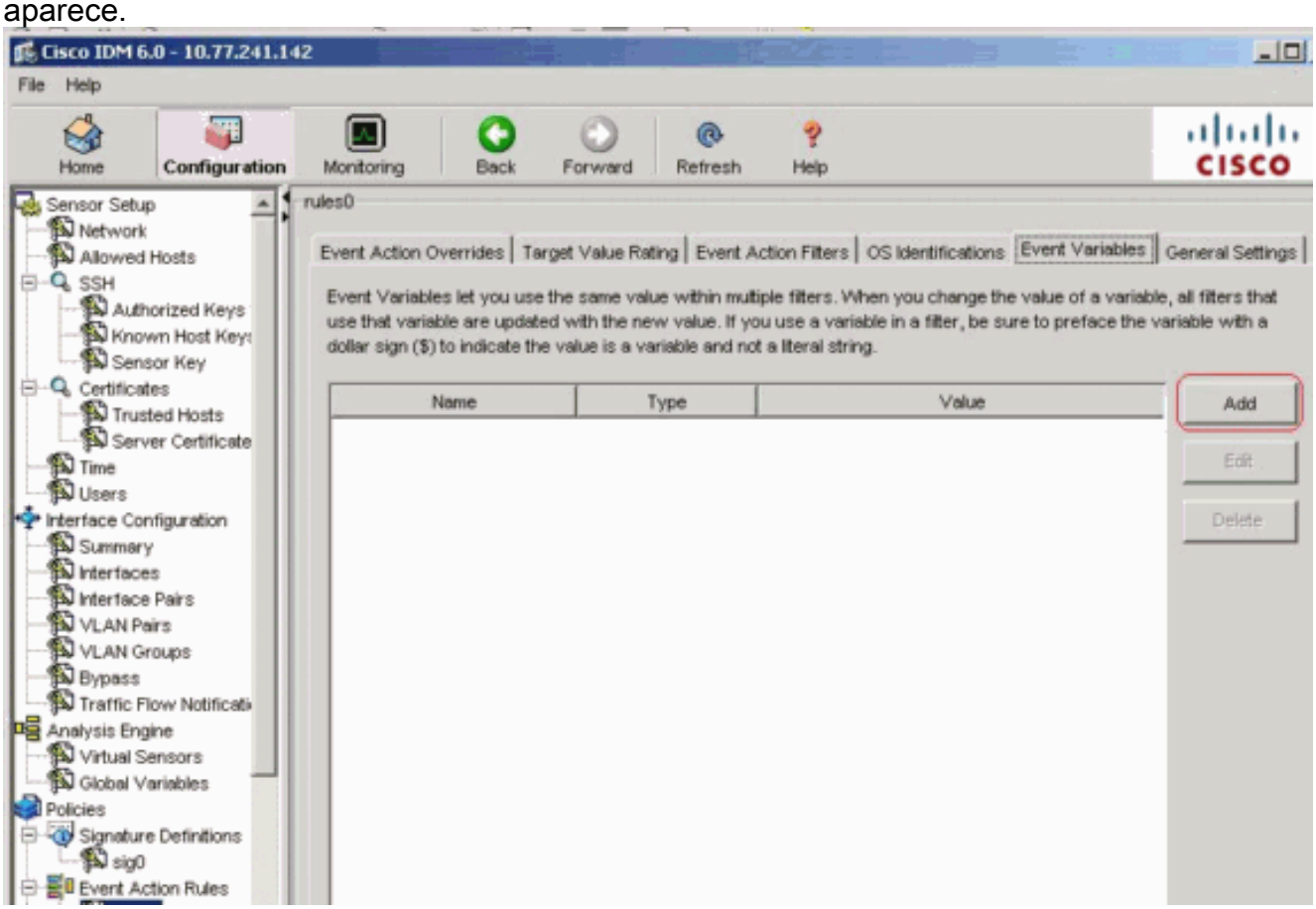
22. Mude todos os valores nos campos que você precisa de alterar.Veja etapas 4 a 18 para obter informações sobre de como terminar os campos.**Tip**: Clique o **cancelamento** a fim desabotoar suas mudanças e fechar a caixa de diálogo do filtro da ação do evento da edição.
23. Click **OK**.O filtro editado da ação do evento aparece agora na lista na aba dos filtros da ação do evento.
24. Verifique a **ação do evento do uso cancela a** caixa de verificação.**Note**: Você deve verificar a **ação do evento do uso cancela a** caixa de verificação na ação do evento cancela a aba ou nenhuma da ação do evento cancela é permitida apesar do valor que você se ajusta na caixa de diálogo do filtro da ação do evento da edição.
25. Escolha um filtro da ação do evento na lista a fim suprimir d, e clique então a **supressão**.O filtro da ação do evento já não aparece na lista na aba dos filtros da ação do evento.

26. Filtre para cima ou para baixo na lista a fim mover uma ação do evento, escolha-a, e clique-a então **movem** ou **abaixam**.**Tip**: Clique **restaurado** a fim remover suas mudanças.
27. Clique **aplicam-se** a fim aplicar suas mudanças e salvar a configuração revisada.

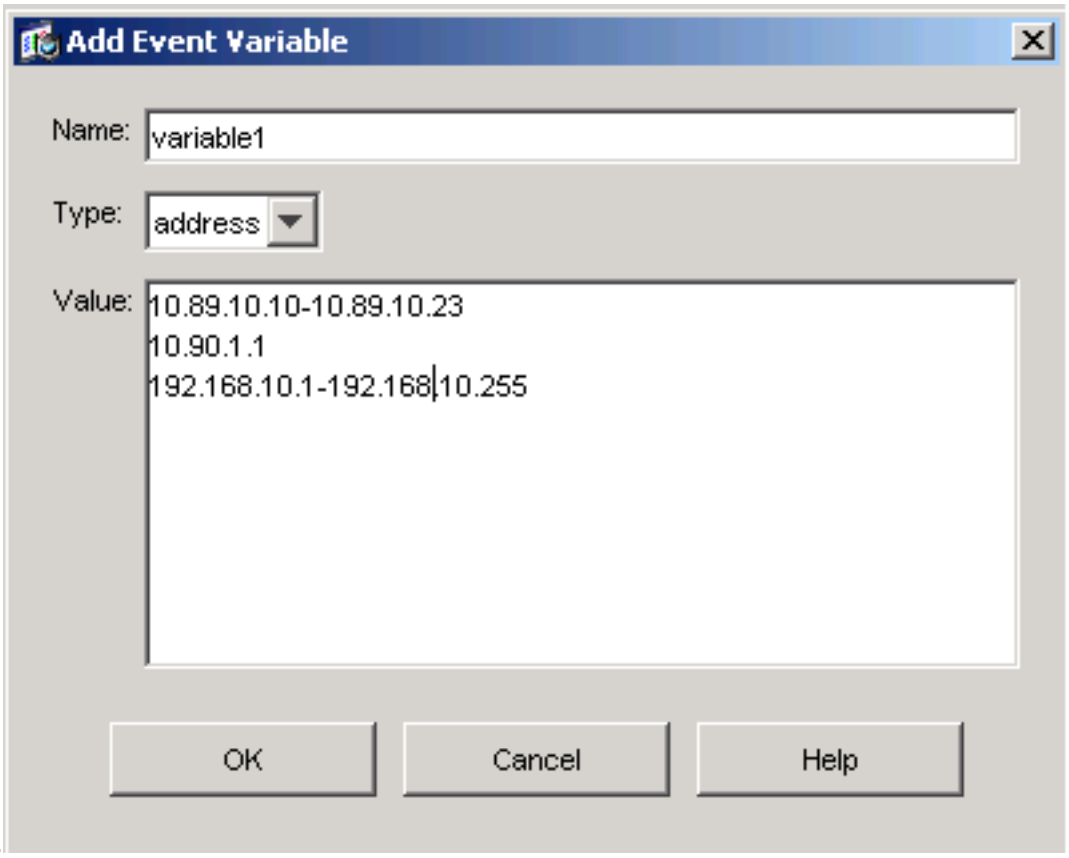
Configuração variável do evento

Termine estas etapas a fim adicionar, editar, e suprimir de variáveis de evento:

1. Início de uma sessão. Por exemplo, use uma conta com privilégios do administrador ou do operador.
2. Escolha a **configuração > as políticas > as regras da ação do evento > o rules0 > as variáveis de evento** se a versão de software é 6.x. Para a versão de software 5.x, escolha **regras da configuração > da ação do evento > variáveis de evento**.A aba das variáveis de evento
   aparece.

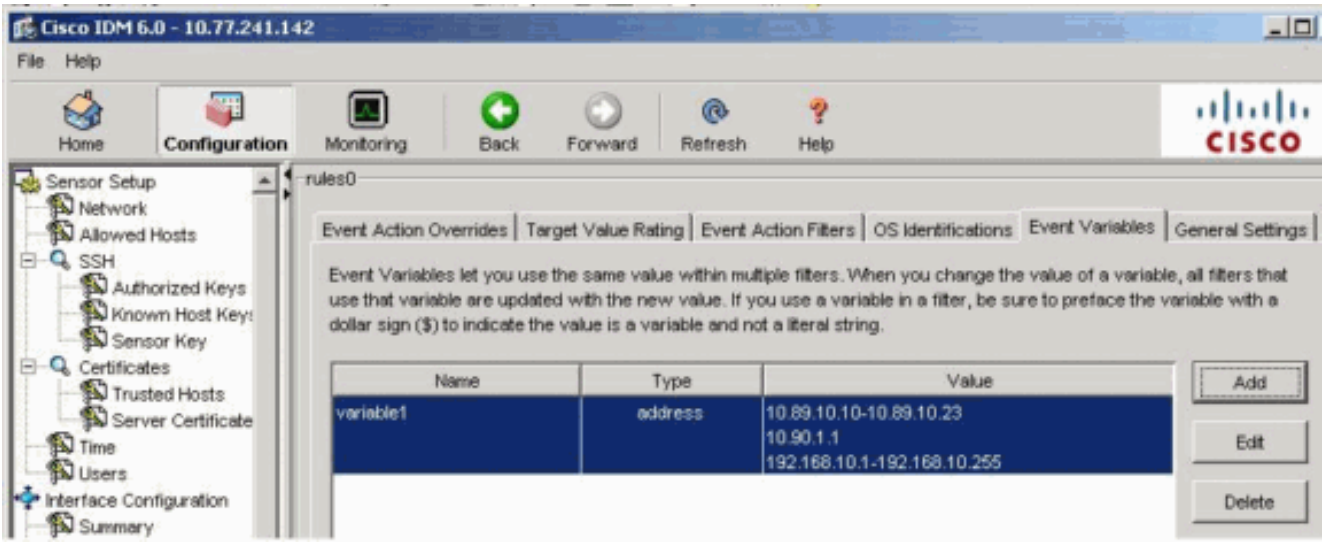


3. O clique **adiciona** a fim criar uma variável.A caixa de diálogo variável adicionar aparece.
4. No campo de nome, dê entrada com um nome para esta variável.**Note**: O nome válido pode somente conter números ou letras. Você pode igualmente usar um hífen (-) ou um relevo (_).
5. No campo de valor, incorpore os valores para esta variável.Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT ou as escalas ou o grupo completo de escalas. Por exemplo:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**Note**: Você pode usar vírgulas como delimitadores. Certifique-se que não há nenhum espaço de trailing após a vírgula. Se não, você recebe um Mensagem de Erro `falhado validação`.**Tip**: Clique o **cancelamento** a fim desabotoar suas mudanças e fechar a caixa de diálogo da variável de



evento adicionar.

6. Click **OK**.A variável nova aparece na lista na aba das variáveis de evento.



7. Escolha a variável existente na lista a fim editá-la, e clique-a então **editam**.A caixa de diálogo da variável de evento da edição aparece.
8. No campo de valor, incorpore suas mudanças ao valor.
9. Click **OK**.A variável de evento editada aparece agora na lista na aba das variáveis de evento.**Tip**: Escolha a **restauração** a fim remover suas mudanças.
10. O clique **aplica-se** a fim aplicar suas mudanças e salvar a configuração revisada.

Informações Relacionadas

- Página de suporte do Sistema de prevenção de intrusões da Cisco
- Suporte Técnico e Documentação - Cisco Systems