IPS 6.X e versioni successive - Configurazione dei sensori virtuali con IME

Sommario

Introduzione

Questo documento spiega la funzione di Analysis Engine e come creare, modificare ed eliminare sensori virtuali su Cisco Secure Intrusion Prevention System (IPS) con Cisco IPS Manager Express (IME). Spiega inoltre come assegnare le interfacce a un sensore virtuale.

Nota: AIM-IPS e NME-IPS non supportano la virtualizzazione.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 4200 IPS Device con software versione 6.0 e successive
- Cisco IPS Manager Express (IME) versione 6.1.1 e successive**Nota:** mentre l'IME può essere utilizzato per monitorare i dispositivi sensore che eseguono Cisco IPS 5.0 e versioni successive, alcune delle nuove funzionalità e caratteristiche fornite con l'IME sono supportate solo sui sensori che eseguono Cisco IPS 6.1 o versioni successive.**Nota:** Cisco Secure Intrusion Prevention System (IPS) 5.x supporta solo il sensore virtuale predefinito vs0. I sensori virtuali diversi da quello predefinito vs0 sono supportati in IPS 6.x e versioni 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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con i seguenti sensori:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20
- AIP-SSM

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Motore di analisi

Analysis Engine esegue l'analisi dei pacchetti e il rilevamento degli avvisi. Controlla il traffico che passa attraverso interfacce specifiche. I sensori virtuali vengono creati in Analysis Engine. Ogni sensore virtuale ha un nome univoco con un elenco di interfacce, coppie di interfacce inline, coppie di VLAN inline e gruppi di VLAN associati. Per evitare problemi di ordinamento delle definizioni, nelle assegnazioni non sono consentiti conflitti o sovrapposizioni. Le interfacce, le coppie di interfacce inline, le coppie di VLAN inline e i gruppi di VLAN vengono assegnati a un sensore virtuale specifico in modo che nessun pacchetto venga elaborato da più di un sensore virtuale. Ogni sensore virtuale è inoltre associato a una specifica definizione di firma, a regole di azione per gli eventi e a una configurazione per il rilevamento di anomalie. I pacchetti provenienti

da interfacce, coppie di interfacce inline, coppie di VLAN inline e gruppi di VLAN non assegnati ad alcun sensore virtuale vengono eliminati in base alla configurazione di bypass inline.

Informazioni sui sensori virtuali

Il sensore può ricevere dati da uno o più flussi di dati monitorati. Questi flussi di dati monitorati possono essere porte di interfaccia fisica o porte di interfaccia virtuale. Ad esempio, un singolo sensore può monitorare il traffico proveniente dalla parte anteriore del firewall, da quella posteriore o dalla parte anteriore e posteriore del firewall contemporaneamente. E un singolo sensore può monitorare uno o più flussi di dati. In questo caso, a tutti i flussi di dati monitorati viene applicata una singola policy o configurazione del sensore. Un sensore virtuale è una raccolta di dati definita da un insieme di criteri di configurazione. Il sensore virtuale viene applicato a un set di pacchetti definito dal componente di interfaccia. Un sensore virtuale può monitorare più segmenti ed è possibile applicare una policy o una configurazione diversa per ogni sensore virtuale all'interno di un singolo sensore fisico. È possibile impostare un criterio diverso per ogni segmento monitorato in fase di analisi. È inoltre possibile applicare la stessa istanza di criterio, ad esempio, sig0, rules0 o ad0, a sensori virtuali diversi. È possibile assegnare interfacce, coppie di interfacce inline, coppie di VLAN inline e gruppi di VLAN a un sensore virtuale.

Nota: Cisco Secure Intrusion Prevention System (IPS) non supporta più di quattro sensori virtuali. Il sensore virtuale predefinito è vs0. Non è possibile eliminare il sensore virtuale predefinito. L'elenco delle interfacce, la modalità operativa di rilevamento delle anomalie, la modalità di rilevamento delle sessioni TCP in linea e la descrizione del sensore virtuale sono le uniche funzionalità di configurazione modificabili per il sensore virtuale predefinito. Non è possibile modificare la definizione della firma, le regole di azione degli eventi o i criteri di rilevamento delle anomalie.

Vantaggi e limitazioni della virtualizzazione

Vantaggi della virtualizzazione

La virtualizzazione presenta i seguenti vantaggi:

- Èpossibile applicare diverse configurazioni a diversi insiemi di traffico.
- Èpossibile monitorare due reti con spazi IP sovrapposti con un solo sensore.
- Èpossibile monitorare sia all'interno che all'esterno di un firewall o di un dispositivo NAT.

Limitazioni della virtualizzazione

La virtualizzazione presenta le seguenti limitazioni:

- Ènecessario assegnare entrambi i lati del traffico asimmetrico allo stesso sensore virtuale.
- L'uso dell'acquisizione VACL o dell'SPAN (monitoraggio promiscuo) non è coerente con il tagging della VLAN, il che causa problemi ai gruppi di VLAN.Quando si usa il software Cisco IOS, una porta di acquisizione VACL o una destinazione SPAN non sempre riceve pacchetti con tag, anche se è configurata per il trunking.Quando si utilizza l'MSFC, la commutazione rapida dei percorsi delle route apprese modifica il comportamento delle acquisizioni VACL e dell'SPAN.
- Archivio permanente limitato.

Requisiti di virtualizzazione

La virtualizzazione ha i seguenti requisiti di acquisizione del traffico:

- Il sensore virtuale deve ricevere il traffico con intestazioni 802.1q, ad eccezione del traffico sulla VLAN nativa della porta di acquisizione.
- Il sensore deve poter vedere entrambe le direzioni del traffico sullo stesso gruppo VLAN e sullo stesso sensore virtuale su ciascun sensore.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per aggiungere, modificare ed eliminare i sensori virtuali.

Aggiungi sensori virtuali

Per creare un sensore virtuale, eseguire il comando virtual-sensor name nella modalità secondaria del motore di analisi del servizio. Al sensore virtuale vengono assegnati criteri (rilevamento anomalie, regole di azione evento e definizione della firma). Quindi, le interfacce (promiscue, coppie di interfacce in linea, coppie di VLAN in linea e gruppi di VLAN) vengono assegnate al sensore virtuale. È necessario configurare le coppie di interfacce in linea e le coppie di VLAN prima di poterle assegnare a un sensore virtuale. Si applicano le seguenti opzioni:

- **anomaly-detection** - Parametri di rilevamento anomalie.**anomaly-detection-name** name - Nome del criterio di rilevamento anomalie**modalità operativa**: modalità di rilevamento delle anomalie (**inattiva, impara, rileva**)
- **description**: descrizione del sensore virtuale
- **event-action-rules**: nome del criterio per le regole d'azione degli eventi
- **inline-TCP-evasion-protection-mode**: consente di scegliere il tipo di modalità di normalizzazione necessaria per l'ispezione del traffico:**asimmetrica**: può vedere solo una direzione del flusso del traffico bidirezionale. La protezione in modalità asimmetrica allenta la protezione contro l'evasione sul layer TCP.**Nota:** la modalità asimmetrica consente al sensore di sincronizzare lo stato con il flusso e di mantenere l'ispezione per i motori che non richiedono entrambe le direzioni. La modalità asimmetrica riduce la sicurezza in quanto la protezione completa richiede la visualizzazione di entrambi i lati del traffico.**strict**: se un pacchetto viene perso per un motivo qualsiasi, tutti i pacchetti successivi a quello mancante non vengono elaborati. La rigida protezione contro l'evasione garantisce l'applicazione completa dello stato TCP e del monitoraggio delle sequenze.**Nota:** i pacchetti non ordinati o mancanti possono produrre firme del motore Normalizer 1300 o 1330, che tentano di correggere la situazione, ma possono causare connessioni negate.
- **inline-TCP-session-tracking-mode**: metodo avanzato che consente di identificare le sessioni TCP duplicate nel traffico inline. L'impostazione predefinita è sensore virtuale, che è quasi sempre la scelta migliore.**virtual-sensor**: tutti i pacchetti con la stessa chiave di sessione (AaBb) all'interno di un sensore virtuale appartengono alla stessa sessione.**interface-and-vlan**: tutti i pacchetti con la stessa chiave di sessione (AaBb) nella stessa VLAN (o coppia di VLAN in linea) e sulla stessa interfaccia appartengono alla stessa sessione. I pacchetti con la stessa chiave ma su VLAN o interfacce diverse vengono tracciati in modo indipendente.**solo vlan**: tutti i pacchetti con la stessa chiave di sessione (AaBb) nella stessa VLAN (o coppia di VLAN

in linea), indipendentemente dall'interfaccia, appartengono alla stessa sessione. I pacchetti con la stessa chiave ma su VLAN diverse vengono tracciati in modo indipendente.

- **signature-definition**: nome del criterio di definizione della firma
- **interfacce logiche** - Nome delle interfacce logiche (coppie di interfacce in linea)
- **interfacce fisiche**: nome delle interfacce fisiche (coppie di VLAN promiscue in linea e gruppi di VLAN)**subinterface-number** - Numero della sottointerfaccia fisica. Se il tipo di sottointerfaccia è none, il valore 0 indica che l'intera interfaccia è assegnata in modalità promiscua.**no** - Rimuove una voce o una selezione

Per aggiungere un sensore virtuale, procedere come segue:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Accedere alla modalità di analisi del servizio.
```
sensor# configure terminal

        sensor(config)# service analysis-engine

        sensor(config-ana)#
```
3. Aggiungi un sensore virtuale.
```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#
```
4. Aggiungere una descrizione per il sensore virtuale.
```
sensor(config-ana-vir)# description virtual sensor 2
```
5. Assegnare una policy di rilevamento delle anomalie e una modalità operativa a questo sensore virtuale.
```
sensor(config-ana-vir)# anomaly-detection

        sensor(config-ana-vir-ano)# anomaly-detection-name ad1

        sensor(config-ana-vir-ano)# operational-mode learn
```
6. Assegna un criterio per le regole di azione degli eventi a questo sensore virtuale.
```
sensor(config-ana-vir-ano)# exit

        sensor(config-ana-vir)# event-action-rules rules1
```
7. Assegna un criterio di definizione della firma a questo sensore virtuale.
```
sensor(config-ana-vir)# signature-definition sig1
```
8. Assegnare la modalità di rilevamento delle sessioni TCP in linea.
```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode virtual-sensor
```
   Il valore predefinito è la modalità sensore virtuale, che è quasi sempre la scelta migliore.
9. Assegnare la modalità di protezione da evasione TCP in linea.
```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```
   L'impostazione predefinita è la modalità rigorosa, che è quasi sempre la scelta migliore.
10. Visualizza l'elenco delle interfacce disponibili.
```
sensor(config-ana-vir)# physical-interface ?

         GigabitEthernet0/0     GigabitEthernet0/0 physical interface.

         GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
```

```
  GigabitEthernet2/0     GigabitEthernet0/2 physical interface.

  GigabitEthernet2/1     GigabitEthernet0/3 physical interface.

  sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?

  <none available>
```

11. Assegnare le interfacce in modalità promiscua che si desidera aggiungere a questo sensore virtuale.
    ```
    sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
    ```
    Ripetere questo passaggio per tutte le interfacce promiscue che si desidera assegnare a questo sensore virtuale.
12. Assegnare le coppie di interfacce inline che si desidera aggiungere al sensore virtuale.
    ```
    sensor(config-ana-vir)# logical-interface inline_interface_pair_name
    ```
    Le interfacce devono essere già state accoppiate.
13. Assegnare le sottointerfacce delle coppie o dei gruppi di VLAN inline che si desidera aggiungere al sensore virtuale come mostrato di seguito:
    ```
    sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
    subinterface_number
    ```
    Ènecessario aver già suddiviso le interfacce in coppie o gruppi VLAN.
14. Verificare le impostazioni del sensore virtuale.
    ```
    sensor(config-ana-vir)# show settings

       name: vs2

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

          description: virtual sensor 1 default:

          signature-definition: sig1 default: sig0

          event-action-rules: rules1 default: rules0

          anomaly-detection

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

             anomaly-detection-name: ad1 default: ad0

             operational-mode: learn default: detect

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

          physical-interface (min: 0, max: 999999999, current: 2)

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

             name: GigabitEthernet0/2

             subinterface-number: 0 <defaulted>

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

```
        inline-TCP-session-tracking-mode: virtual-sensor default: virtual-sensor

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

        logical-interface (min: 0, max: 999999999, current: 0)

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

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

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

sensor(config-ana-vir)#
```

15. Uscire dalla modalità del motore di analisi.

```
sensor(config-ana-vir)# exit

        sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

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

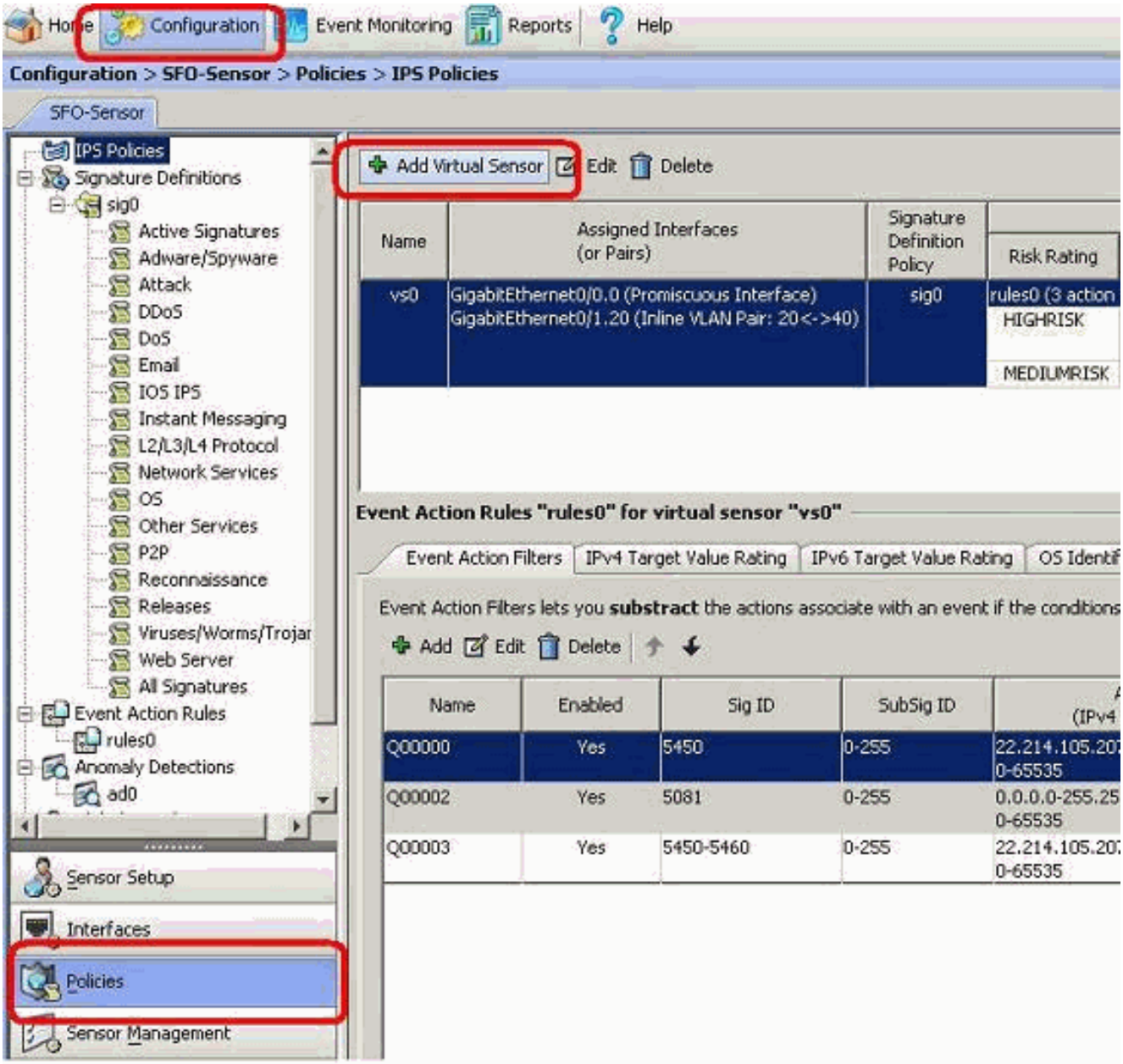
La procedura per aggiungere un sensore virtuale a Cisco Secure Intrusion Prevention System (IPS) è stata completata. Completare la stessa procedura per aggiungere altri sensori virtuali.

Nota: Cisco Secure Intrusion Prevention System (IPS) non supporta più di quattro sensori virtuali. Il sensore virtuale predefinito è vs0.

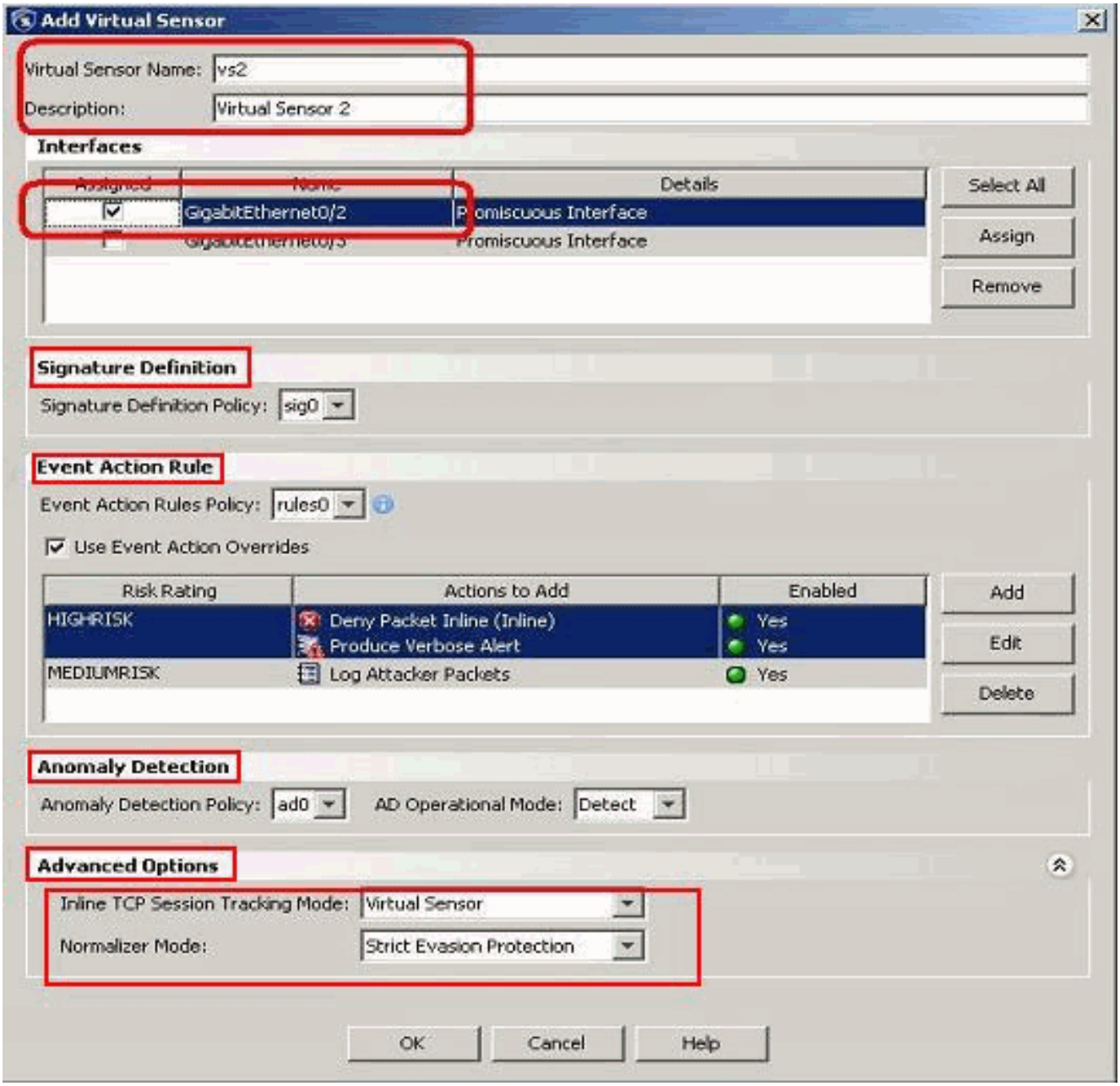
Aggiungi sensore virtuale con IME

Completare questa procedura per configurare un sensore virtuale su Cisco Secure Intrusion Prevention System (IPS) con Cisco IPS Manager Express:

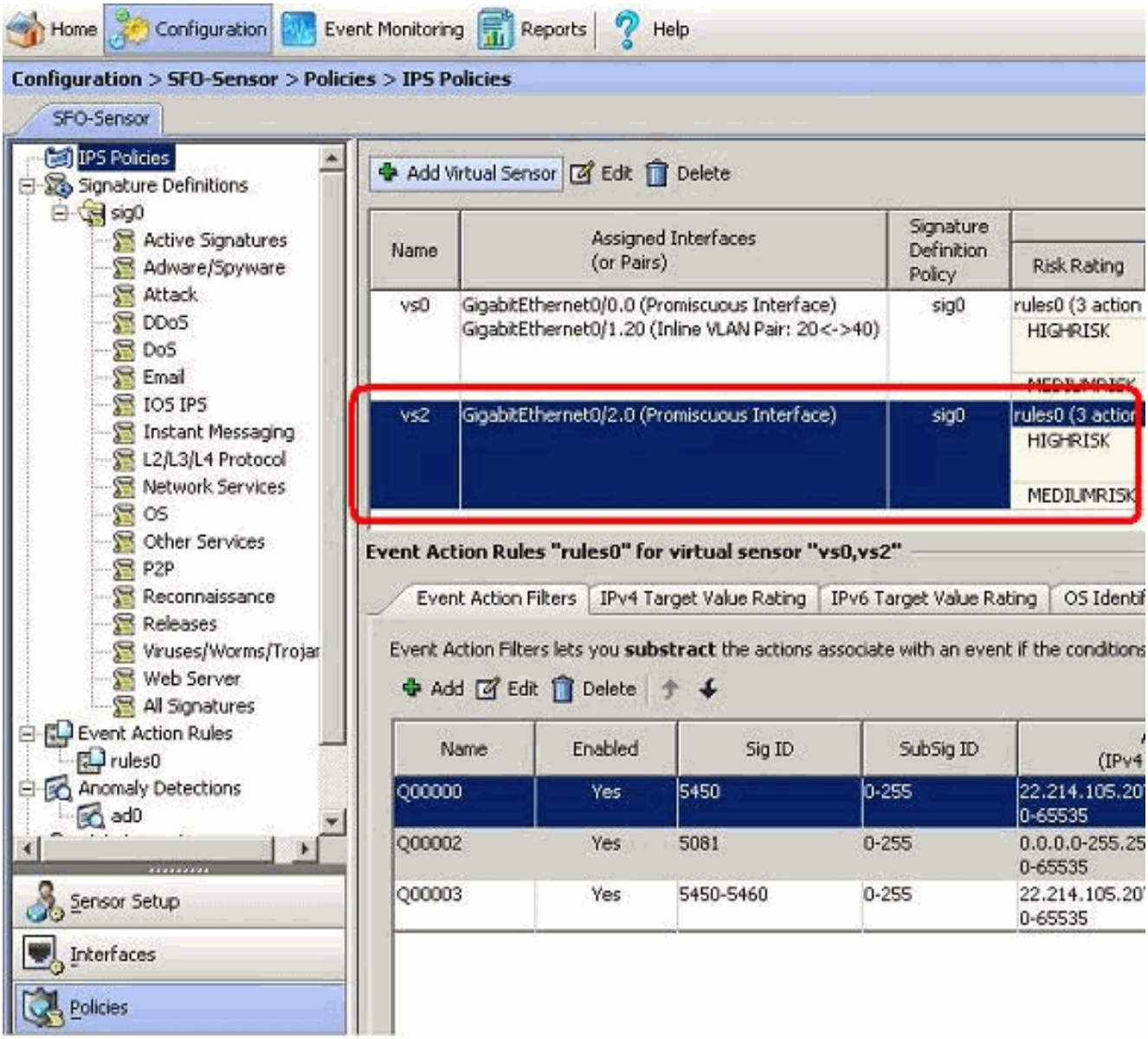
1. Scegliere **Configurazione > SFO-Sensor> Criteri> Criteri IPS**. Quindi, fare clic su **Add virtual sensor** (Aggiungi sensore virtuale) come mostrato nella schermata.



2. Assegnare un nome al sensore virtuale (vs2 in questo esempio) e aggiungere una descrizione al sensore virtuale nello spazio fornito. Assegnare inoltre le interfacce in modalità promiscua che si desidera aggiungere a questo sensore virtuale. Gigabit Ethernet 0/2 è selezionato qui. A questo punto, fornire i dettagli nelle sezioni **Definizione firma**, **Regola azione evento**, **Rilevamento anomalie** e **Opzioni avanzate** come mostrato nella schermata.In **Opzioni avanzate** fornire i dettagli relativi alla modalità di rilevamento delle sessioni TCP e alla modalità normalizzatore. Qui la **modalità TCP Session Tracking** è un **sensore virtuale** e la **modalità Normalizer** è la modalità **Strict Evasion Protection**.



3. Fare clic su **OK**.
4. Il sensore virtuale vs2 appena aggiunto viene visualizzato nell'elenco dei sensori virtuali. Fare clic su **Apply** (Applica) per inviare la nuova configurazione del sensore virtuale a Cisco Secure Intrusion Prevention System
(IPS).



La configurazione per l'aggiunta di un sensore virtuale è stata completata.

Modifica di sensori virtuali

I seguenti parametri di un sensore virtuale possono essere modificati:

- Criteri di definizione della firma
- Criteri regole d'azione evento
- Criteri di rilevamento delle anomalie
- Modalità operativa rilevamento anomalie
- Modalità di rilevamento sessioni TCP in linea
- Descrizione
- Interfacce assegnate

Per modificare un sensore virtuale, procedere come segue:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Accedere alla modalità di analisi del servizio.

```
sensor# configure terminal

        sensor(config)# service analysis-engine
```

```
        sensor(config-ana)#
```

3. Modificare il sensore virtuale, vs1.

```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#
```

4. Modificare la descrizione di questo sensore virtuale.

```
sensor(config-ana-vir)# description virtual sensor A
```

5. Modificare il criterio di rilevamento delle anomalie e la modalità operativa assegnati al sensore virtuale.

```
sensor(config-ana-vir)# anomaly-detection

        sensor(config-ana-vir-ano)# anomaly-detection-name ad0

        sensor(config-ana-vir-ano)# operational-mode learn
```

6. Modifica il criterio delle regole d'azione degli eventi assegnato al sensore virtuale.

```
sensor(config-ana-vir-ano)# exit

        sensor(config-ana-vir)# event-action-rules rules0
```

7. Modifica i criteri di definizione della firma assegnati a questo sensore virtuale.

```
sensor(config-ana-vir)# signature-definition sig0
```

8. Modificare la modalità di rilevamento delle sessioni TCP in linea.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

   Il valore predefinito è la modalità sensore virtuale, che è quasi sempre la scelta migliore.

9. Visualizza l'elenco delle interfacce disponibili.

```
sensor(config-ana-vir)# physical-interface ?

        GigabitEthernet0/0     GigabitEthernet0/0 physical interface.

        GigabitEthernet0/1     GigabitEthernet0/1 physical interface.

        GigabitEthernet2/0     GigabitEthernet0/2 physical interface.

        GigabitEthernet2/1     GigabitEthernet0/3 physical interface.

        sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?

        <none available>
```

10. Modificare le interfacce in modalità promiscua assegnate a questo sensore virtuale.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

11. Modificare le coppie di interfacce inline assegnate a questo sensore virtuale.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

    Le interfacce devono essere già state accoppiate.

12. Modificare la sottointerfaccia con le coppie o i gruppi di VLAN inline assegnati al sensore virtuale.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

    Ènecessario aver già suddiviso le interfacce in coppie o gruppi VLAN.

13. Verificare le impostazioni modificate del sensore virtuale.

```
sensor(config-ana-vir)# show settings

   name: vs2

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

      description: virtual sensor 1 default:

      signature-definition: sig1 default: sig0

      event-action-rules: rules1 default: rules0

      anomaly-detection

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

         anomaly-detection-name: ad1 default: ad0

         operational-mode: learn default: detect

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

      physical-interface (min: 0, max: 999999999, current: 2)

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

         name: GigabitEthernet0/2

         subinterface-number: 0 <defaulted>

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

      inline-TCP-session-tracking-mode: interface-and-vlan default: virtual-sensor

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

      logical-interface (min: 0, max: 999999999, current: 0)

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

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

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

sensor(config-ana-vir)#
```

14. Uscire dalla modalità del motore di analisi.

```
sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

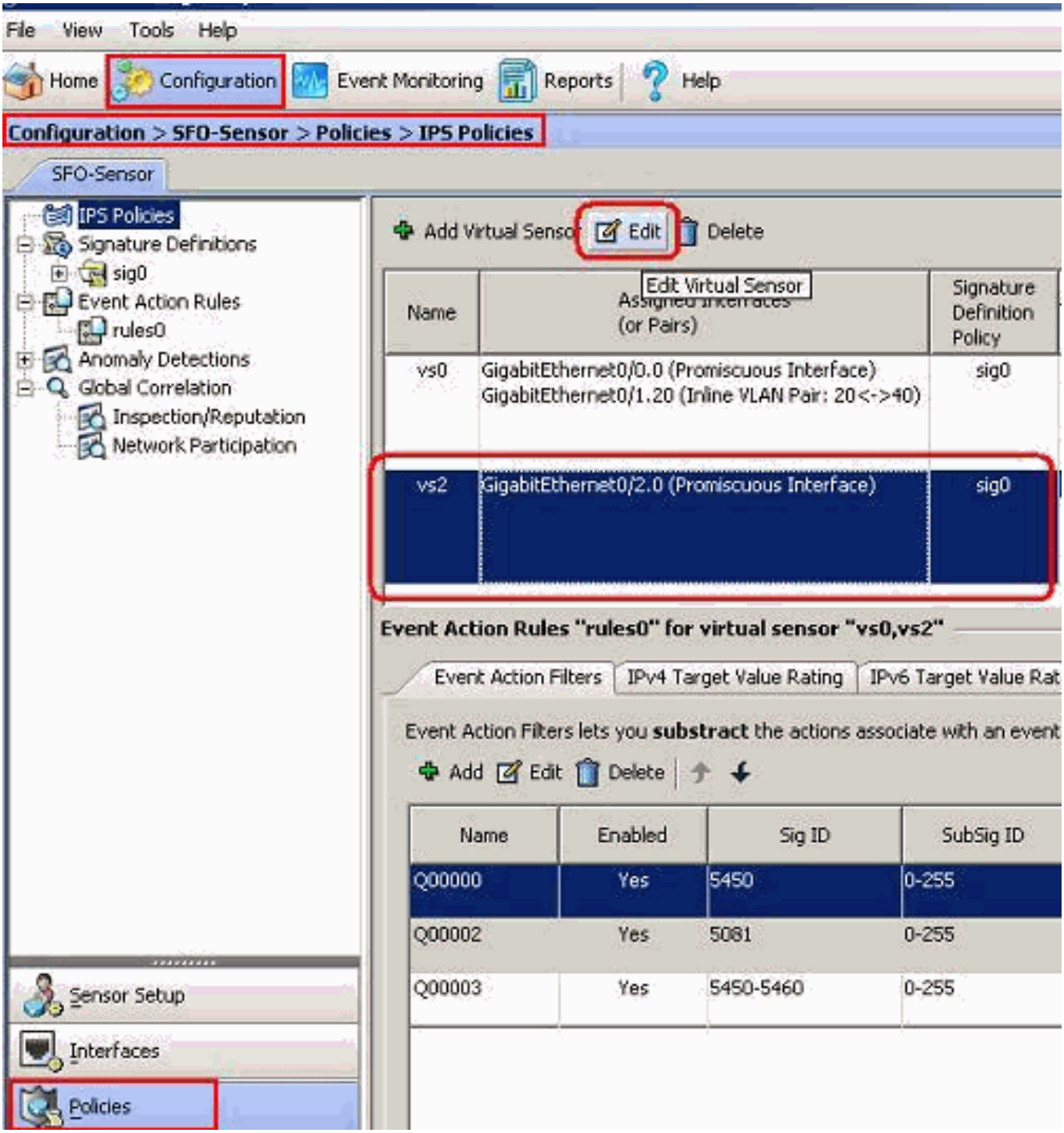
15. Premere **Invio** per applicare le modifiche o immettere **no** per ignorarle.

Modifica sensore virtuale con IME

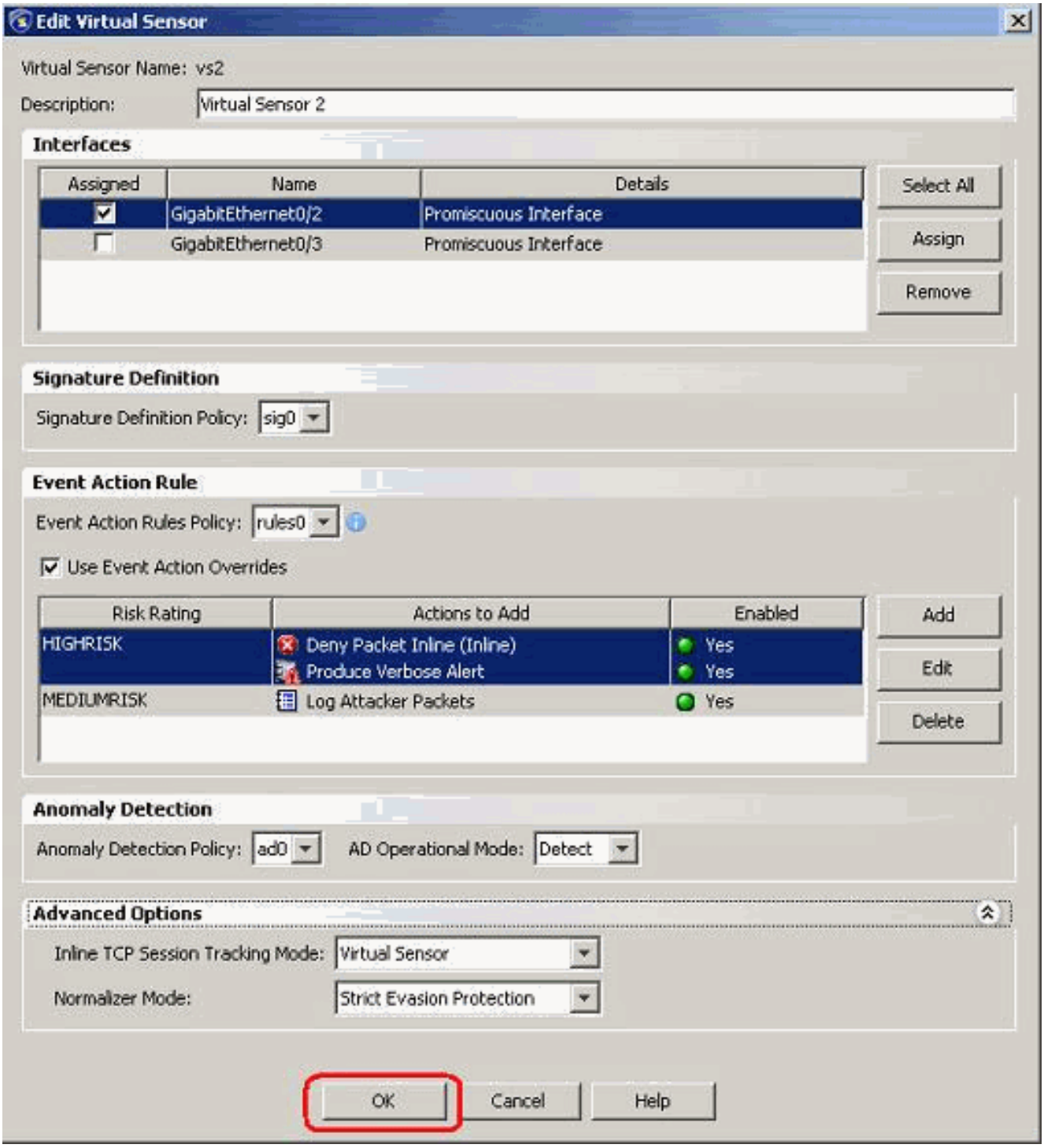
Completare questi passaggi per modificare un sensore virtuale su Cisco Secure Intrusion Prevention System (IPS) con Cisco IPS Manager Express:

1. Scegliere **Configurazione > SFO-Sensor> Criteri> Criteri IPS**.
2. Scegliere il sensore virtuale da modificare, quindi fare clic su **Modifica** come mostrato nella

schermata. Nell'esempio, vs2 è il sensore virtuale da modificare.



3. Nella finestra Modifica sensore virtuale, apportare le modifiche ai parametri per il sensore virtuale presente nelle sezioni **definizione della firma**, **Regola azione evento**, **Rilevamento anomalie** e **opzioni avanzate**. Fare clic su **OK**, quindi su **Applica**.



Il processo di modifica di un sensore virtuale è stato completato.

Elimina sensori virtuali

Per eliminare un sensore virtuale, procedere come segue:

1. Per eliminare un sensore virtuale, usare il comando **no virtual-sensor**.

```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#

        sensor(config-ana-vir)# exit

        sensor(config-ana)# no virtual-sensor vs2
```

2. Verificare il sensore virtuale eliminato.

```
sensor(config-ana)# show settings

   global-parameters

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

      ip-logging

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

         max-open-iplog-files: 20 <defaulted>

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

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

   virtual-sensor (min: 1, max: 255, current: 2)

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

      <protected entry>

      name: vs0 <defaulted>

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

         description: default virtual sensor <defaulted>

         signature-definition: sig0 <protected>

         event-action-rules: rules0 <protected>

         anomaly-detection

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

            anomaly-detection-name: ad0 <protected>

            operational-mode: detect <defaulted>

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

         physical-interface (min: 0, max: 999999999, current: 0)

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

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

         logical-interface (min: 0, max: 999999999, current: 0)

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

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

sensor(config-ana)#
```

Èpresente solo il sensore virtuale predefinito, **vs0**.

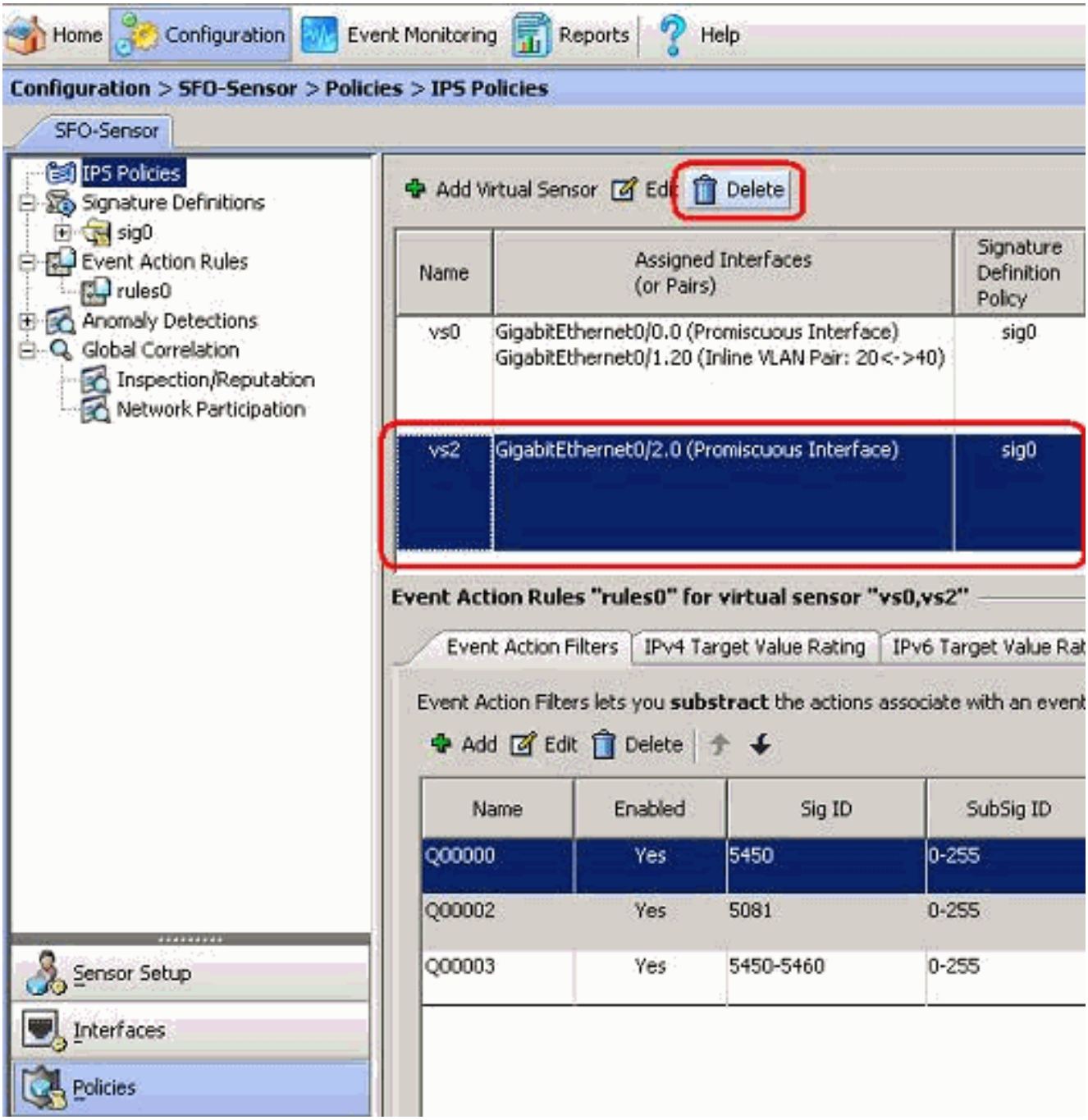
3. Uscire dalla modalità del motore di analisi.

```
sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

Elimina sensore virtuale con IME

Completare questa procedura per eliminare un sensore virtuale da Cisco Secure Intrusion Prevention System (IPS) con Cisco IPS Manager Express:

1. Scegliere **Configurazione > SFO-Sensor> Criteri> Criteri IPS**.
2. Scegliere il sensore virtuale da eliminare, quindi fare clic su **Elimina**, come mostrato nella schermata. Nell'esempio, vs2 è il sensore virtuale da eliminare.



Il processo di eliminazione di un sensore virtuale è stato completato. Il sensore virtuale vs2 viene eliminato.

Risoluzione dei problemi

IPS Manager Express non si avvia

Problema

Quando si tenta di accedere all'IPS tramite l'IME, IPS Manager Express non si avvia e viene visualizzato questo messaggio di errore:

```
"Cannot start IME client. Please check if it is already started.
Exception: Address already in use: Cannot bind"
```

Soluzione

Per risolvere questo problema, ricaricare il PC della workstation IME.

Informazioni correlate

- Pagina di supporto di Cisco Intrusion Prevention System
- Pagina di supporto di Cisco IPS Manager Express
- Protocollo NTP (Network Time Protocol)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems