IPS 5.x e versioni successive: Tuning della firma con il filtro azioni evento tramite CLI e IDM

Sommario

Introduzione

In questo documento viene descritto come ottimizzare la firma con il filtro azioni per eventi di Cisco Intrusion Prevention System (IPS) con l'interfaccia della riga di comando (CLI) e IDS Device Manager (IDM).

Prerequisiti

Requisiti

in questo documento si presume che Cisco IPS sia installato e funzioni correttamente.

Componenti usati

Per la stesura del documento, è stato usato un dispositivo Cisco serie 4200 IDS/IPS con software versione 5.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

nei suggerimenti tecnici.

Filtri azioni eventi

Informazioni sui filtri per le azioni degli eventi

I filtri delle azioni evento vengono elaborati come un elenco ordinato ed è possibile spostare i filtri verso l'alto o verso il basso nell'elenco.

I filtri consentono al sensore di eseguire determinate azioni in risposta all'evento senza richiedere l'esecuzione di tutte le azioni o la rimozione dell'intero evento. I filtri funzionano tramite la rimozione di azioni da un evento. Un filtro che rimuove tutte le azioni da un evento utilizza l'evento in modo efficiente.

Nota: quando si filtrano le firme di ridimensionamento, Cisco consiglia di non filtrare gli indirizzi di destinazione. Se sono presenti più indirizzi di destinazione, per la corrispondenza al filtro verrà utilizzato solo l'ultimo indirizzo.

Èpossibile configurare i filtri delle azioni evento per rimuovere azioni specifiche da un evento o per eliminare un intero evento e impedire l'ulteriore elaborazione da parte del sensore. È possibile utilizzare le variabili di azione evento definite per raggruppare gli indirizzi dei filtri. Per la procedura relativa alla configurazione delle variabili di azione degli eventi, vedere la sezione Aggiunta, modifica ed eliminazione di variabili di azione degli eventi.

Nota: è necessario anteporre alla variabile un segno di dollaro ($) per indicare che si utilizza una variabile anziché una stringa. In caso contrario, viene visualizzato l'`errore Origine e destinazione non valide`.

Event Action Filtra la configurazione tramite CLI

Completare questa procedura per configurare i filtri azioni evento:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Immettere la modalità secondaria delle regole di azione evento:
   ```
   sensor#configure terminal
   sensor(config)#service event-action-rules rules1
   sensor(config-eve)#
   ```
3. Creare il nome del filtro:
   ```
   sensor(config-eve)#filters insert name1 begin
   ```

   Utilizzare **name1, name2** e così via per assegnare un nome ai filtri azioni evento. Utilizzare il pulsante **Inizia | fine | inattivo | prima | dopo** le parole chiave per specificare dove inserire il filtro.
4. Specificare i valori per il filtro:Specificare l'intervallo di ID firma:
   ```
   sensor(config-eve-fil)#signature-id-range 1000-1005
   ```

   Il valore predefinito è compreso tra 900 e 65535.Specificare l'intervallo di ID della firma secondaria:
   ```
   sensor(config-eve-fil)#subsignature-id-range 1-5
   ```

   Il valore predefinito è compreso tra 0 e 255.Specificare l'intervallo di indirizzi dell'autore

dell'attacco:

```
sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23
```

Il valore predefinito è compreso tra 0.0.0.0 e 255.255.255.255.Specificare l'intervallo di indirizzi della vittima:

```
sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255
```

Il valore predefinito è compreso tra 0.0.0.0 e 255.255.255.255.Specificare l'intervallo di porte vittima:

```
sensor(config-eve-fil)#victim-port-range 0-434
```

Il valore predefinito è compreso tra 0 e 65535.Specificare la pertinenza del sistema operativo:

```
sensor(config-eve-fil)#os-relevance relevant
```

Il valore predefinito è compreso tra 0 e 100.Specificare l'intervallo di valutazione del rischio.

```
sensor(config-eve-fil)#risk-rating-range 85-100
```

Il valore predefinito è compreso tra 0 e 100.Specificare le azioni da rimuovere:

```
sensor(config-eve-fil)#actions-to-remove reset-tcp-connection
```

Se si filtra un'azione di negazione, impostare la percentuale di azioni di negazione desiderata:

```
sensor(config-eve-fil)#deny-attacker-percentage 90
```

Il valore predefinito è 100.Specificare lo stato del filtro da disabilitare o abilitare.

```
sensor(config-eve-fil)#filter-item-status {enabled | disabled}
```

L'impostazione predefinita è attivata.Specificare il parametro stop on match.

```
sensor(config-eve-fil)#stop-on-match {true | false}
```

True indica al sensore di interrompere l'elaborazione dei filtri se l'elemento corrisponde. **False** indica al sensore di continuare a elaborare i filtri anche se l'elemento corrisponde.Aggiungere i commenti che si desidera utilizzare per spiegare questo filtro:

```
sensor(config-eve-fil)#user-comment NEW FILTER
```

5. Verificare le impostazioni del 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. Per modificare un filtro esistente:

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

7. Modificare i parametri e vedere i passaggi da 4a a 4l per ulteriori informazioni.
8. Per spostare un filtro verso l'alto o verso il basso nell'elenco dei filtri:

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

9. Verificare di aver spostato i filtri:

```
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. Per spostare un filtro nell'elenco degli elementi inattivi:

```
sensor(config-eve)#filters move name1 inactive
```

11. Verificare che il filtro sia stato spostato nell'elenco dei filtri inattivi:

```
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. Uscire dalla modalità secondaria delle regole di azione evento:

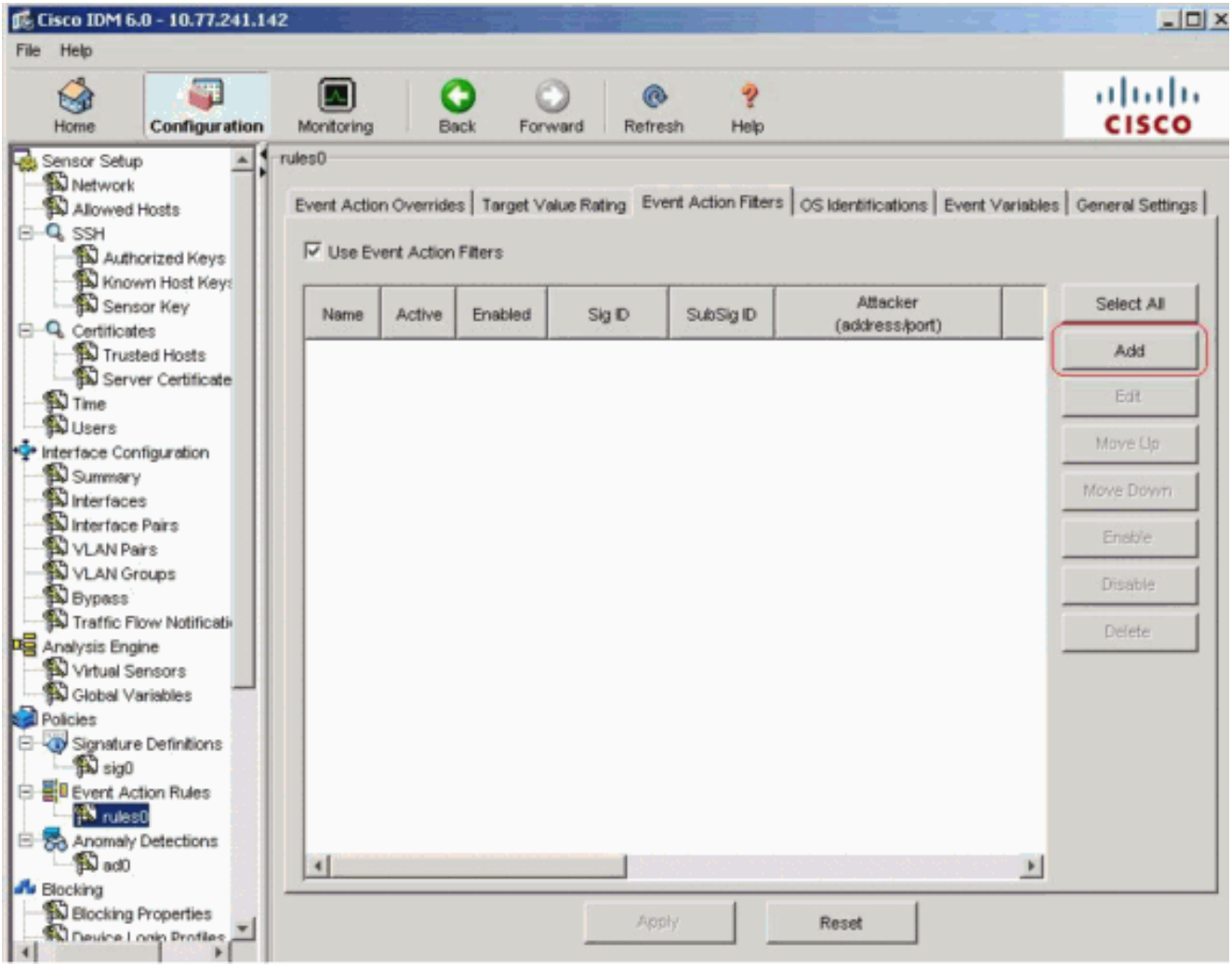
```
sensor(config-eve)#exit
Apply Changes:?[yes]:
```

13. Premere **Invio** per applicare le modifiche o immettere **no** per ignorarle.

Configurazione dei filtri per le azioni degli eventi tramite IDM

Completare questa procedura per aggiungere, modificare, eliminare, abilitare, disabilitare e spostare i filtri azioni evento:

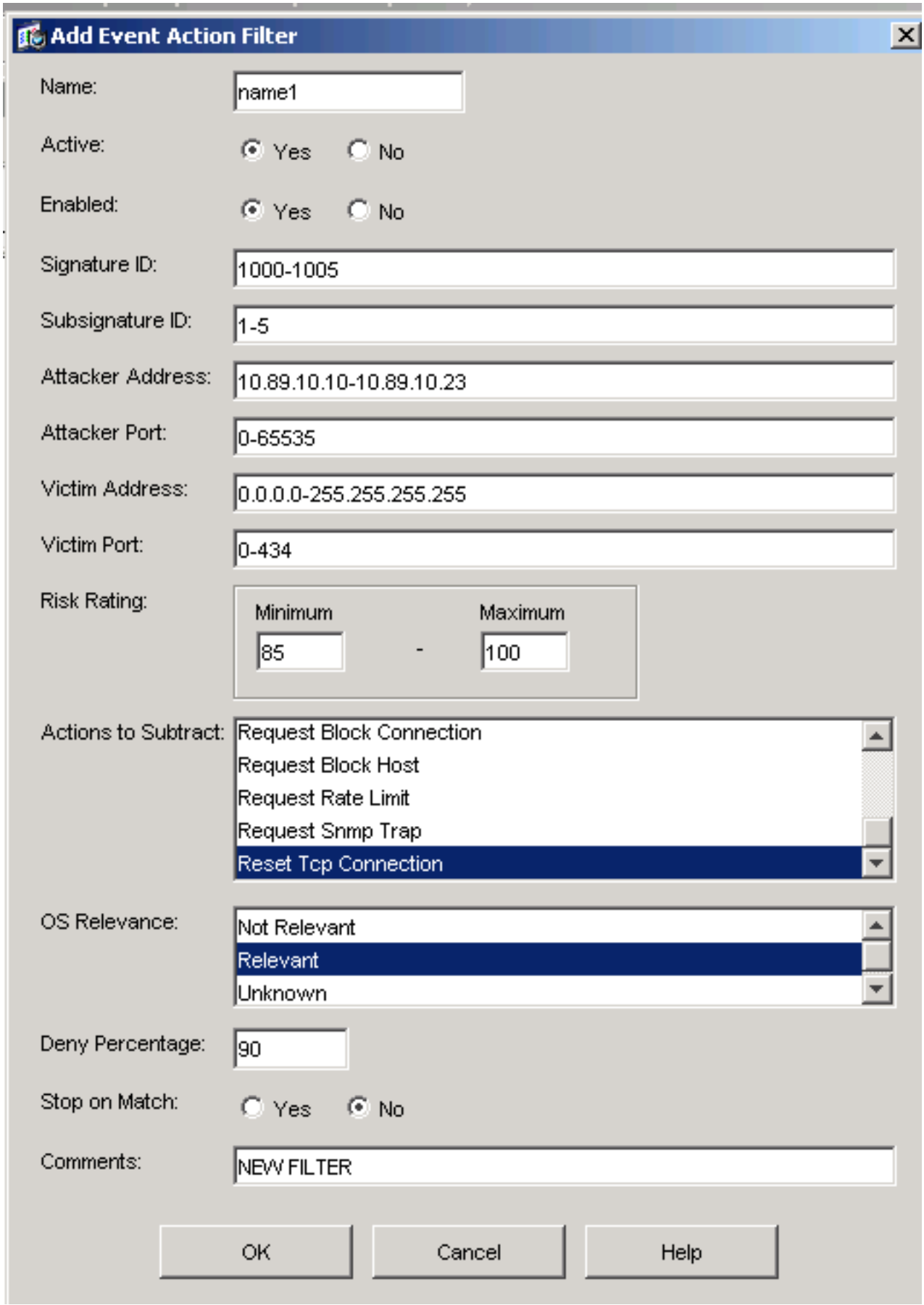
1. Accedere a IDM con un account che disponga di privilegi di amministratore o di operatore.
2. Scegliere **Configurazione > Criteri > Regole d'azione evento > regole0 > Filtri azioni evento** se la versione software è 6.x. Per la versione software 5.x, scegliere **Configurazione > Regole d'azione evento > Filtri azione evento.**La scheda Filtri azioni eventi viene visualizzata come
illustrato.



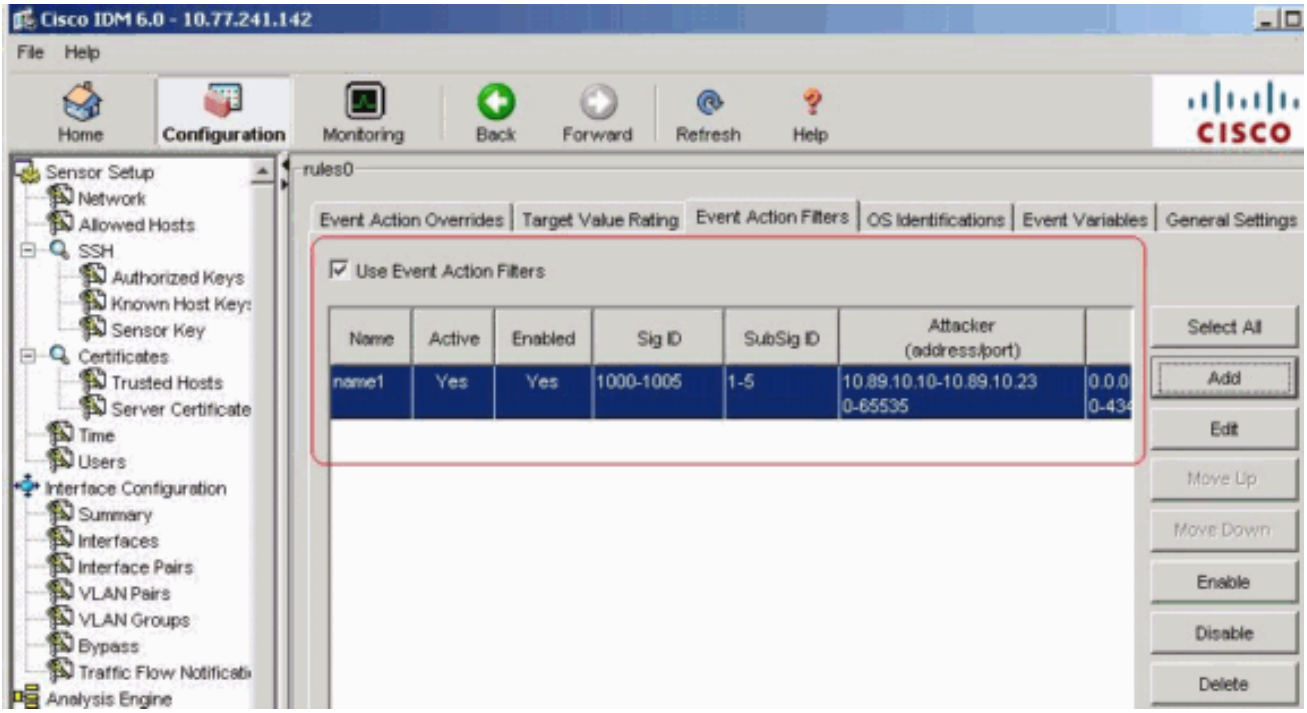
3. Per aggiungere un filtro azioni evento, fare clic su **Add** (Aggiungi).Verrà visualizzata la finestra di dialogo Aggiungi filtro azioni evento.
4. Nel campo Nome, immettere un nome come **nome1** per il filtro azioni evento.Viene fornito un nome predefinito, ma è possibile modificarlo in un nome più significativo.
5. Nel campo Attivo, fare clic sul pulsante di opzione **Sì** per aggiungere il filtro all'elenco in modo che abbia effetto sugli eventi filtro.
6. Per abilitare il filtro, nel campo Attivato fare clic sul pulsante di opzione **Sì**.**Nota: è** inoltre necessario selezionare la casella di controllo **Usa filtri azione evento** nella scheda Filtri azione evento oppure nessuno dei filtri dell'azione evento viene attivato indipendentemente dal fatto che sia stata selezionata o meno la casella di controllo **Sì** nella finestra di dialogo Aggiungi filtro azione evento.
7. Nel campo Signature ID immettere gli ID di tutte le firme a cui applicare il filtro.Èpossibile

utilizzare un elenco, ad esempio 1000, 1005, o un intervallo, ad esempio **1000-1005** o una delle variabili SIG se sono state definite nella scheda Variabili evento. Inserire $ come prefisso per la variabile.

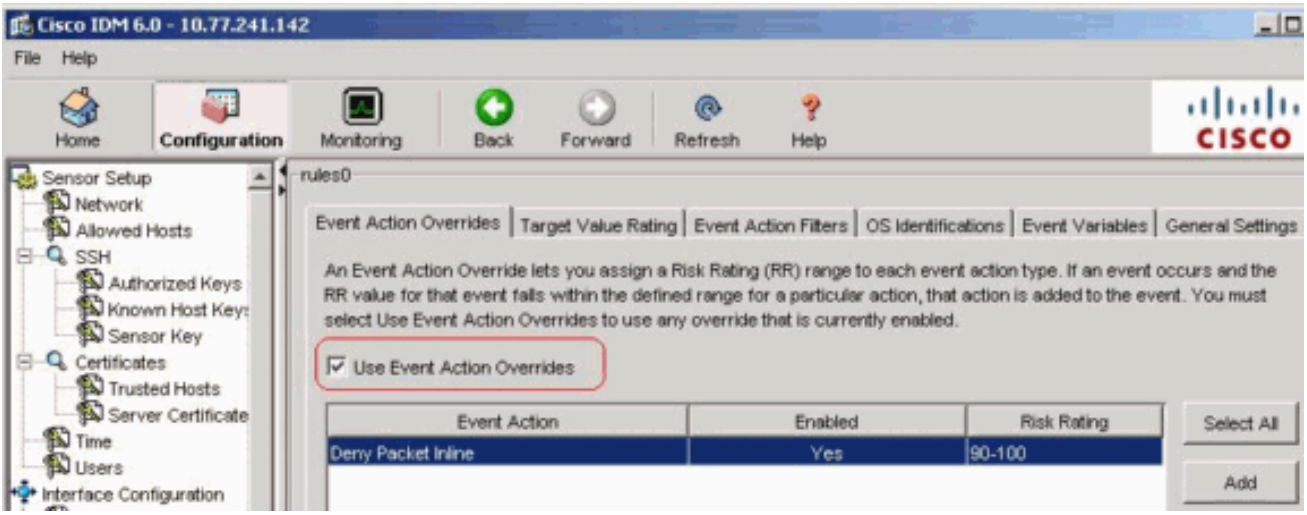
8. Nel campo ID firma secondaria immettere gli ID delle firme secondarie a cui applicare il filtro. Ad esempio, **1-5**.
9. Nel campo Indirizzo utente malintenzionato, immettere l'indirizzo IP dell'host di origine.Èpossibile utilizzare una delle variabili definite nella scheda Variabili evento. Inserire $ come prefisso per la variabile. È inoltre possibile immettere un intervallo di indirizzi, ad esempio **10.89.10.10-10.89.10.23**. Il valore predefinito è 0.0.0-255.255.255.255.
10. Nel campo Porta utente non autorizzato immettere il numero di porta utilizzato dall'utente non autorizzato per inviare il pacchetto che ha causato il problema.
11. Nel campo Indirizzo della vittima, immettere l'indirizzo IP dell'host destinatario.Èpossibile utilizzare una delle variabili definite nella scheda Variabili evento. Inserire $ come prefisso per la variabile. È inoltre possibile immettere un intervallo di indirizzi, ad esempio **192.56.10.1-192.56.10.255**. Il valore predefinito è 0.0.0-255.255.255.255.
12. Nel campo Porta vittima, immettere il numero di porta utilizzato dall'host vittima per ricevere il pacchetto che ha causato il danno. Ad esempio, **0-434**.
13. Nel campo Rating rischio immettere un intervallo RR per il filtro. Ad esempio, **85-100**.Se il valore RR di un evento rientra nell'intervallo specificato, l'evento viene elaborato in base ai criteri di questo filtro.
14. Dall'elenco a discesa Azioni da sottrarre scegliere le azioni che si desidera rimuovere dall'evento tramite questo filtro. Ad esempio, scegliere **Reimposta connessione TCP**.**Suggerimento:** tenere premuto il tasto **Ctrl** per scegliere più di un'azione evento nell'elenco.
15. Nell'elenco a discesa Rilevanza sistema operativo scegliere se si desidera sapere se l'avviso è relativo al sistema operativo identificato per la vittima. Ad esempio, scegliere **Pertinente**.
16. Nel campo Percentuale di rifiuto, immettere la percentuale di pacchetti da negare per le funzionalità di attacco Deny. Ad esempio, **90**.Il valore predefinito è 100%.
17. Nel campo Interrompi in corrispondenza scegliere uno dei seguenti pulsanti di opzione:**Sì**: se si desidera che il componente Filtri azioni eventi interrompa l'elaborazione dopo la rimozione delle azioni di questo particolare filtroI filtri rimanenti non vengono elaborati; pertanto, non è possibile rimuovere ulteriori azioni dall'evento.**No** - Se si desidera continuare l'elaborazione di filtri aggiuntivi
18. Nel campo Commenti immettere i commenti che si desidera memorizzare con il filtro, ad esempio lo scopo del filtro o il motivo per cui il filtro è stato configurato in modo particolare. Ad esempio, **NUOVO FILTRO**.**Suggerimento:** fare clic su **Annulla** per annullare le modifiche e chiudere la finestra di dialogo Aggiungi filtro azione evento.



19. Fare clic su **OK**.Il nuovo filtro delle azioni evento viene ora visualizzato nell'elenco della scheda Filtri azioni evento come illustrato.

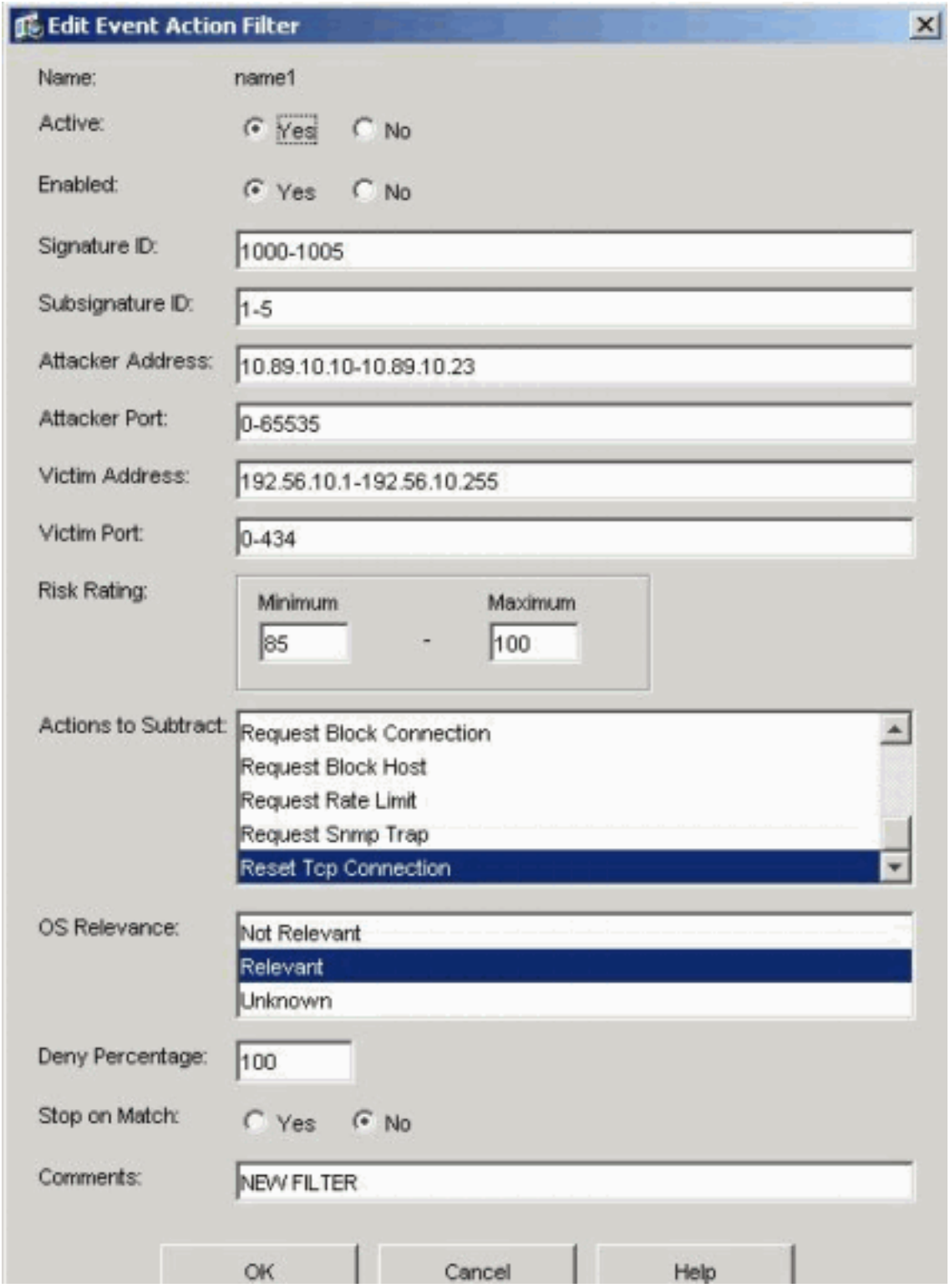


20. Selezionare la casella di controllo **Usa sostituzioni azione evento** come illustrato.



Nota: è necessario selezionare la casella di controllo **Usa sostituzioni azione evento** nella scheda Sostituzioni azione evento oppure nessuna delle sostituzioni dell'azione evento deve essere attivata indipendentemente dal valore impostato nella finestra di dialogo Aggiungi filtro azione evento.

21. Selezionare un filtro azioni evento esistente nell'elenco per modificarlo e quindi fare clic su **Modifica**.Verrà visualizzata la finestra di dialogo Modifica filtro azioni



evento.

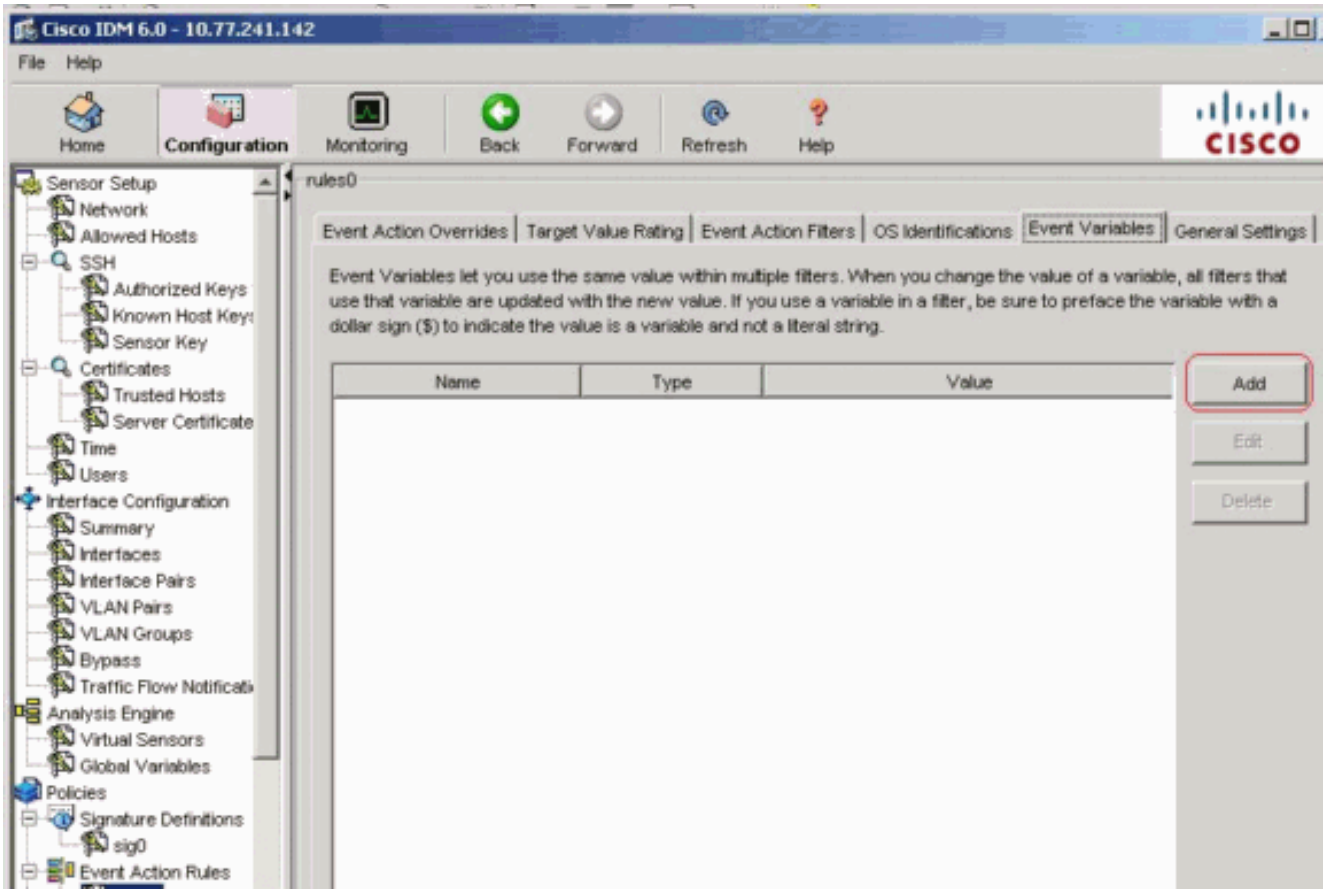
22. Modificare i valori nei campi che è necessario modificare.Per informazioni su come completare i campi, vedere i passaggi da 4 a 18.**Suggerimento:** fare clic su **Annulla** per annullare le modifiche e chiudere la finestra di dialogo Modifica filtro azioni evento.
23. Fare clic su **OK**.Il filtro delle azioni evento modificato verrà visualizzato nell'elenco della scheda Filtri azioni evento.
24. Selezionare la casella di controllo **Usa sostituzioni azione evento**.**Nota: è** necessario selezionare la casella di controllo **Usa sostituzioni azione evento** nella scheda Sostituzioni azione evento oppure nessuna delle sostituzioni dell'azione evento è abilitata indipendentemente dal valore impostato nella finestra di dialogo Modifica filtro azione evento.
25. Selezionare un filtro azioni evento nell'elenco per eliminarlo e quindi fare clic su **Elimina**.Il filtro azioni evento non è più visualizzato nell'elenco della scheda Filtri azioni evento.

26. Filtrare l'elenco verso l'alto o verso il basso per spostare un'azione evento, selezionarla e quindi fare clic su **Sposta su** o **Sposta giù**.**Suggerimento:** fare clic su **Reimposta** per rimuovere le modifiche.
27. Per applicare le modifiche e salvare la configurazione modificata, fare clic su **Apply** (Applica).

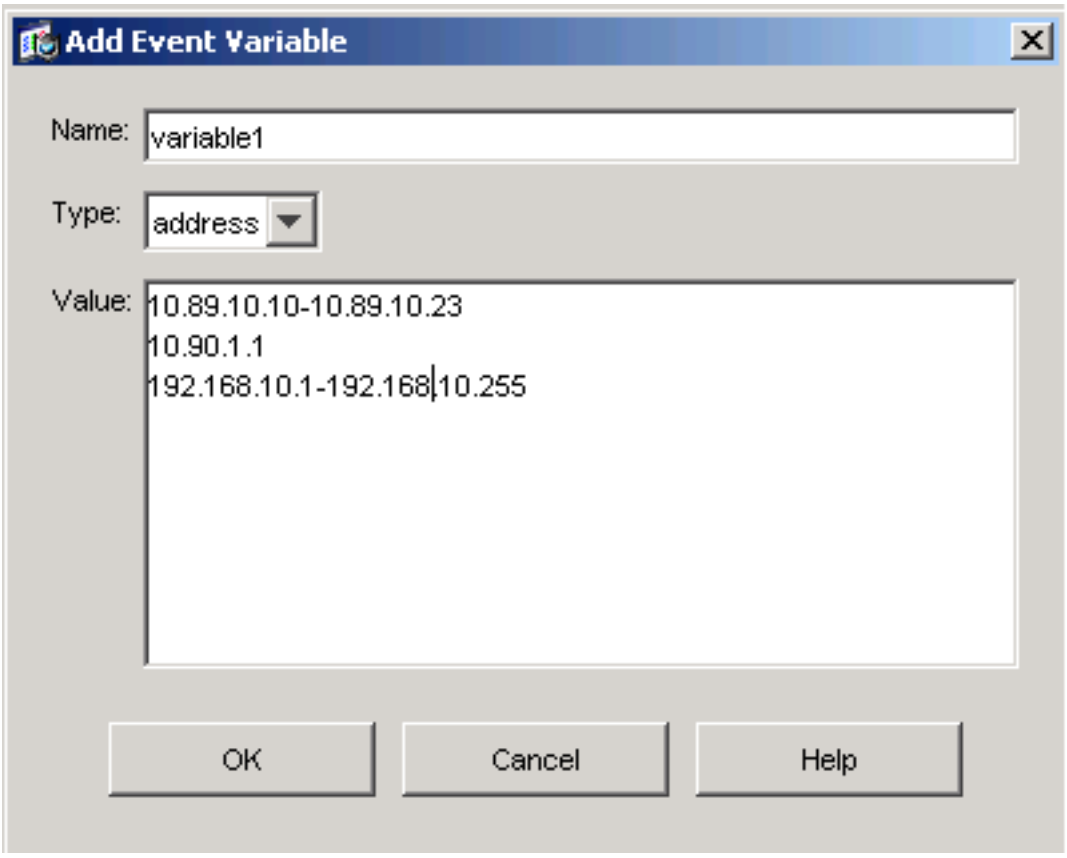
Configurazione variabile evento

Completare questi passaggi per aggiungere, modificare ed eliminare le variabili di evento:

1. Accedi. Ad esempio, utilizzare un account con privilegi di amministratore o di operatore.
2. Scegliere **Configurazione > Criteri > Regole d'azione evento > Regole0 > Variabili di evento** se la versione del software è 6.x. Per la versione del software 5.x, scegliere **Configurazione > Regole d'azione evento > Variabili evento**.Viene visualizzata la scheda Variabili evento.

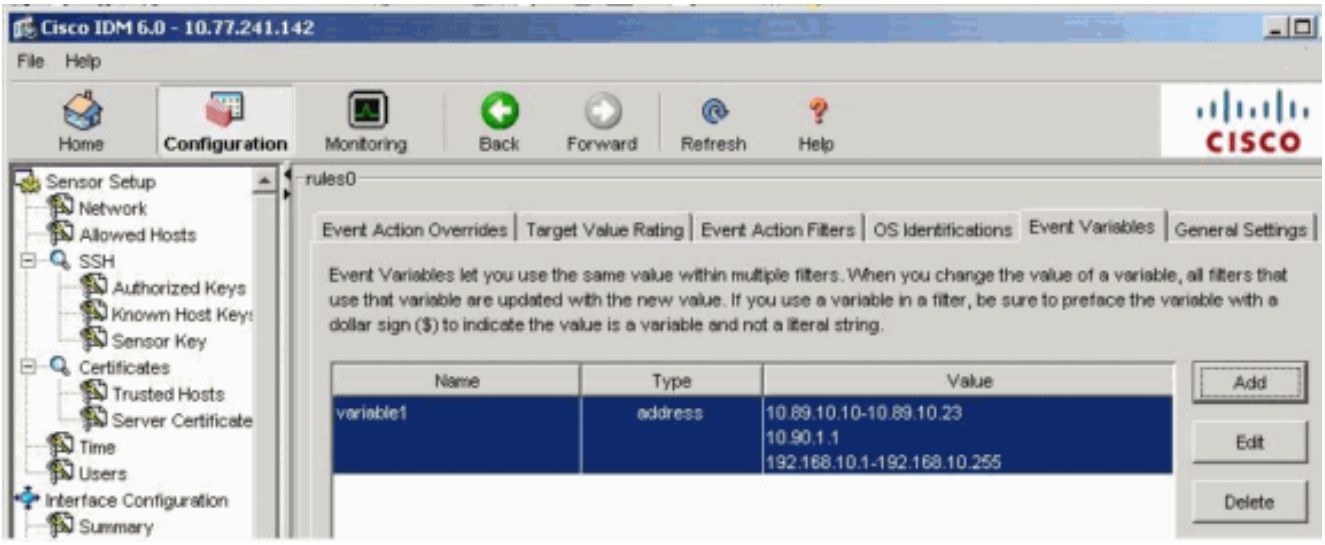


3. Per creare una variabile, fare clic su **Add** (Aggiungi).Verrà visualizzata la finestra di dialogo Aggiungi variabile.
4. Nel campo Nome immettere un nome per la variabile.**Nota:** il nome valido può contenere solo numeri o lettere. È inoltre possibile utilizzare un trattino (-) o un carattere di sottolineatura (_).
5. Nel campo Valore immettere i valori per questa variabile.Specificare l'indirizzo IP completo o gli intervalli o il set di intervalli. Ad esempio:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**Nota:** è possibile utilizzare le virgole come delimitatori. Accertarsi che non vi siano spazi alla fine della virgola. In caso contrario, viene visualizzato un messaggio di errore `Convalida non riuscita`.**Suggerimento:** fare clic su **Annulla** per annullare le modifiche e chiudere la finestra di dialogo Aggiungi variabile



evento.

6. Fare clic su **OK**.La nuova variabile verrà visualizzata nell'elenco della scheda Variabili di evento.



7. Scegliere la variabile esistente nell'elenco per modificarla e quindi fare clic su **Modifica**.Verrà visualizzata la finestra di dialogo Modifica variabile evento.
8. Nel campo Valore immettere le modifiche apportate al valore.
9. Fare clic su **OK**.La variabile di evento modificata verrà visualizzata nell'elenco della scheda Variabili di evento.**Suggerimento:** scegliere **Reimposta** per rimuovere le modifiche.
10. Per applicare le modifiche e salvare la configurazione modificata, fare clic su **Apply** (Applica).

Informazioni correlate

- Pagina di supporto di Cisco Intrusion Prevention System
- Documentazione e supporto tecnico – Cisco Systems