Cisco Secure IPS - Esclusione di falsi allarmi positivi

Sommario

Introduzione

Questo documento descrive l'esclusione di falsi allarmi positivi per Cisco Secure Intrusion Prevention System (IPS).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, sono stati usati Cisco Secure Intrusion Prevention System (IPS) versione 7.0 e Cisco IPS Manager Express 7.0.

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.

Falsi allarmi positivi e falsi allarmi negativi

Cisco Secure IPS attiva un allarme quando un determinato pacchetto o una determinata sequenza di pacchetti corrisponde alle caratteristiche di profili di attacco noti definiti nelle firme Cisco Secure IPS. Un criterio critico per la progettazione delle firme IPS è quello di ridurre al minimo la presenza di falsi allarmi positivi e falsi negativi.

I falsi positivi (trigger benigni) si verificano quando l'IPS segnala come dannosa una determinata attività benigna. Ciò richiede l'intervento umano per diagnosticare l'evento. Un gran numero di falsi positivi può esaurire in modo significativo le risorse, e le competenze specializzate necessarie per analizzarle sono costose e difficili da trovare.

I falsi negativi si verificano quando l'IPS non rileva e segnala attività dannose effettive. La conseguenza di ciò può essere catastrofica e le firme devono essere continuamente aggiornate man mano che vengono scoperte nuove scoperte e tecniche di hacking. Ridurre al minimo i falsi negativi è una priorità molto alta, a volte a scapito di più ricorrenze di falsi positivi.

A causa della natura delle firme utilizzate dagli IPS per rilevare le attività dannose, è quasi impossibile eliminare completamente i falsi positivi e negativi senza compromettere gravemente l'efficacia dell'IPS o compromettere gravemente l'infrastruttura di elaborazione di un'organizzazione (ad esempio host e reti). Il tuning personalizzato quando viene implementato un IPS riduce al minimo i falsi positivi. Quando l'ambiente informatico cambia (ad esempio quando vengono installati nuovi sistemi e applicazioni), è necessario eseguire periodicamente un nuovo tuning. Cisco Secure IPS offre una funzionalità di sintonizzazione flessibile in grado di ridurre al minimo i falsi positivi durante le operazioni in stato stazionario.

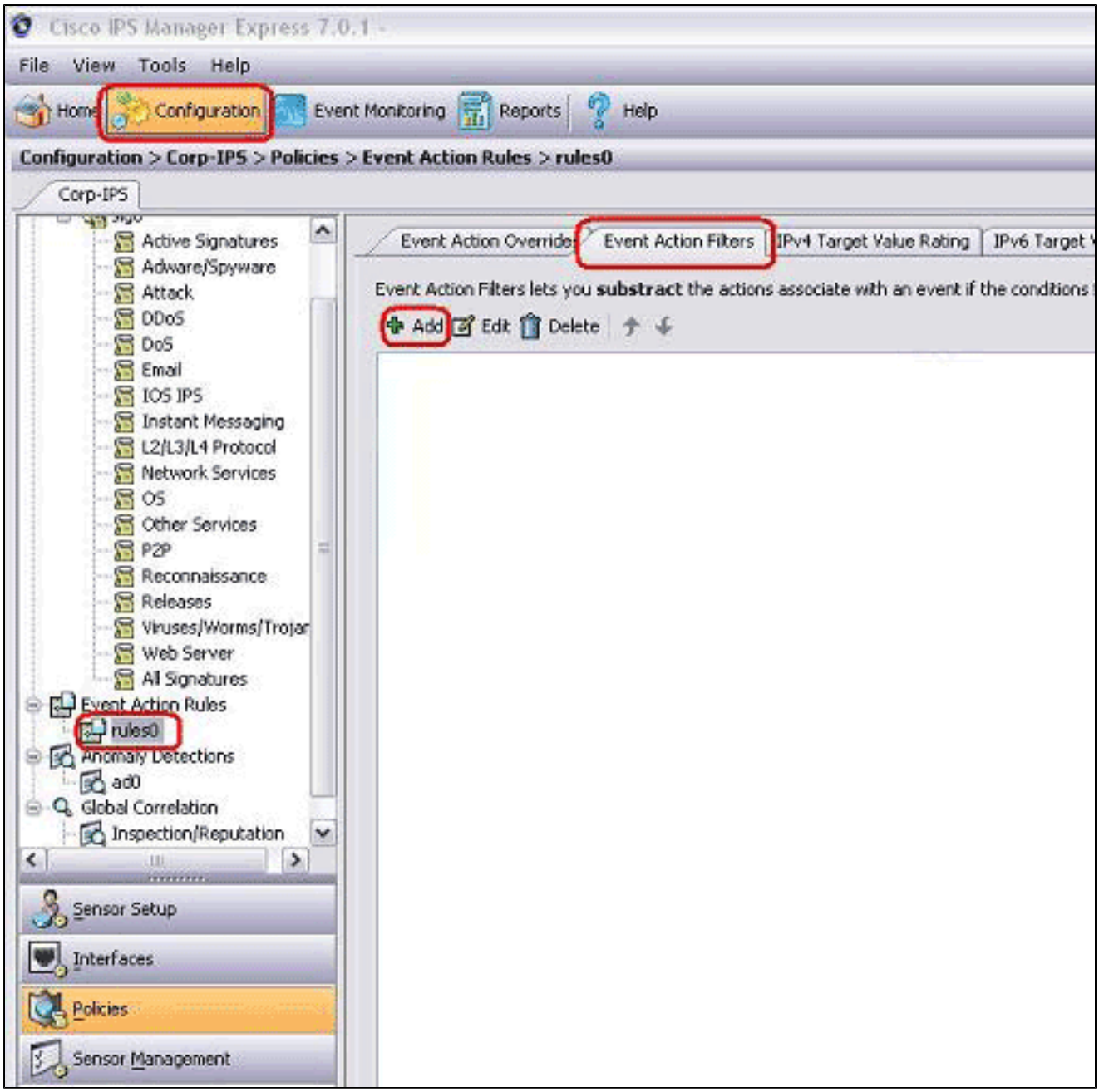
Meccanismo di esclusione Cisco Secure IPS

Cisco Secure IPS consente di escludere una firma specifica da o verso un host o indirizzi di rete specifici. Le firme escluse non generano icone di allarme o record di registro quando vengono attivate dagli host o dalle reti specificamente escluse tramite questo meccanismo. Ad esempio, una stazione di gestione di rete può eseguire il rilevamento della rete eseguendo il ping delle sweep, che attivano lo sweep di rete ICMP con firma Echo (ID firma 2100). Se si esclude la firma, non è necessario analizzare l'avviso ed eliminarlo ogni volta che viene eseguito il processo di rilevamento della rete.

Escludere un host

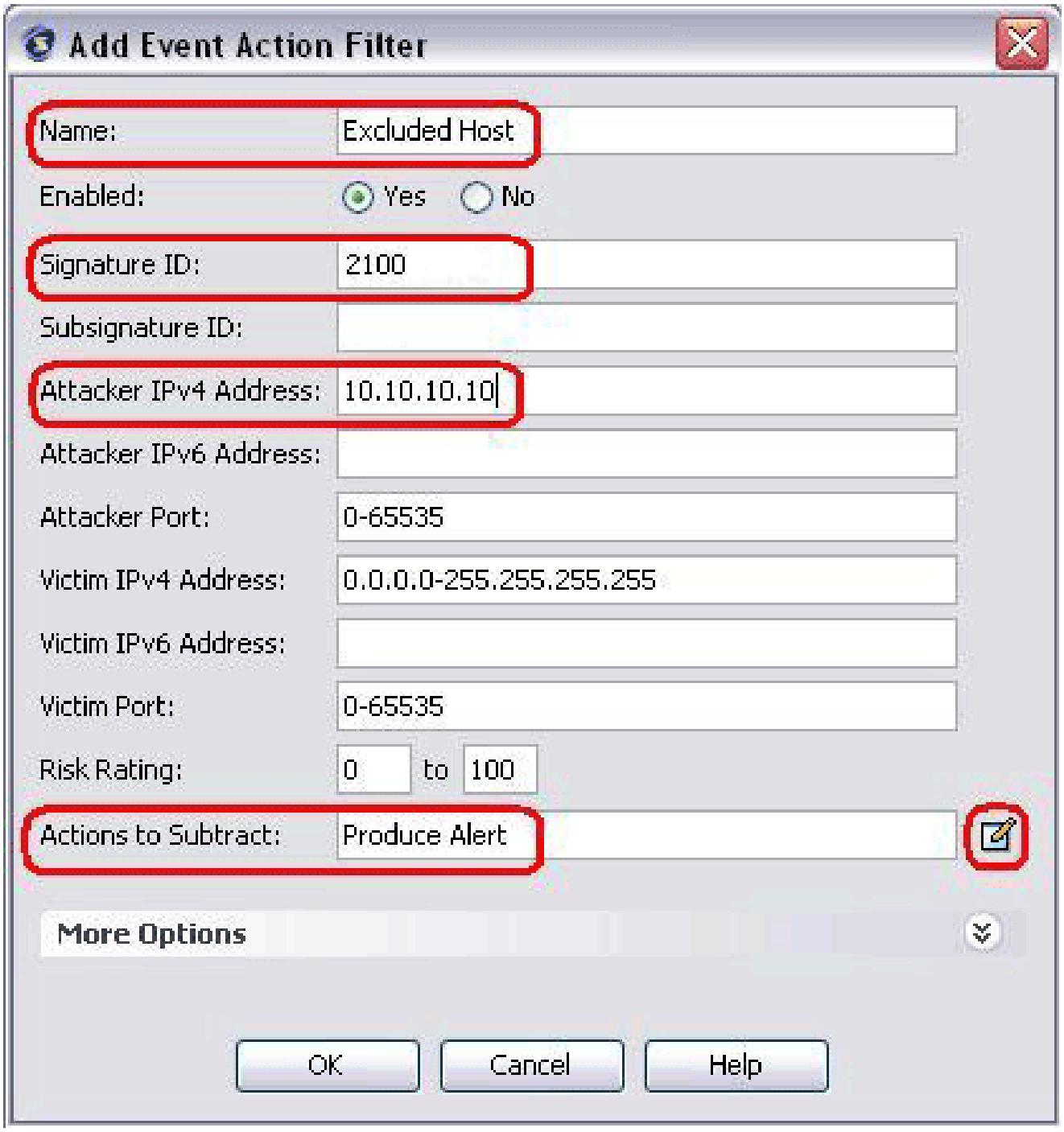
Completare questi passaggi per escludere un host specifico (un indirizzo IP di origine) dalla generazione di un avviso di firma specifico:

1. Scegliere Configurazione > IPS aziendale > Criteri > Regole azione evento > regole0, quindi fare clic sulla scheda Filtri azioni evento.



2. Fare clic su Add.

3. Digitare il nome del filtro, l'ID della firma, l'indirizzo IPv4 dell'autore dell'attacco e l'azione da sottrarre nei campi appropriati, quindi fare clic su OK.



Nota: se è necessario escludere più indirizzi IP da reti diverse, è possibile utilizzare la virgola come delimitatore. Se invece si utilizza la virgola, evitare di inserire uno spazio alla fine della virgola. In caso contrario, potrebbe essere visualizzato un messaggio di errore.

Nota: è inoltre possibile utilizzare le variabili definite nella scheda Variabili evento. Queste variabili sono utili quando lo stesso valore deve essere ripetuto in più filtri azioni evento. È necessario utilizzare il simbolo del dollaro ($) come prefisso per la variabile. La variabile può avere uno dei formati seguenti:

- Indirizzo IP completo; ad esempio, 10.77.23.23.
- Intervallo di indirizzi IP, ad esempio, 10.9.2.10-10.9.2.155.

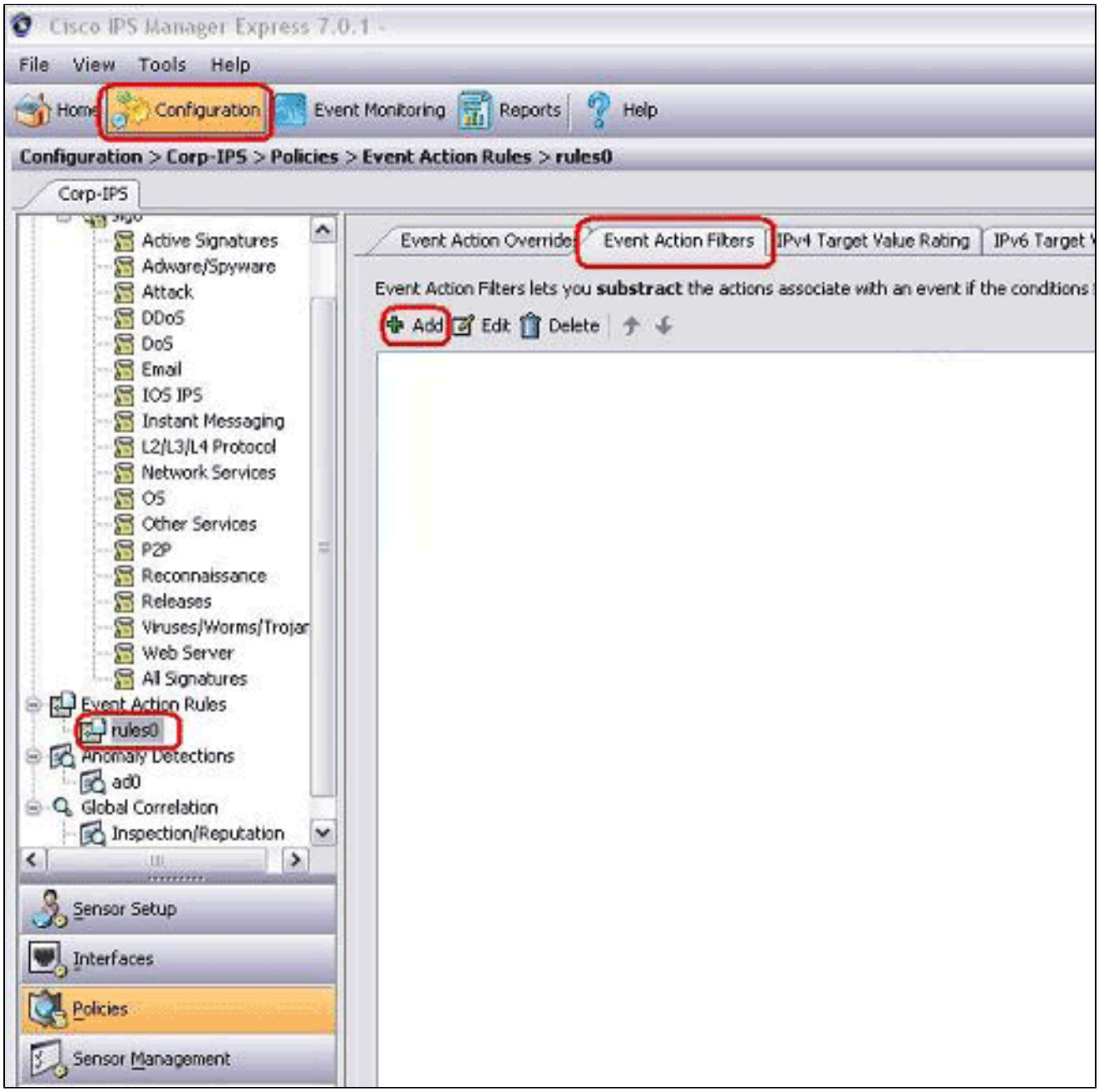
- Gruppo di indirizzi IP: ad esempio, 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11.

Escludi una rete

Il filtro azioni evento esclude inoltre firme specifiche per attivare un allarme in base a un indirizzo di rete di origine o di destinazione.

Completare questi passaggi per escludere una rete dalla generazione di un avviso di firma specifico:

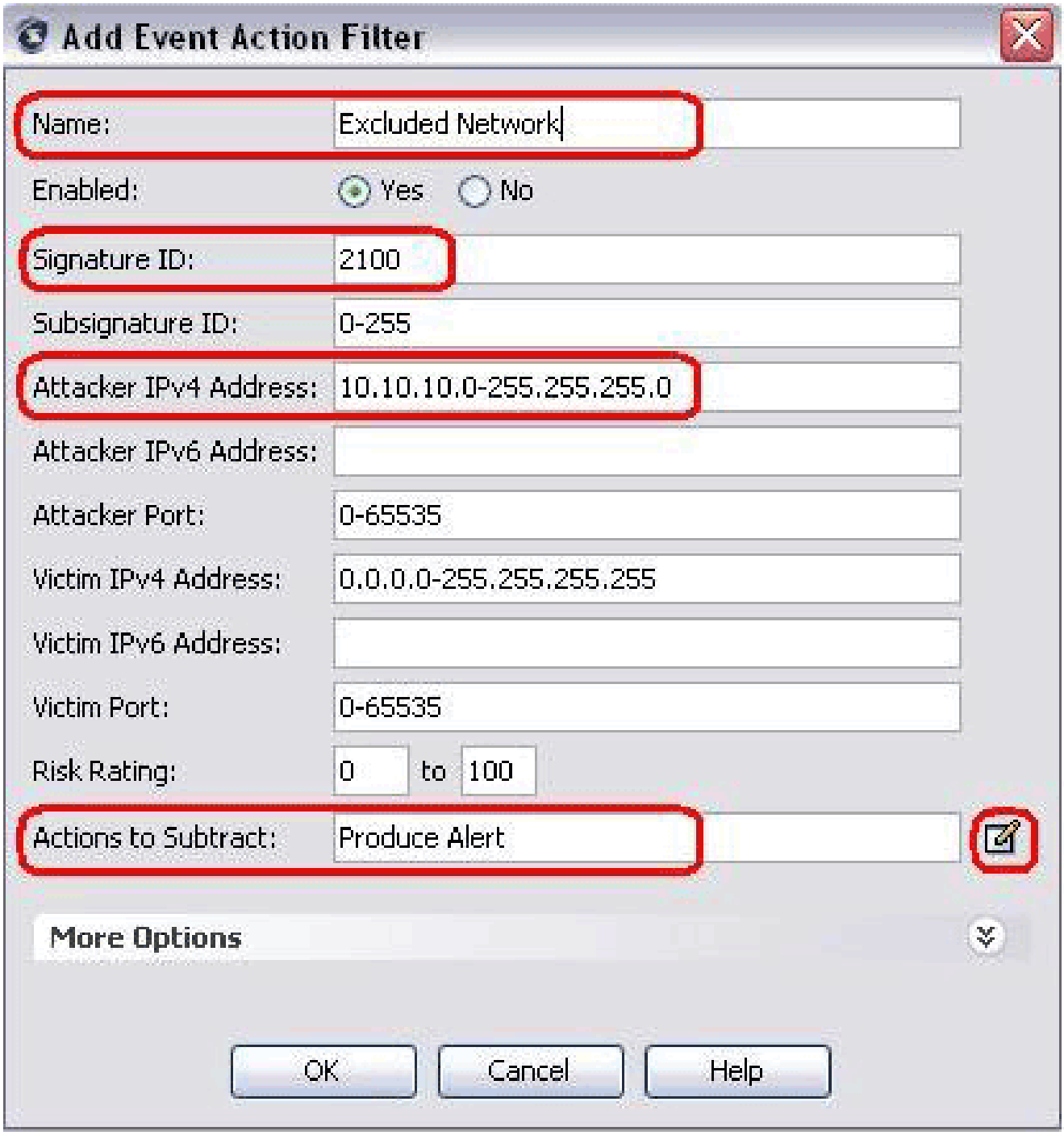
1. Fare clic sulla scheda Filtri azioni eventi.



2. Fare clic su Add.

3. Digitare il nome del filtro, l'ID firma, l'indirizzo di rete con subnet mask e l'azione da sottrarre

nei campi appropriati, quindi fare clic su OK.



Disabilita firme a livello globale

È possibile disattivare l'attivazione di avvisi per una firma in qualsiasi momento. Per abilitare, disabilitare e ritirare le firme, eseguire la procedura seguente:

1. Accedere a IME utilizzando un account con privilegi di amministratore o di operatore.
2. Scegliere Configurazione > nome_sensore > Criteri > Definizioni firme > sig0 > Tutte le firme.
3. Per individuare una firma, scegliere un'opzione di ordinamento dall'elenco a discesa Filtro.

Ad esempio, se si sta cercando una firma ICMP Network Sweep, scegliere Tutte le firme in sig0, quindi eseguire la ricerca per ID o nome della firma. Il riquadro sig0 viene aggiornato e vengono visualizzate solo le firme che corrispondono ai criteri di ordinamento specificati.

4. Per abilitare o disabilitare una firma esistente, scegliere la firma e completare la procedura seguente:

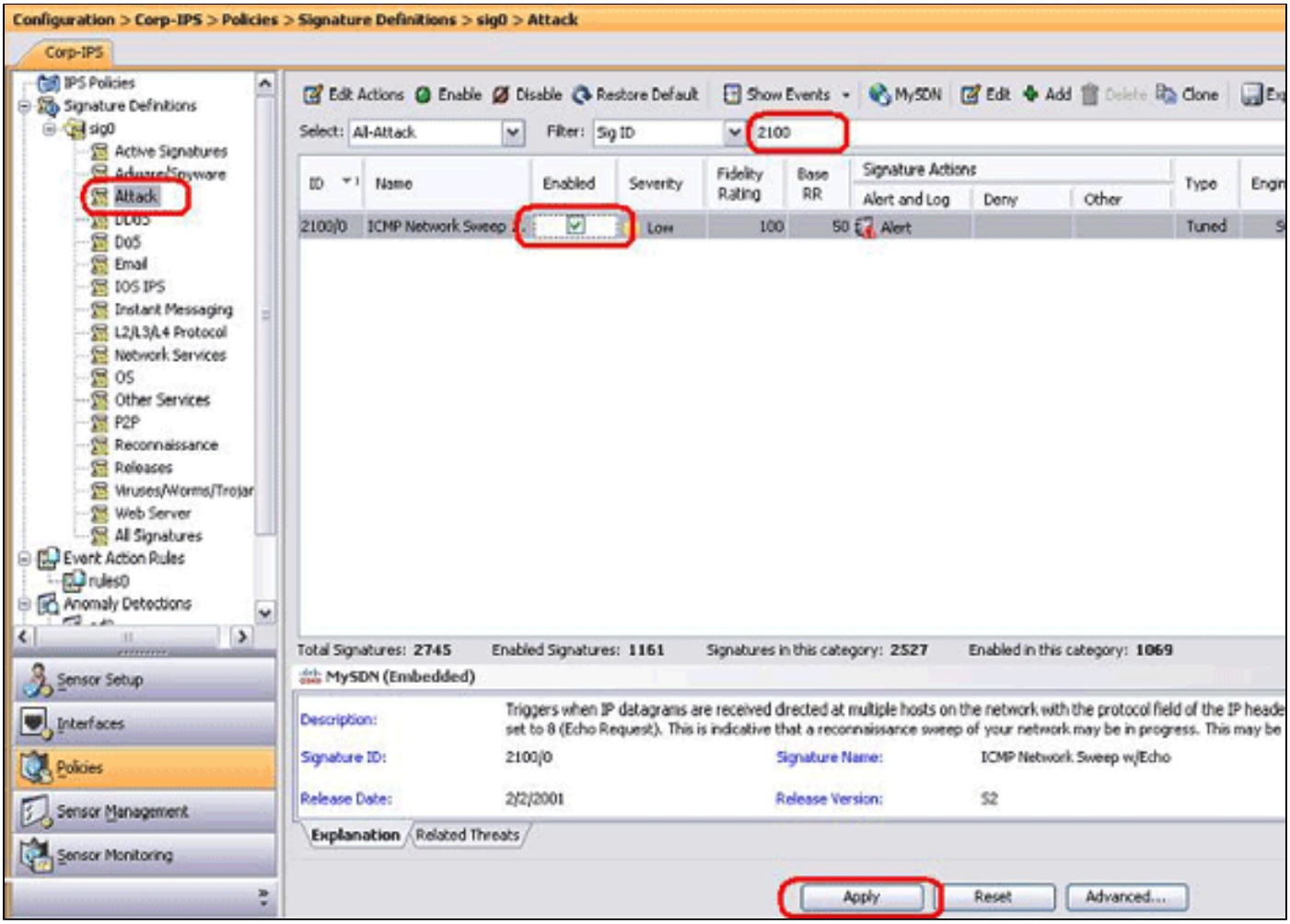
    a. Visualizzare la colonna Attivato per determinare lo stato della firma. Se la firma è attivata, la casella di controllo è selezionata.

    b. Per attivare una firma disattivata, selezionare la casella di controllo Attivata.

    c. Per disattivare una firma abilitata, deselezionare la casella di controllo Abilitato.

    d. Per ritirare una o più firme, scegliere le firme, fare clic con il pulsante destro del mouse e quindi scegliere Cambia stato in > Ritirata.

5. Per applicare le modifiche e salvare la configurazione modificata, fare clic su Apply (Applica).



Informazioni correlate

- [Fine vendita per Cisco Secure IDS Director]

- Pagina di supporto per Cisco Secure Intrusion Detection
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).