Cisco Secure IPS - zonder valse positieve alarmen

Inhoud

Inleiding

Dit document beschrijft de uitsluiting van valse positieve alarmen voor Cisco Secure Inbraakpreventiesysteem (IPS).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure Inbraakpreventiesysteem (IPS) versie 7.0 en Cisco IPS Manager Express 7.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Fout-positieve en fout-negatieve alarmen

Cisco Secure IPS activeert een alarm wanneer een bepaald pakket of een bepaalde reeks pakketten overeenkomt met de kenmerken van bekende aanvalsprofielen die in de beveiligde IPS van Cisco-handtekeningen zijn gedefinieerd. Een kritisch IPS-handtekeningsontwerpcriterium is het optreden van valse positieve en valse negatieve alarmen tot een minimum te beperken.

Valse positieven (benigne triggers) doen zich voor wanneer IPS bepaalde benigne activiteit als kwaadaardig rapporteert. Dit vergt menselijk ingrijpen om de diagnose te stellen. Een groot aantal fout-positieven kan aanzienlijk middelen wegpompen, en de gespecialiseerde vaardigheden die nodig zijn om ze te analyseren zijn duur en moeilijk te vinden.

Vals negatieven komen voor wanneer IPS geen daadwerkelijke kwaadaardige activiteit ontdekt en rapporteert. Dit kan rampzalige gevolgen hebben en de handtekeningen moeten voortdurend worden bijgewerkt naarmate er nieuwe exploits en hacktechnieken worden ontdekt. Het minimaliseren van valse negatieven krijgt een zeer hoge prioriteit, soms ten koste van hogere gevallen van valse positieven.

Vanwege de aard van de handtekeningen die IPSs gebruiken om kwaadaardige activiteit te detecteren, is het bijna onmogelijk om valse positieven en negatieve punten volledig te elimineren zonder de effectiviteit van IPS ernstig te ondermijnen of de computerinfrastructuur van een organisatie (zoals hosts en netwerken) ernstig te verstoren. Aangepaste afstemming wanneer een IPS wordt geïmplementeerd minimaliseert valse positieven. Periodieke afstemming is vereist wanneer de computeromgeving verandert (bijvoorbeeld wanneer nieuwe systemen en toepassingen worden geïmplementeerd). Cisco Secure IPS biedt een flexibele afstemmingsmogelijkheid die valse positieven kan minimaliseren tijdens steady-state-bewerkingen.

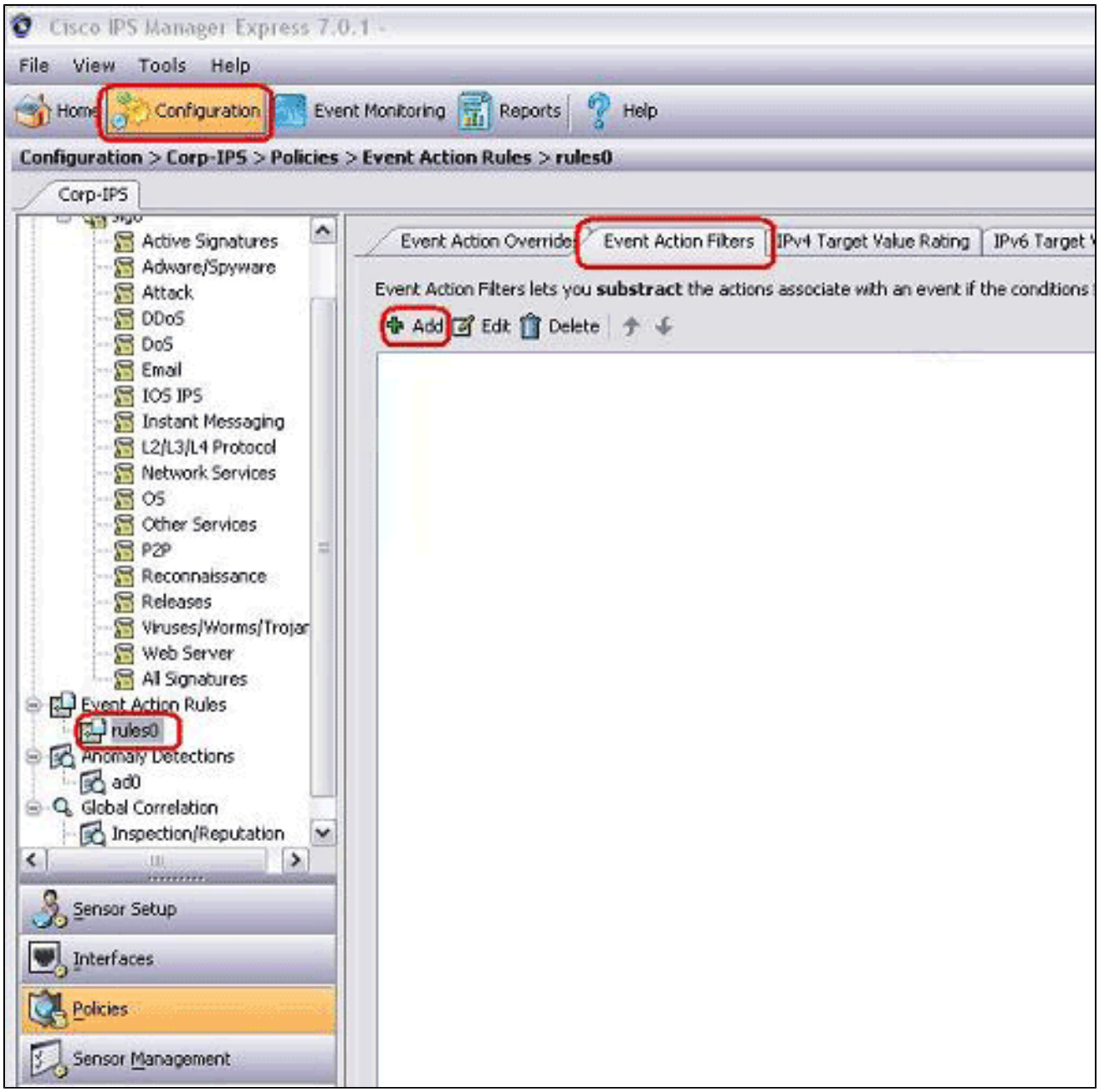
Het mechanisme van uitsluiting van Cisco Secure IPS

Cisco Secure IPS biedt de mogelijkheid om een specifieke handtekening uit te sluiten van of naar een specifieke host- of netwerkadressen. Uitgesloten handtekeningen genereren geen alarmpictogrammen of logrecords wanneer ze worden geactiveerd vanaf de hosts of netwerken die specifiek zijn uitgesloten via dit mechanisme. Een netwerkbeheerstation kan bijvoorbeeld netwerkdetectie uitvoeren door pingsweeps uit te voeren, die de ICMP-netwerksweep met Echo-handtekening (handtekening-ID 2100) activeren. Als u de handtekening uitsluit, hoeft u het alarm niet te analyseren en te verwijderen telkens wanneer het netwerkdetectieproces wordt uitgevoerd.

Een host uitsluiten

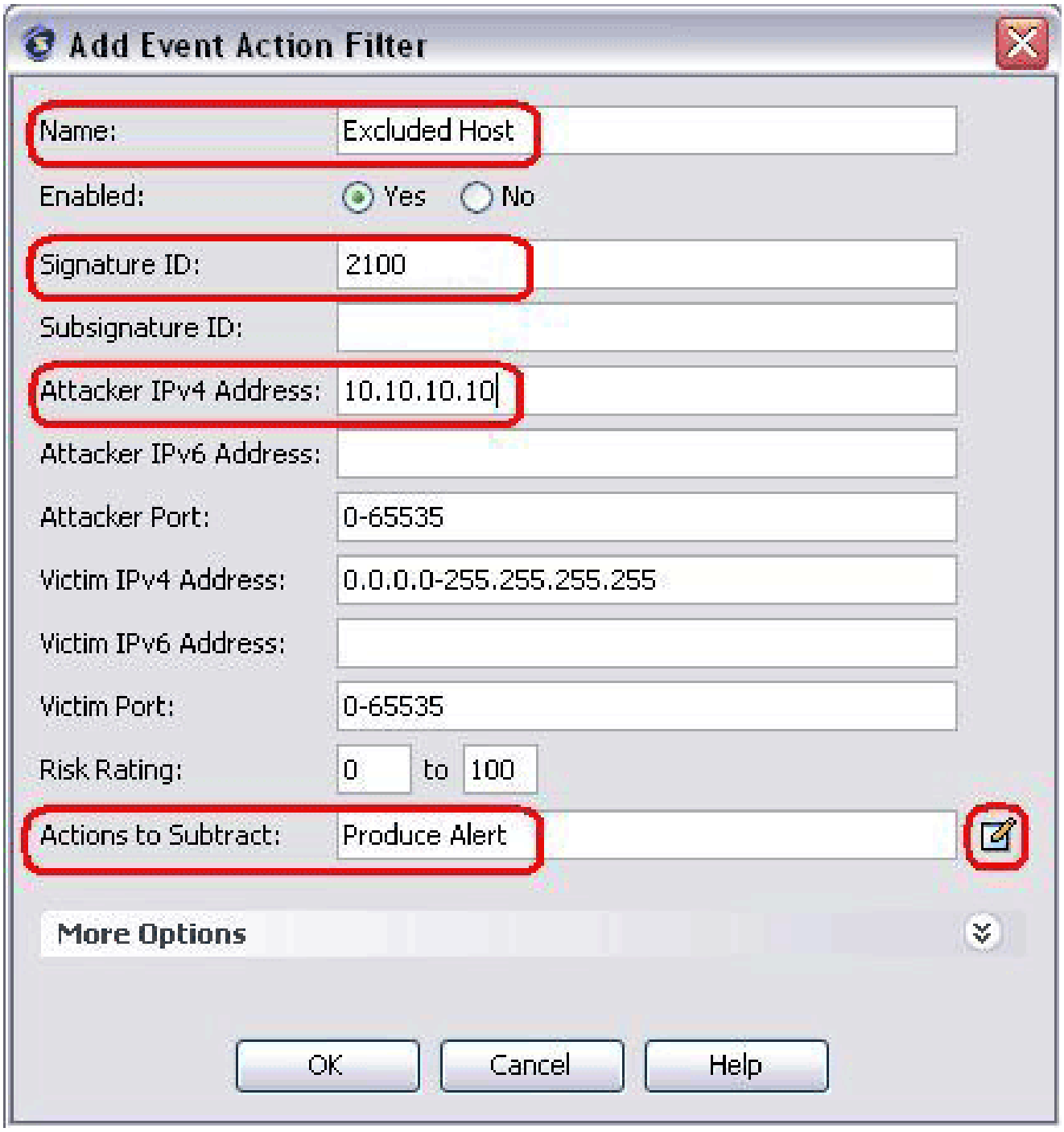
Voltooi deze stappen om een specifieke gastheer (een bron IP adres) van het produceren van een specifiek handtekeningsalarm uit te sluiten:

1. Kies Configuratie > Corp-IPS > Beleid > Regels voor Gebeurtenis > Regels0, en klik op het tabblad Filters voor Gebeurtenis.



2. Klik op Add (Toevoegen).

3. Typ de filternaam, handtekening-ID, IPv4-adres van de aanvaller en actie om af te trekken in de betreffende velden en klik vervolgens op OK.



Opmerking: als u meerdere IP-adressen van verschillende netwerken wilt uitsluiten, kunt u de komma als scheidingsteken gebruiken. Als u echter een komma gebruikt, vermijdt u de ruimte achter de komma; anders krijgt u mogelijk een fout.

Opmerking: Daarnaast kunt u de variabelen gebruiken die zijn gedefinieerd in het tabblad Gebeurtenisvariabelen. Deze variabelen zijn nuttig wanneer dezelfde waarde moet worden herhaald in meerdere gebeurtenisactiefilters. U moet een dollarteken ($) gebruiken als voorvoegsel voor de variabele. De variabele kan één van deze formaten zijn:

- Volledig IP-adres, bijvoorbeeld 10.7.23.23.
- Bereik van IP-adressen, bijvoorbeeld 10.9.2.10-10.9.2.15.

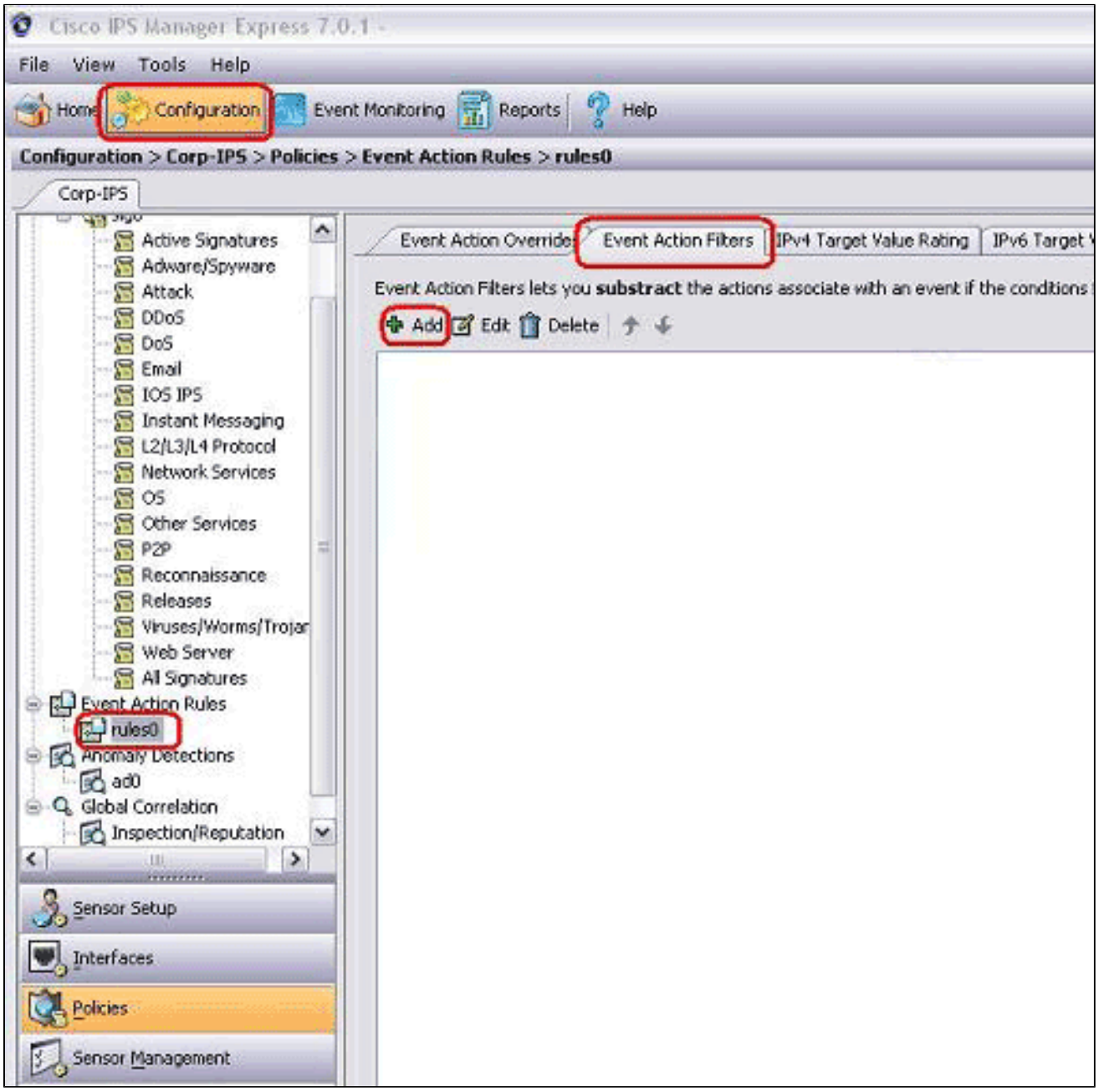
- Set van IP-adressen; bijvoorbeeld 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.1-192.168.100.11.

Een netwerk uitsluiten

De Event Action Filter sluit ook specifieke handtekeningen uit om een alarm af te vuren op basis van een bron- of doelnetwerkadres.

Voltooi deze stappen om een netwerk van het produceren van een specifiek handtekeningsalarm uit te sluiten:

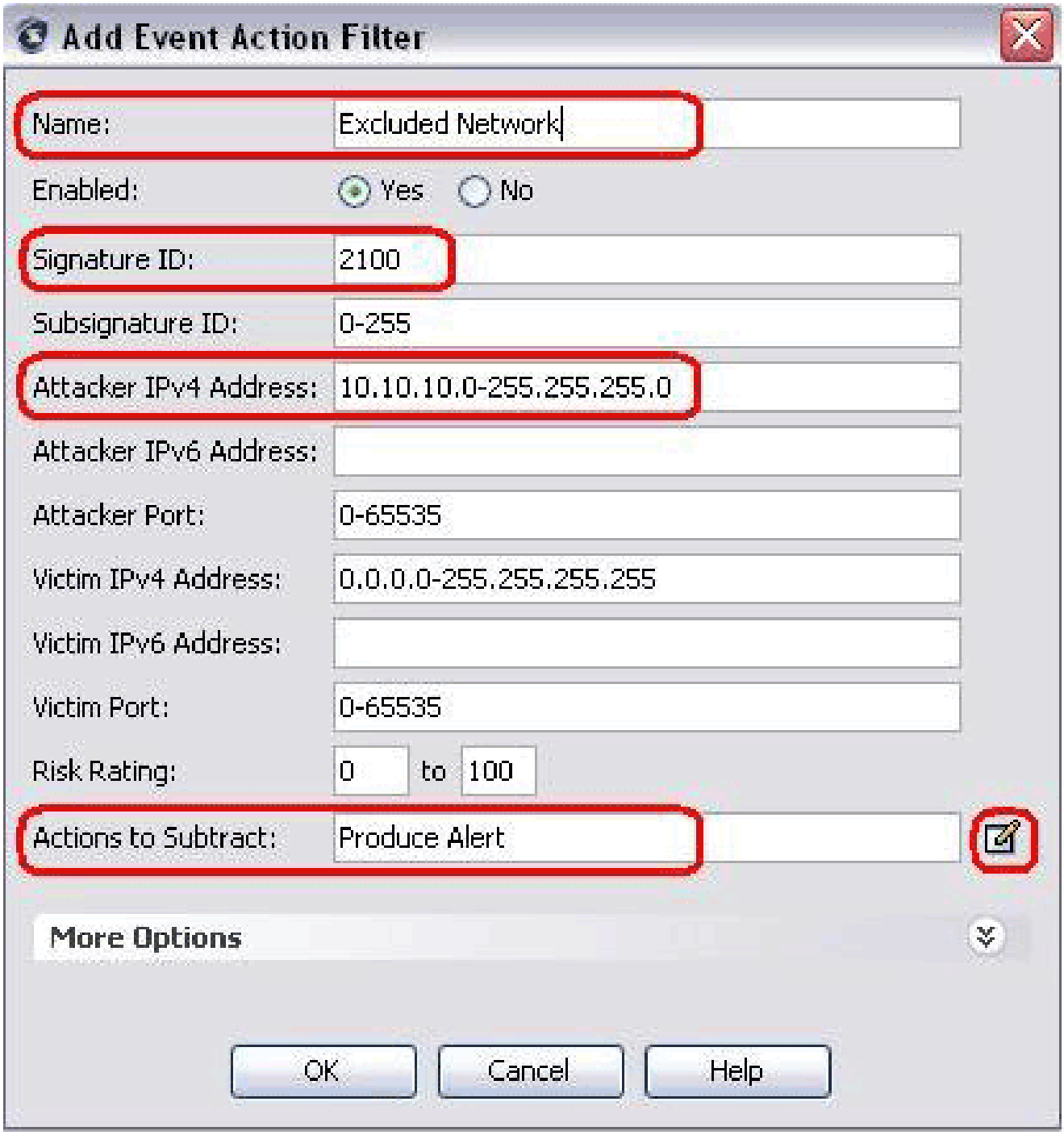
1. Klik op het tabblad Event Action Filters.



2. Klik op Add (Toevoegen).

3. Typ de filternaam, de handtekeningsidentificatie, het netwerkadres met subnetmasker en de

actie om af te trekken in de betreffende velden en klik vervolgens op OK.



Handtekeningen wereldwijd uitschakelen

U zou een handtekening van alarmerend op elk ogenblik kunnen willen onbruikbaar maken. Voltooi de volgende stappen om handtekeningen in te schakelen, uit te schakelen en terug te trekken:

1. Log in op IME met een account met beheerder- of operatorrechten.
2. Kies Configuratie > sensor_name > Beleid > Handtekeningdefinities > sig0 > Alle handtekeningen.

3. Kies een sorteeroptie in de vervolgkeuzelijst Filter om een handtekening te vinden. Als u bijvoorbeeld op zoek bent naar een ICMP Network Sweep-handtekening, kies dan Alle handtekeningen onder sig0, en zoek dan op handtekening ID of naam. Het sig0-venster ververst alleen de handtekeningen die overeenkomen met uw sorteringscriteria en geeft deze weer.

4. Om een bestaande handtekening in te schakelen of uit te schakelen, kiest u de handtekening en voert u de volgende stappen uit:

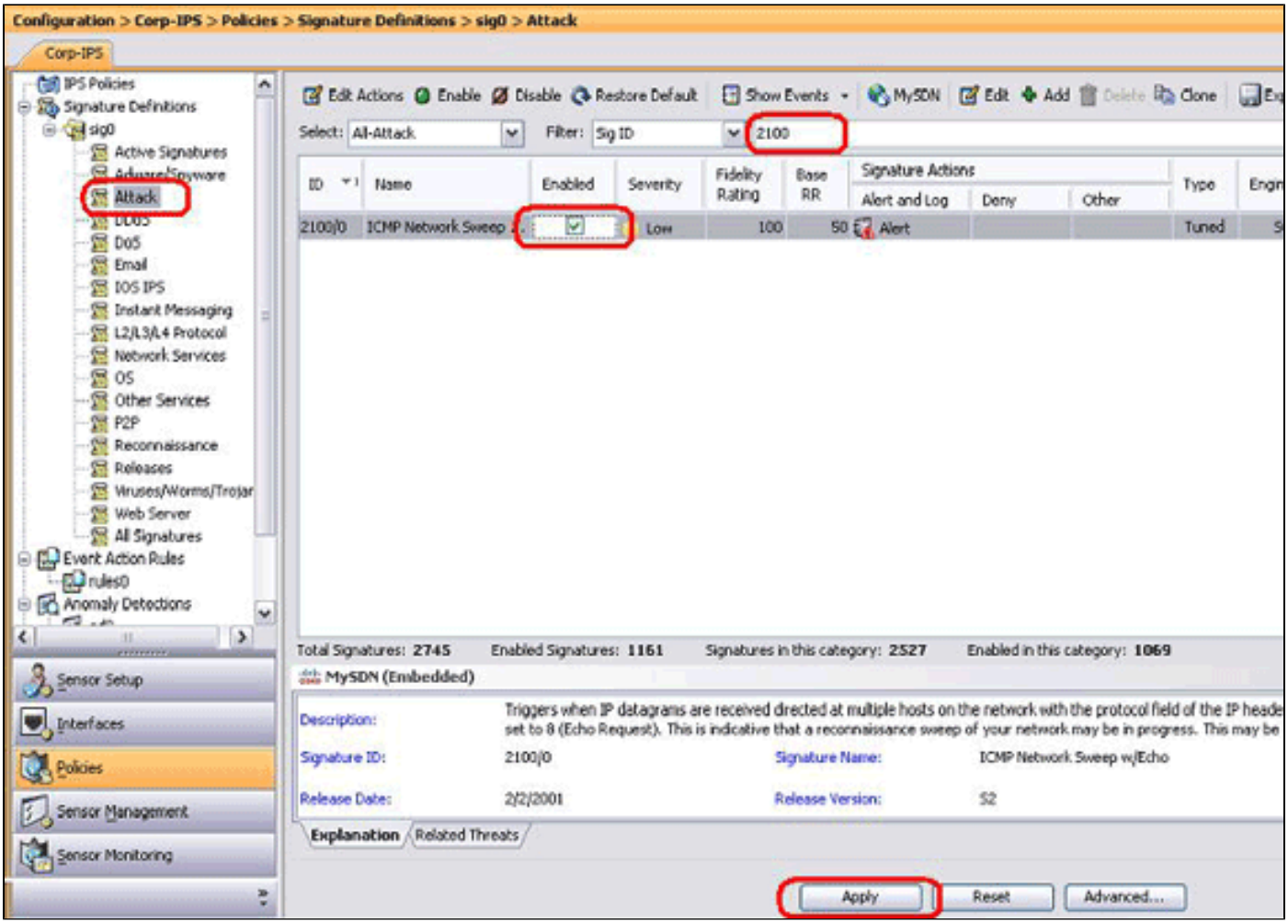
    a. Bekijk de kolom Ingeschakeld om de status van de handtekening te bepalen. Een handtekening die is ingeschakeld, heeft het aankruisvakje ingeschakeld.

    b. Om een handtekening in te schakelen die is uitgeschakeld, schakelt u het vakje Ingeschakeld in.

    c. Schakel het selectievakje Ingeschakeld uit om een handtekening uit te schakelen die is ingeschakeld.

    d. Als u een of meer handtekeningen wilt intrekken, kiest u de handtekening(en), klikt u met de rechtermuisknop en vervolgens klikt u op Status wijzigen in > Ingetrokken.

5. Klik op Toepassen om uw wijzigingen toe te passen en de herziene configuratie op te slaan.



Gerelateerde informatie

- End-of-sale voor Cisco Secure IDS-directeur
- Cisco Secure Inbraakdetectiepagina
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.