Cisco Secure IPS - ohne Fehlalarme

Inhalt

Einführung

Dieses Dokument beschreibt den Ausschluss von Fehlalarmen für das Cisco Secure Intrusion Prevention System (IPS).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Secure Intrusion Prevention System (IPS) Version 7.0 und dem Cisco IPS Manager Express 7.0.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Fehlalarme und falsch negative Alarme

Cisco Secure IPS löst einen Alarm aus, wenn ein bestimmtes Paket oder eine bestimmte Paketsequenz den Eigenschaften bekannter Angriffsprofile entspricht, die in den Cisco Secure IPS-Signaturen definiert sind. Ein wichtiges Design-Kriterium für die IPS-Signatur besteht darin, das Auftreten von falsch positiven und falsch negativen Alarmen zu minimieren.

Fehlalarme (harmlose Auslöser) treten auf, wenn das IPS bestimmte harmlose Aktivitäten als schädlich meldet. Dies erfordert menschliches Eingreifen, um das Ereignis zu diagnostizieren. Eine große Anzahl von Fehlalarmen kann die Ressourcen erheblich beanspruchen, und die für ihre Analyse erforderlichen Fachkenntnisse sind kostspielig und schwer zu finden.

Falsche Negative treten auf, wenn das IPS schädliche Aktivitäten nicht erkennt und nicht meldet. Dies kann katastrophale Folgen haben, und Signaturen müssen fortlaufend aktualisiert werden, sobald neue Exploits und Hacking-Techniken entdeckt werden. Die Minimierung von Fehlalarmen hat eine sehr hohe Priorität, manchmal auf Kosten von Fehlalarmen.

Aufgrund der Art der Signaturen, die IPS zur Erkennung schädlicher Aktivitäten verwenden, ist es nahezu unmöglich, Fehlalarme und -negative vollständig zu beseitigen, ohne die Effektivität des IPS erheblich zu beeinträchtigen oder die Computing-Infrastruktur eines Unternehmens (z. B. Hosts und Netzwerke) erheblich zu unterbrechen. Durch die benutzerdefinierte Anpassung bei der Bereitstellung eines IPS werden Fehlalarme minimiert. Wenn sich die Computing-Umgebung ändert (z. B. wenn neue Systeme und Anwendungen bereitgestellt werden), ist eine regelmäßige Neueinstellung erforderlich. Cisco Secure IPS bietet eine flexible Anpassungsfunktion, mit der Fehlalarme bei Dauerbetrieb minimiert werden können.

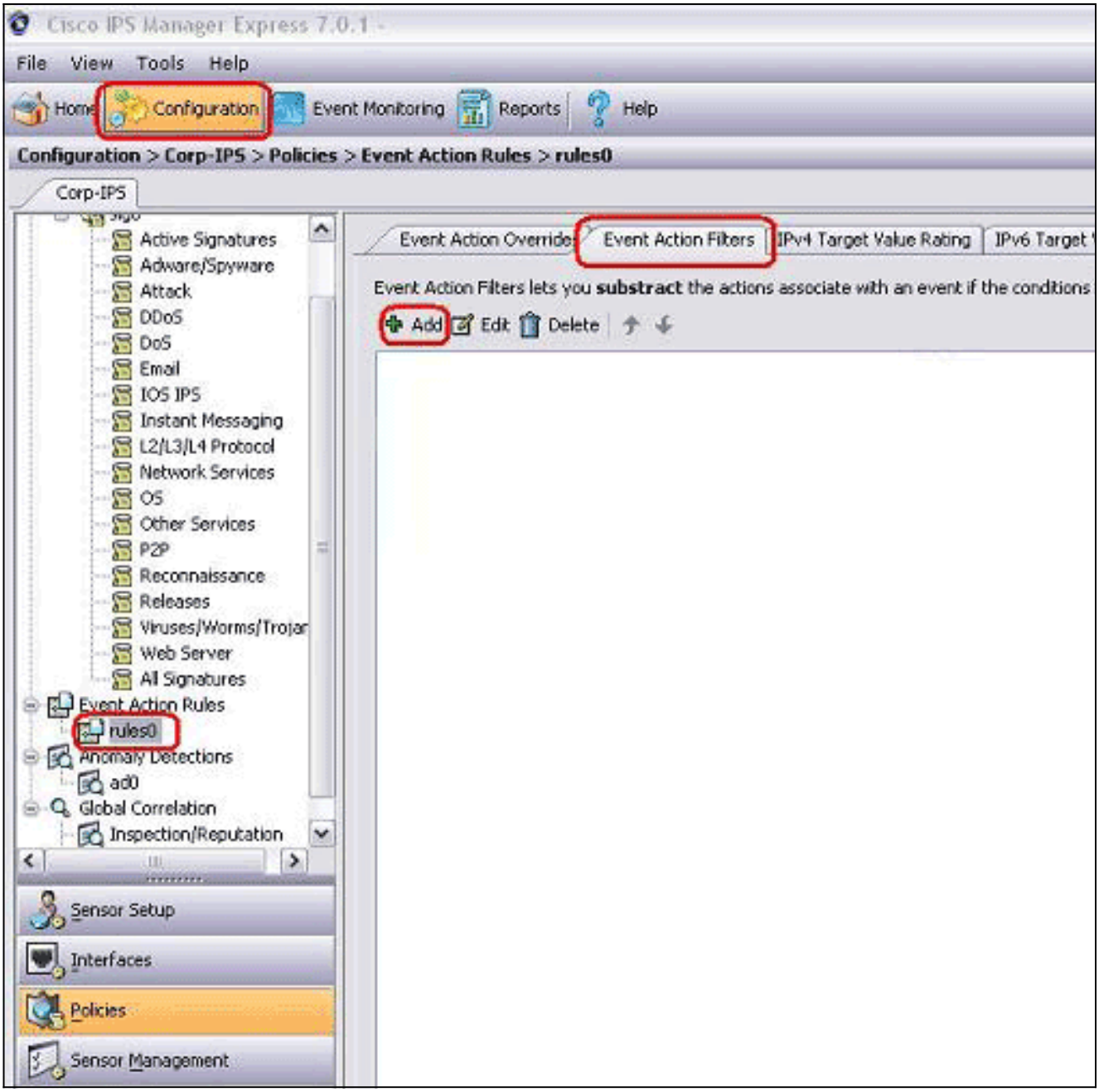
Cisco Secure IPS Exklusivmechanismus

Cisco Secure IPS bietet die Möglichkeit, eine bestimmte Signatur von oder zu einem bestimmten Host oder einer bestimmten Netzwerkadresse auszuschließen. Ausgeschlossene Signaturen generieren keine Alarmsymbole oder Protokolldatensätze, wenn sie von Hosts oder Netzwerken ausgelöst werden, die durch diesen Mechanismus ausdrücklich ausgeschlossen sind. Beispielsweise kann eine Netzwerkmanagementstation eine Netzwerkerkennung durchführen, indem sie Ping-Sweeps ausführt, die den ICMP-Netzwerk-Sweep mit Echo-Signatur (Signatur-ID 2100) auslösen. Wenn Sie die Signatur ausschließen, müssen Sie den Alarm nicht jedes Mal analysieren und löschen, wenn der Netzwerkerkennungsvorgang ausgeführt wird.

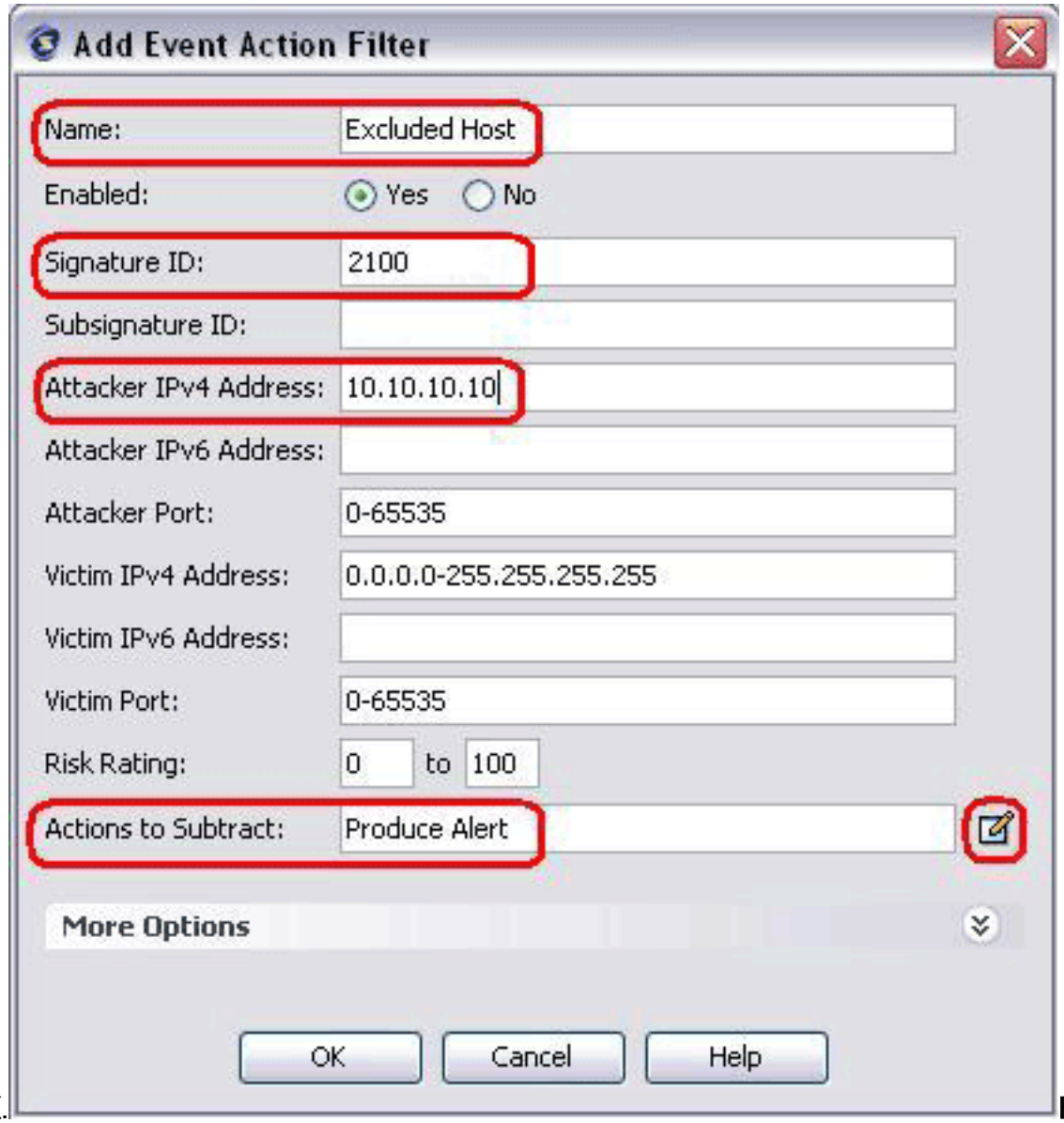
Ausschließen eines Hosts

Führen Sie diese Schritte aus, um einen bestimmten Host (eine Quell-IP-Adresse) von der Generierung eines bestimmten Signaturalarms auszuschließen:

1. Wählen Sie **Configuration > Corp-IPS > Policies > Event Action Rules > rules0 aus**, und klicken Sie auf die Registerkarte **Event Action Filters (Ereignisreaktionsfilter)**.



2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den Filternamen, die Signatur-ID, die IPv4-Adresse des Angreifers und die Aktion zum Subtrahieren in die entsprechenden Felder ein, und klicken Sie dann auf



OK.**Hinweis:** Wenn Sie mehrere IP-Adressen aus verschiedenen Netzwerken ausschließen müssen, können Sie das Komma als Trennzeichen verwenden. Wenn Sie jedoch ein Komma verwenden, vermeiden Sie das nachfolgende Leerzeichen nach dem Komma. Andernfalls erhalten Sie möglicherweise einen Fehler.**Hinweis:** Darüber hinaus können Sie die in der Registerkarte Ereignisvariablen definierten Variablen verwenden. Diese Variablen sind nützlich, wenn derselbe Wert in mehreren Ereignisreaktionsfiltern wiederholt werden muss. Sie müssen ein Dollarzeichen ($) als Präfix für die Variable verwenden. Die Variable kann eines der folgenden Formate sein:Vollständige IP-Adresse; beispielsweise 10.77.23.23.Bereich der IP-Adressen; beispielsweise 10.9.2.10-10.9.2.155.Bereich der IP-Adressen Beispiel: 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11.

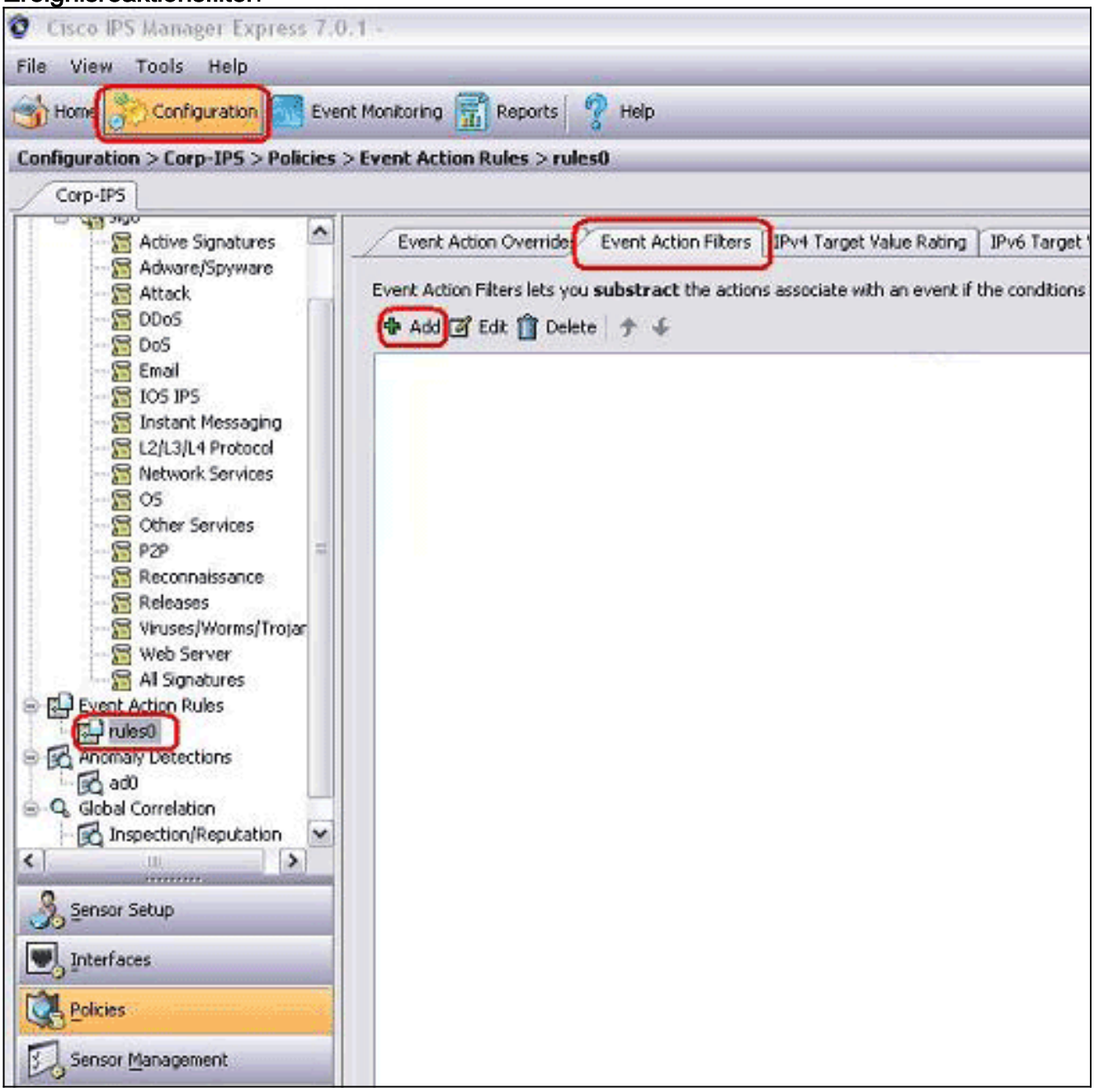
Netzwerk ausschließen

Der Ereignisreaktionsfilter schließt auch bestimmte Signaturen aus, um einen Alarm basierend auf einer Quell- oder Zielnetzwerkadresse auszulösen.

Gehen Sie wie folgt vor, um zu verhindern, dass ein Netzwerk einen bestimmten Signaturalarm auslöst:

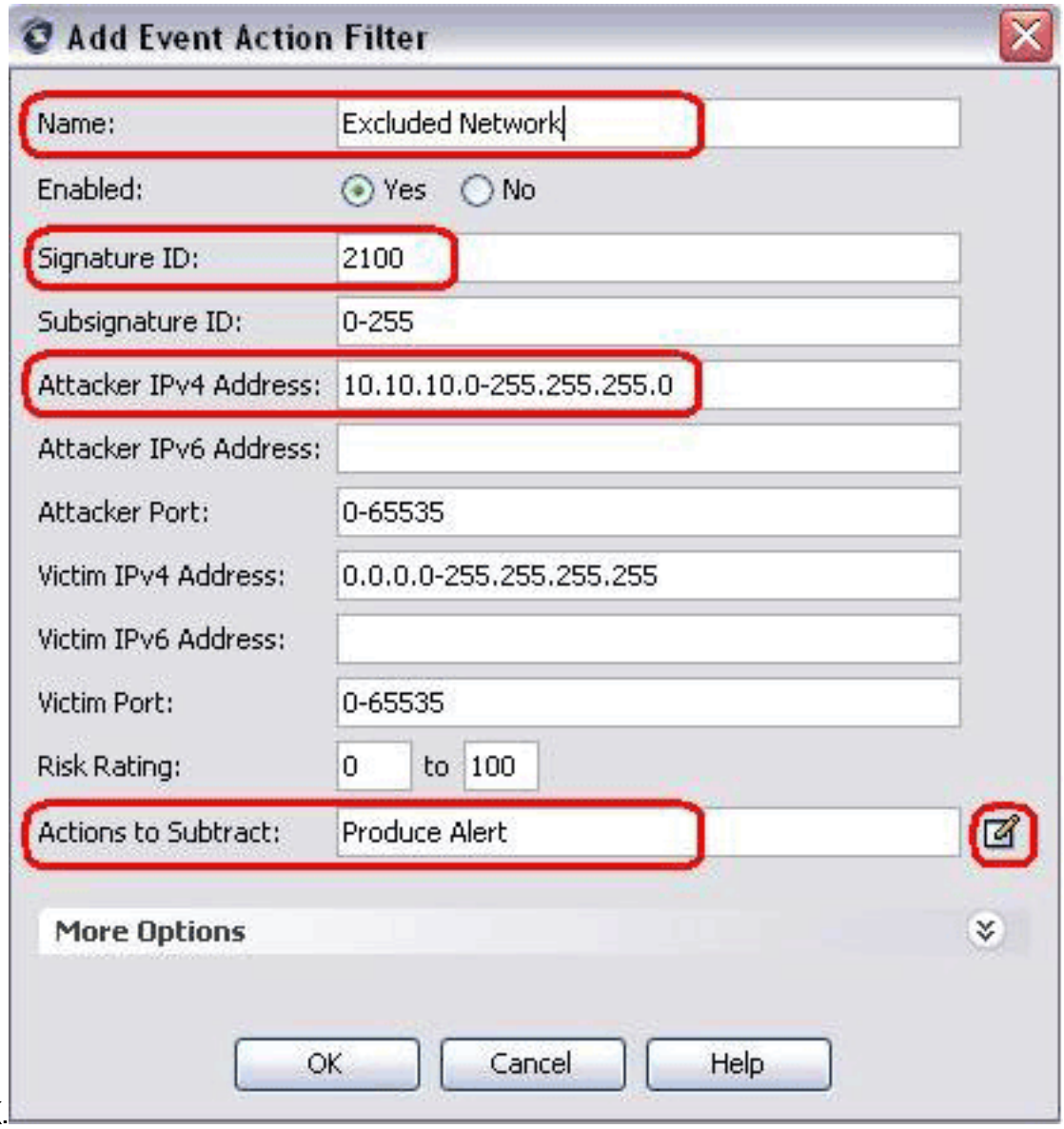
1. Klicken Sie auf die Registerkarte

Ereignisreaktionsfilter.



2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den Filternamen, die Signatur-ID, die Netzwerkadresse mit Subnetzmaske und die Aktion ein, die in die entsprechenden Felder subtrahiert werden soll, und klicken Sie dann

auf **OK**.



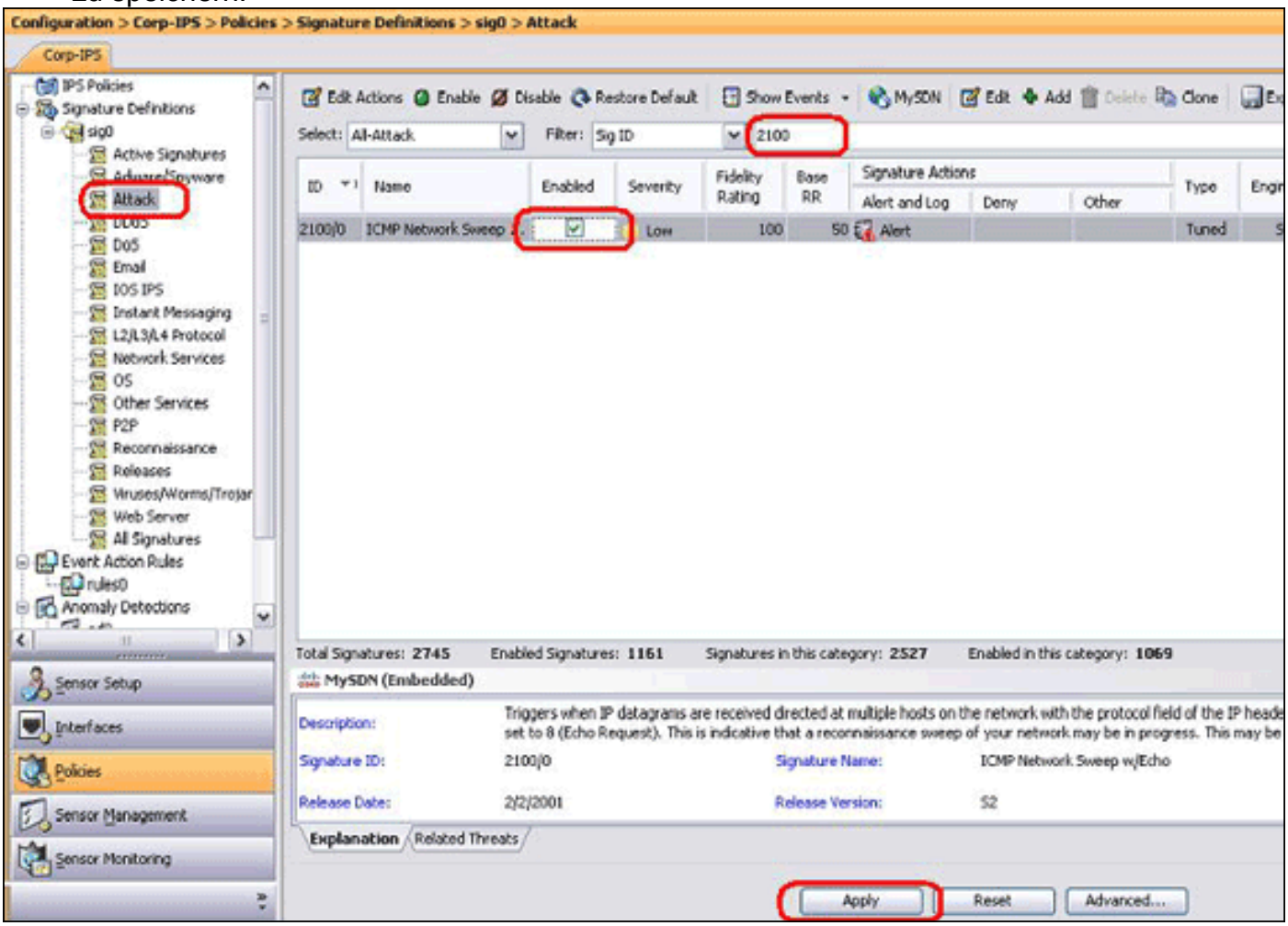
Signaturen global deaktivieren

Sie können eine Signatur jederzeit von der Alarming deaktivieren. Gehen Sie wie folgt vor, um Signaturen zu aktivieren, zu deaktivieren und zu löschen:

1. Melden Sie sich bei IME mit einem Konto mit Administrator- oder Operatorberechtigungen an.
2. Wählen Sie **Configuration > sensor_name > Policies > Signature Definitions > sig0 > All Signatures aus.**
3. Um eine Signatur zu suchen, wählen Sie in der Dropdown-Liste Filter (Filter) eine Sortieroption aus. Wenn Sie z. B. nach einer ICMP-Netzwerk-Sweep-Signatur suchen, wählen Sie **Alle Signaturen** unter sig0 aus, und suchen Sie dann nach der Signatur-ID oder dem Namen. Der sig0-Bereich wird aktualisiert und nur die Signaturen angezeigt, die Ihren Sortierkriterien entsprechen.
4. Um eine vorhandene Signatur zu aktivieren oder zu deaktivieren, wählen Sie die Signatur aus, und führen Sie die folgenden Schritte aus:Zeigen Sie die Spalte Aktiviert an, um den Status der Signatur zu bestimmen. Bei einer aktivierten Signatur ist das Kontrollkästchen aktiviert.Um eine Signatur zu aktivieren, die deaktiviert ist, aktivieren Sie das Kontrollkästchen **Aktiviert**.Um eine aktivierte Signatur zu deaktivieren, deaktivieren Sie das

Kontrollkästchen **Aktiviert**.Um eine oder mehrere Signaturen außer Kraft zu setzen, wählen Sie die Signatur(en) aus, klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Status ändern zu > Zurückgesetzt**.

5. Klicken Sie auf **Apply**, um Ihre Änderungen anzuwenden und die überarbeitete Konfiguration zu speichern.



Zugehörige Informationen

- Vertriebsende für Cisco Secure IDS Director
- Support-Seite für Cisco Secure Intrusion Detection
- Technischer Support und Dokumentation - Cisco Systems