Cisco Secure IPS – Exclusion des alarmes de faux positifs

Contenu

Introduction

Ce document décrit l'exclusion des alarmes de faux positif pour le Système de prévention d'intrusion (IPS) Cisco Secure.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 7.0 Cisco Secure et le Cisco IPS Manager Express 7.0 de Système de prévention d'intrusion (IPS).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Alarmes de faux positif et de faux négatif

L'IPS Cisco Secure déclenche une alarme quand un paquet ou un ordre donné des paquets apparie les caractéristiques des profils d'attaque connue définis dans les signatures IPS Cisco Secures. Un critère de conception essentiel de signature IPS est de réduire l'occurrence des alarmes de faux positif et de faux négatif.

Les faux positifs (déclencheurs bénins) se produisent quand l'IPS signale certaine activité bénigne comme malveillante. Ceci exige de l'intervention humaine de diagnostiquer l'événement. Un grand nombre de faux positifs peuvent de manière significative vider des ressources, et les qualifications spécialisées exigées de les analyser sont coûteuses et difficiles aux trouver.

Les faux négatifs se produisent quand l'IPS ne détecte pas et signale l'action malveillante réelle. La conséquence de ceci peut être catastrophique et des signatures doivent être continuellement mises à jour pendant que de nouvelles exploits et techniques de entailler sont découvertes. Réduire des faux négatifs est accordé très un prioritaire, parfois aux dépens des occurrences plus élevées des faux positifs.

En raison de la nature des signatures que l'utilisation d'IPSs de détecter l'action malveillante, il est presque impossible d'éliminer complètement des faux positifs et des négatifs sans dégrader sévèrement l'efficacité de l'IPS ou perturber sévèrement l'infrastructure calculante d'une organisation (telle que des hôtes et des réseaux). Customized accordant quand un IPS est déployé réduit des faux positifs. Réaccorder périodique est exigé quand l'environnement informatique change (par exemple, quand de nouveaux systèmes et applications sont déployés). L'IPS Cisco Secure fournit une capacité de accord flexible qui peut réduire des faux positifs pendant des exécutions équilibrées.

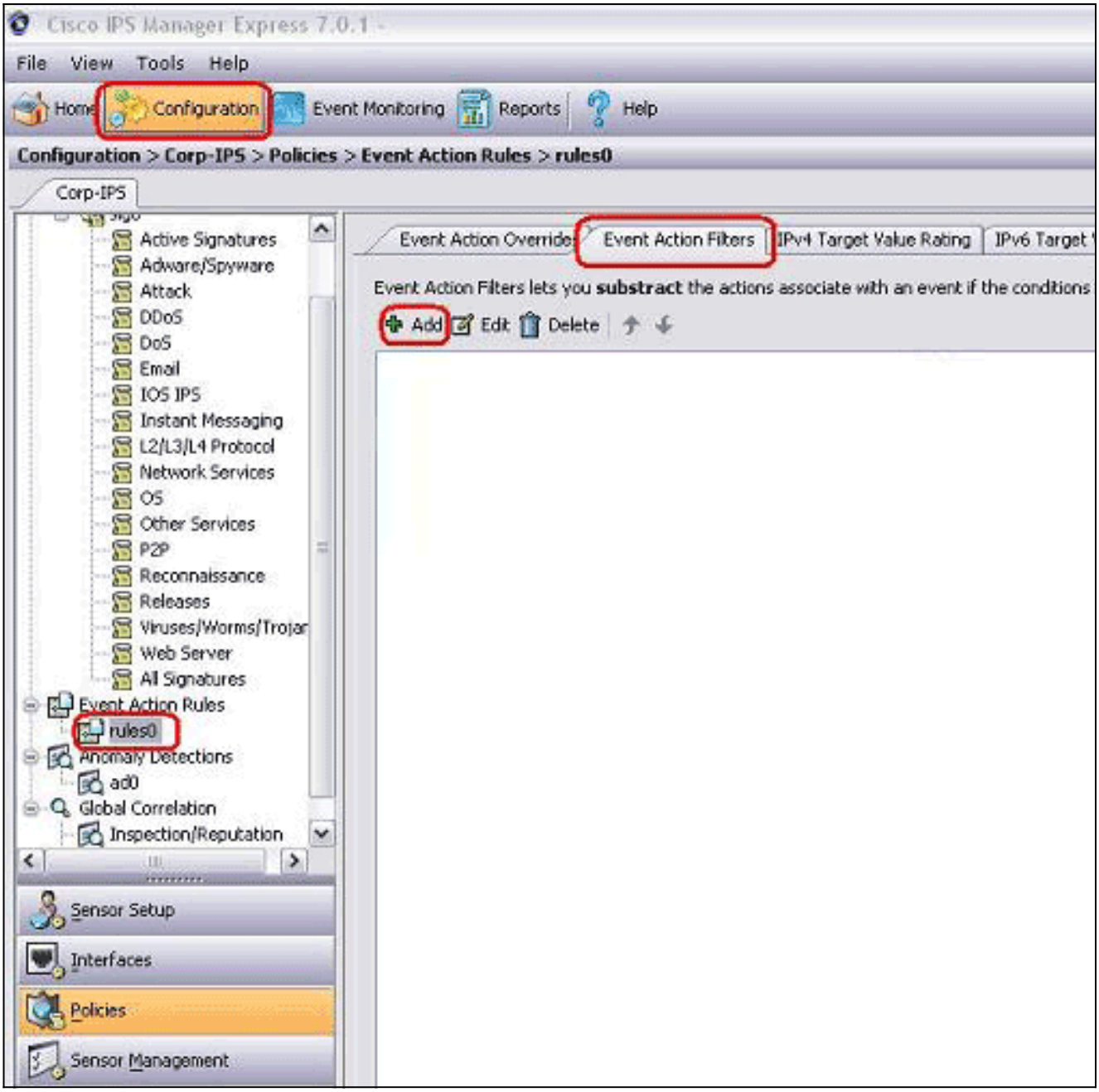
Les IPS Cisco Secures excluent le mécanisme

L'IPS Cisco Secure fournit la capacité pour exclure une signature spécifique ou derrière un hôte spécifique ou derrière des adresses réseau. Les signatures exclues ne génèrent pas des icônes d'alarme ou se connectent des enregistrements quand elles sont déclenchées des hôtes ou des réseaux qui sont spécifiquement exclus par ce mécanisme. Par exemple, une station de Gestion de réseau pourrait exécuter la détection de réseau par les balayages pings d'exécution, qui déclenchent le champ de réseau d'ICMP avec la signature d'écho (ID 2100 de signature). Si vous excluez la signature, vous ne devez pas analyser l'alarme et la supprimer chaque fois que le processus de découverte de réseau fonctionne.

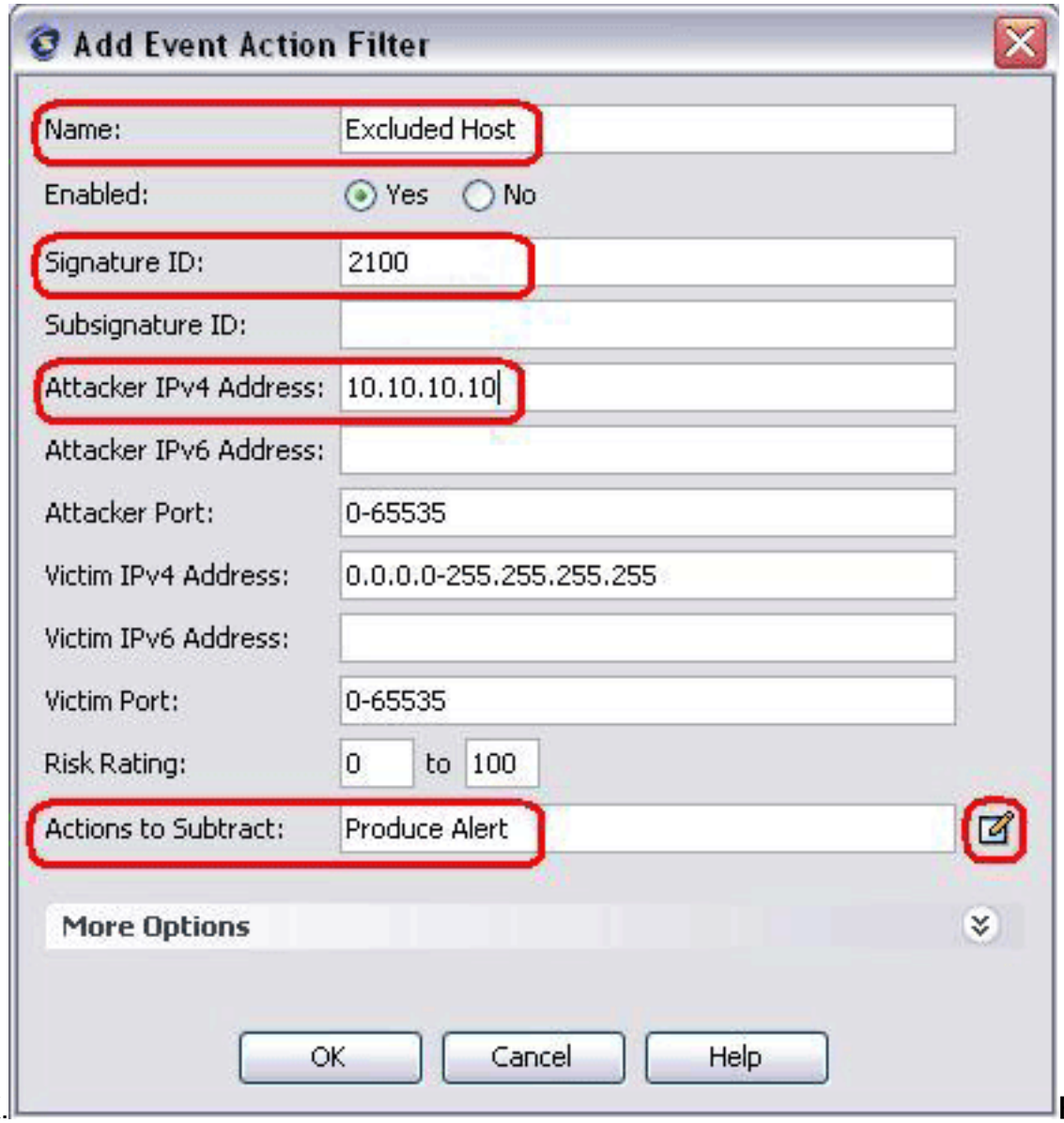
Excluez un hôte

Terminez-vous ces étapes afin d'exclure un hôte spécifique (une adresse IP source) de générer une alarme spécifique de signature :

1. Choisissez la **configuration > le Corp.-IPS > les stratégies > les règles d'action d'événement > le rules0**, et cliquez sur l'onglet de **filtres d'action d'événement**.



2. Cliquez sur **Add**.
3. Tapez le nom du filtre, l'ID de signature, l'ipv4 addres de l'attaquant, et l'action de soustraire dans les champs appropriés, et puis cliquez sur



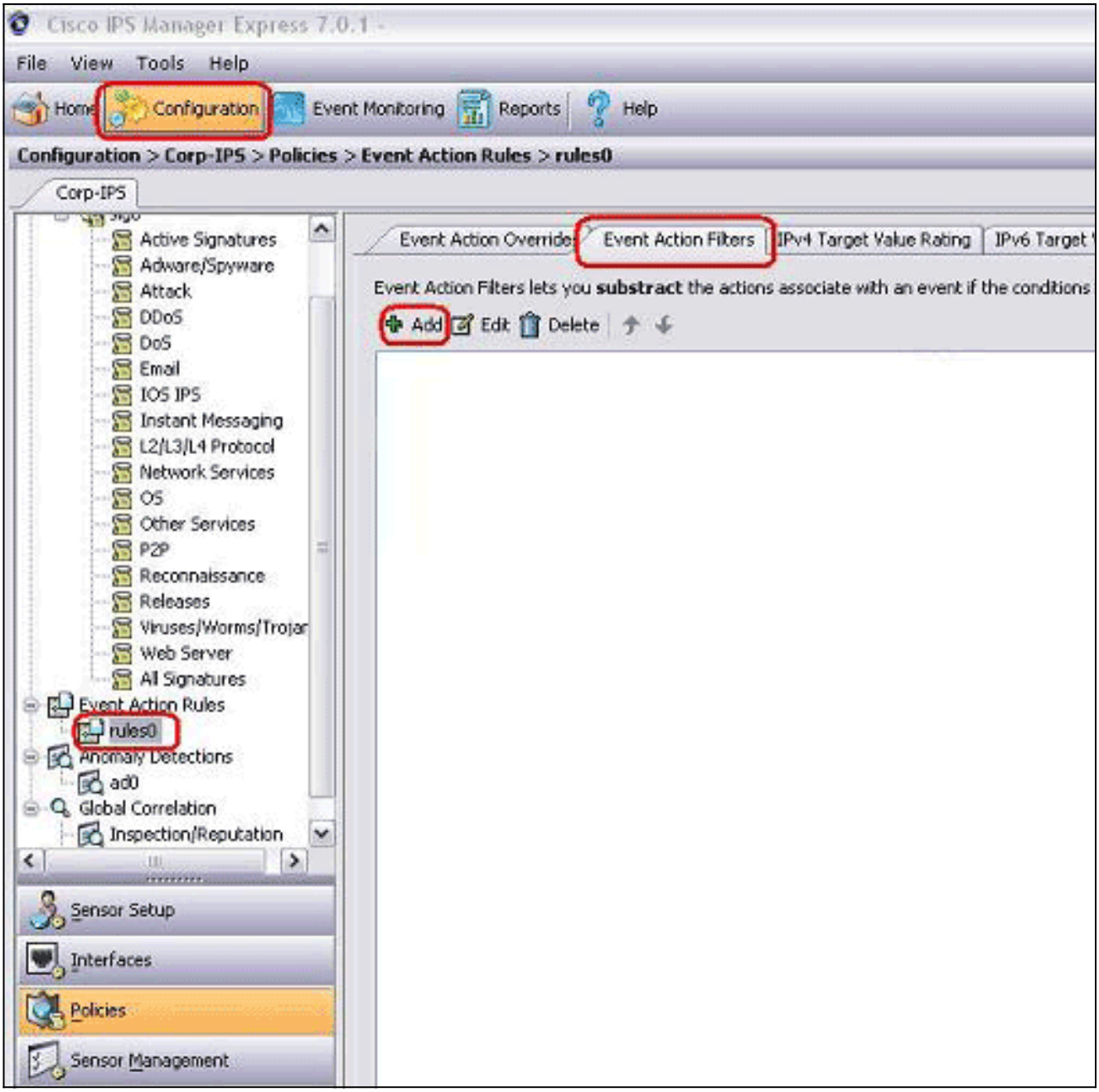
OK.**Remarque:** Si vous devez exclure de plusieurs adresses IP de différents réseaux, vous pouvez utiliser la virgule comme délimiteur. Cependant, si vous utilisez une virgule, évitez l'espace de remorquage après la virgule ; autrement, vous pourriez recevoir une erreur.**Remarque:** En outre, vous pouvez utiliser en cas l'onglet de variables défini par variables. Ces variables sont utiles quand la même valeur doit être répétée dans de plusieurs filtres d'action d'événement. Vous devez utiliser un symbole dollar ($) comme préfixe à la variable. La variable peut être l'un de ces formats :Pleine adresse IP ; par exemple, 10.77.23.23.Plage des adresses IP ; par exemple, 10.9.2.10-10.9.2.155.Ensemble de plage des adresses IP ; par exemple, 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11.

Excluez un réseau

Le filtre d'action d'événement exclut également les signatures spécifiques pour se déclencher une alarme basée sur une source ou une adresse réseau de destination.

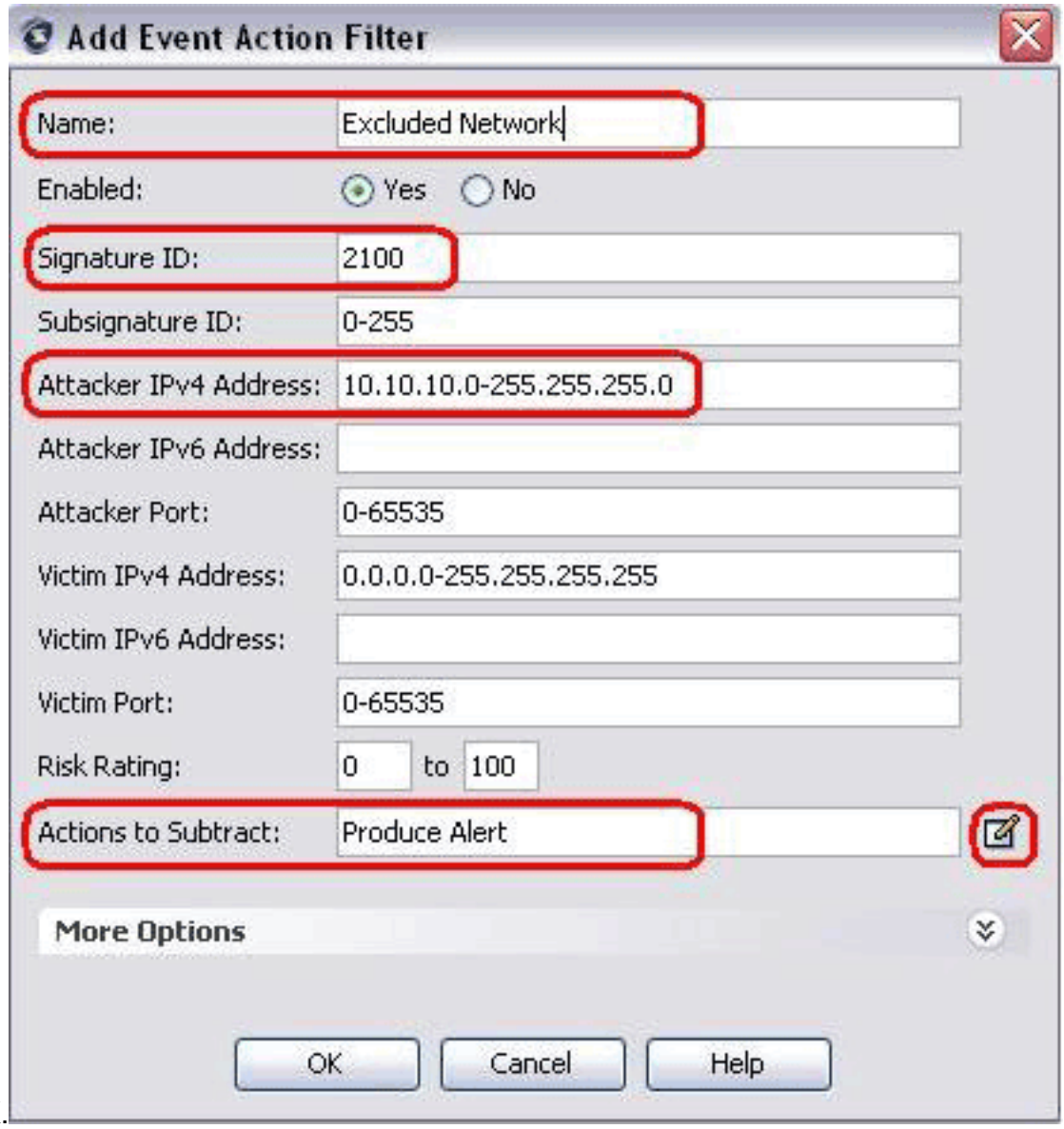
Terminez-vous ces étapes afin d'exclure un réseau de générer une alarme spécifique de signature :

1. Cliquez sur l'onglet de **filtres d'action d'événement**.



2. Cliquez sur **Add**.
3. Tapez le nom du filtre, l'ID de signature, l'adresse réseau avec le masque de sous-réseau, et l'action de soustraire dans les champs appropriés, et puis cliquez sur

OK.

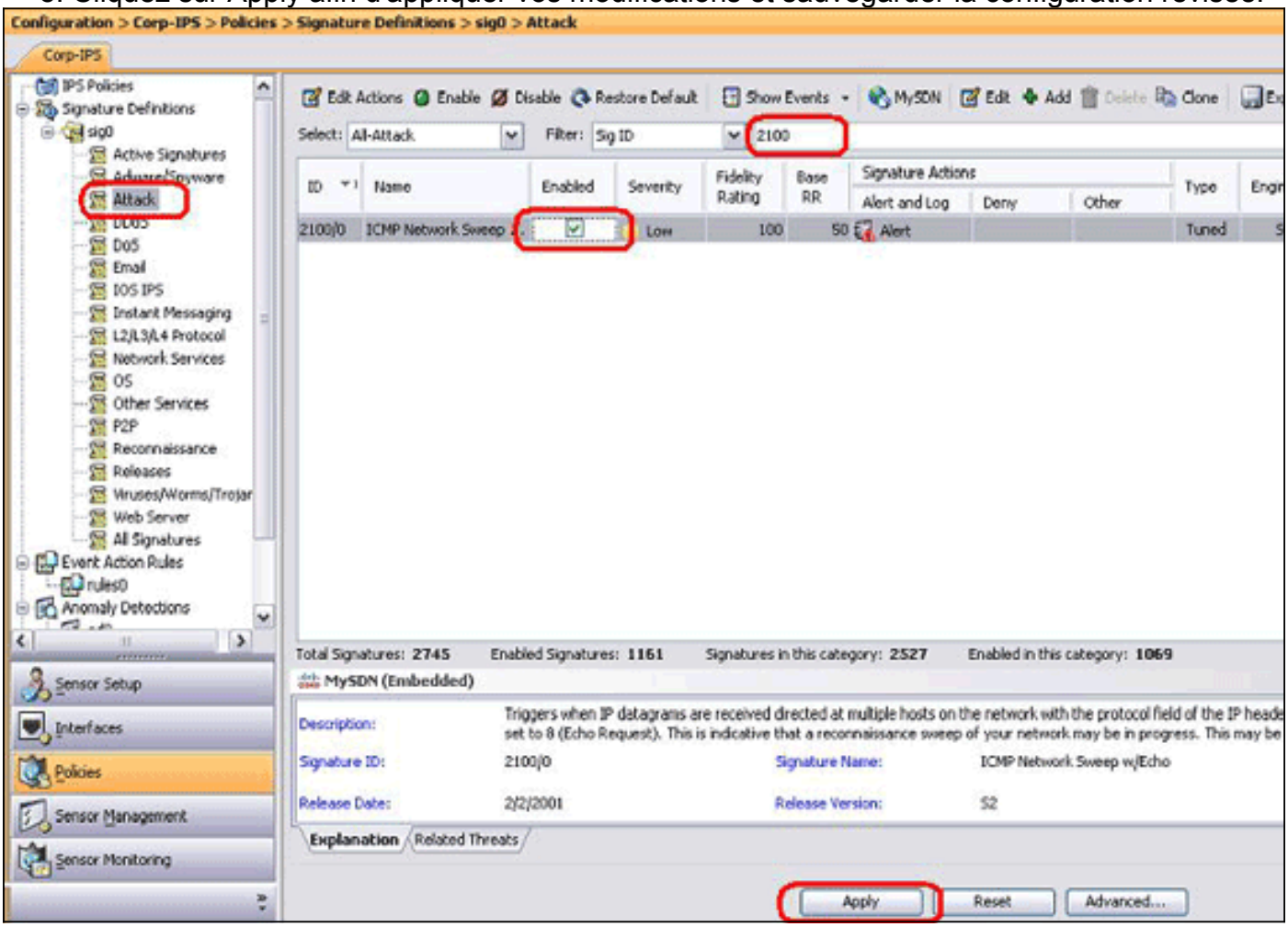


Globalement signatures de débronchement

Vous pourriez vouloir désactiver une signature de l'alarme à tout moment. Afin d'activer, désactiver, et retirer des signatures, terminez-vous ces étapes :

1. Ouvrez une session à IME utilisant un compte avec des privilèges d'administrateur ou d'opérateur.
2. Choisissez la **configuration** > le **sensor_name** > les **stratégies** > les **définitions de signature** > le **sig0** > **toutes les signatures**.
3. Afin de localiser une signature, choisissez une option la triant de la liste déroulante de filtre. Par exemple, si vous recherchez une signature de champ de réseau d'ICMP, choisissez **toutes les signatures** sous sig0, puis les recherchez par ID ou nom de signature. Le volet sig0 régénère et affiche seulement ces signatures qui apparient vos critères les triant.
4. Afin d'activer ou désactiver une signature existante, choisissez la signature, et terminez-vous ces étapes :Visualisez la colonne activée pour déterminer l'état de la signature. Une signature qui est activée a la case cochée.Afin d'activer une signature qui est désactivée, cochez la case **activée**.Afin de désactiver une signature qui est activée, décochez la case **activée**.Afin de retirer un ou plusieurs signatures, choisissez les signatures, cliquez avec le bouton droit, et puis cliquez sur l'**état de modification à > retiré**.

5. Cliquez sur Apply afin d'appliquer vos modifications et sauvegarder la configuration révisée.



Informations connexes

- Fin de vente pour le Cisco Secure IDS Director
- Page Cisco Secure de prise en charge de la détection d'intrusion
- Support et documentation techniques - Cisco Systems