Cisco IPS seguros - Alarmes de falso positivo

Índice

Introdução

Este original descreve a exclusão dos alarmes falsos positivos para o Intrusion Prevention System (IPS) seguro de Cisco.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 7.0 segura do Intrusion Prevention System (IPS) de Cisco e o gerente do ips Cisco expressa 7.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Alarmes falso positivo e falso negativo

Cisco IPS seguro provoca um alarme quando um pacote ou uma sequência dada dos pacotes combinam as características dos perfis do ataque conhecido definidos nas assinaturas seguras de Cisco IPS. Uns critérios de projeto críticos da assinatura IPS são minimizar a ocorrência do falso positivo e dos alarmes falsos negativos.

Os falsos positivos (disparadores benignos) ocorrem quando o IPS relata determinada atividade benigna como maliciosa. Isto exige a intervenção humana diagnosticar o evento. Um grande número falsos positivos podem significativamente drenar recursos, e as habilidades especializadas exigidas analisá-los são caras e difíceis de encontrar.

Os falsos negativos ocorrem quando o IPS não detecta e relata a atividade mal-intencionada real. A consequência desta pode ser catastrófica e as assinaturas devem continuamente ser atualizadas enquanto as façanhas e as técnicas novas do corte são descobertas. Minimizar negativos falsos tem uma prioridade bem alta, às vezes, a custa de ocorrências mais altas de positivos falsos.

Devido à natureza das assinaturas que o uso de IPSs detectar a atividade mal-intencionada, ele é quase impossível eliminar completamente falsos positivos e negativos sem severamente degradar a eficácia do IPS ou severamente interromper a infraestrutura de computação de uma organização (tal como anfitriões e redes). O ajustamento personalizado quando um IPS é distribuído minimiza falsos positivos. O reajuste periódico é necessário quando o ambiente de computação muda (por exemplo, quando novos sistemas e aplicativos são implantados). Cisco IPS seguro fornece uma potencialidade de ajuste flexível que possa minimizar falsos positivos durante operações de estado estacionário.

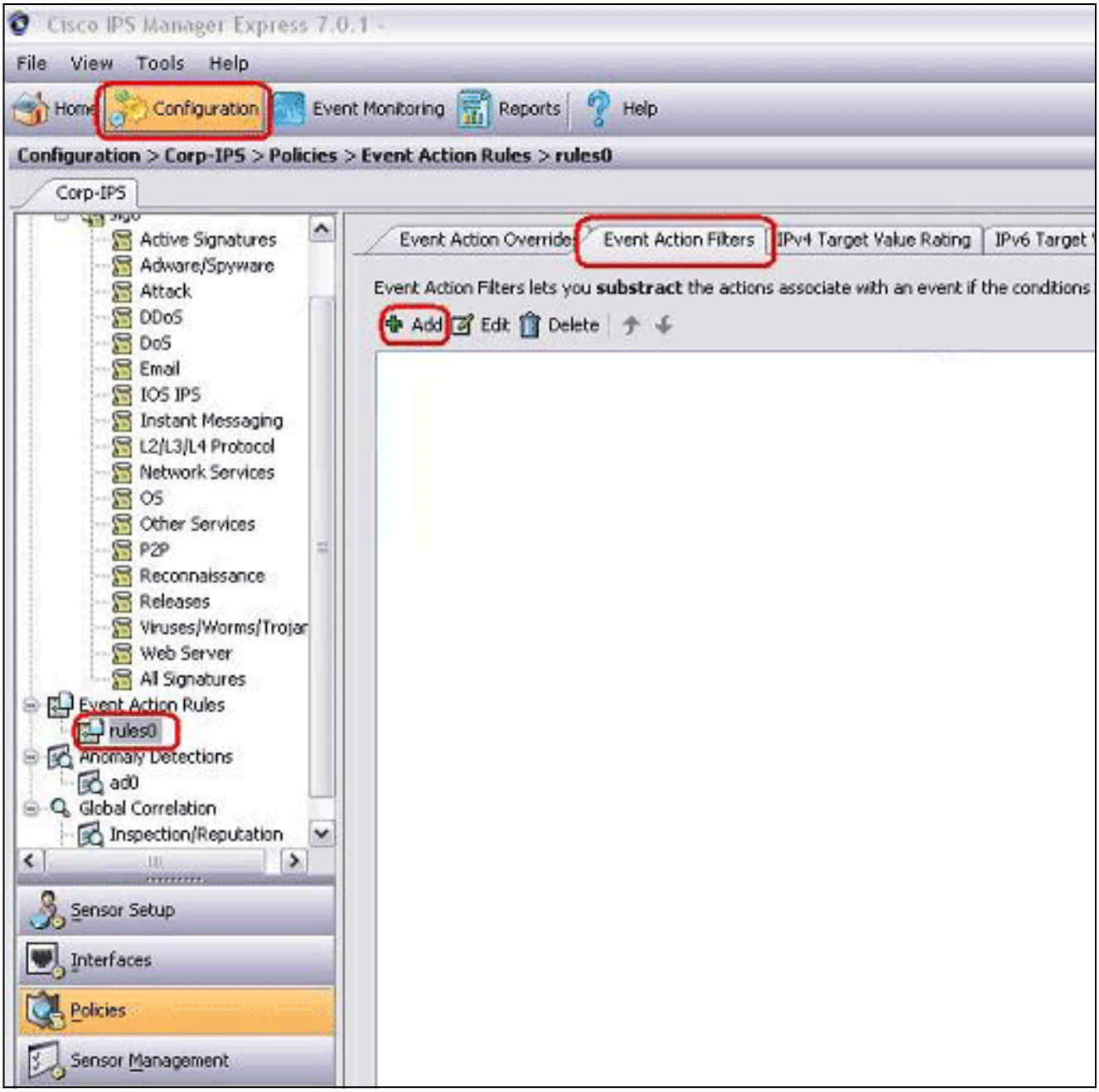
Cisco IPS seguro exclui o mecanismo

Cisco IPS seguro fornece a capacidade de excluir uma assinatura específica ou a um host específico ou aos endereços de rede. As assinaturas excluídas não geram ícones de alarme nem registros de log quando são disparadas de hosts ou redes excluídas especificamente por meio desse mecanismo. Por exemplo, uma estação de gerenciamento de rede pôde executar a descoberta da rede executando os ping sweeps, que provocam a varredura de rede ICMP com assinatura do eco (ID de assinatura 2100). Se você exclui a assinatura, você não tem que analisar o alarme e suprimir d cada vez que o processo de descoberta de rede é executado.

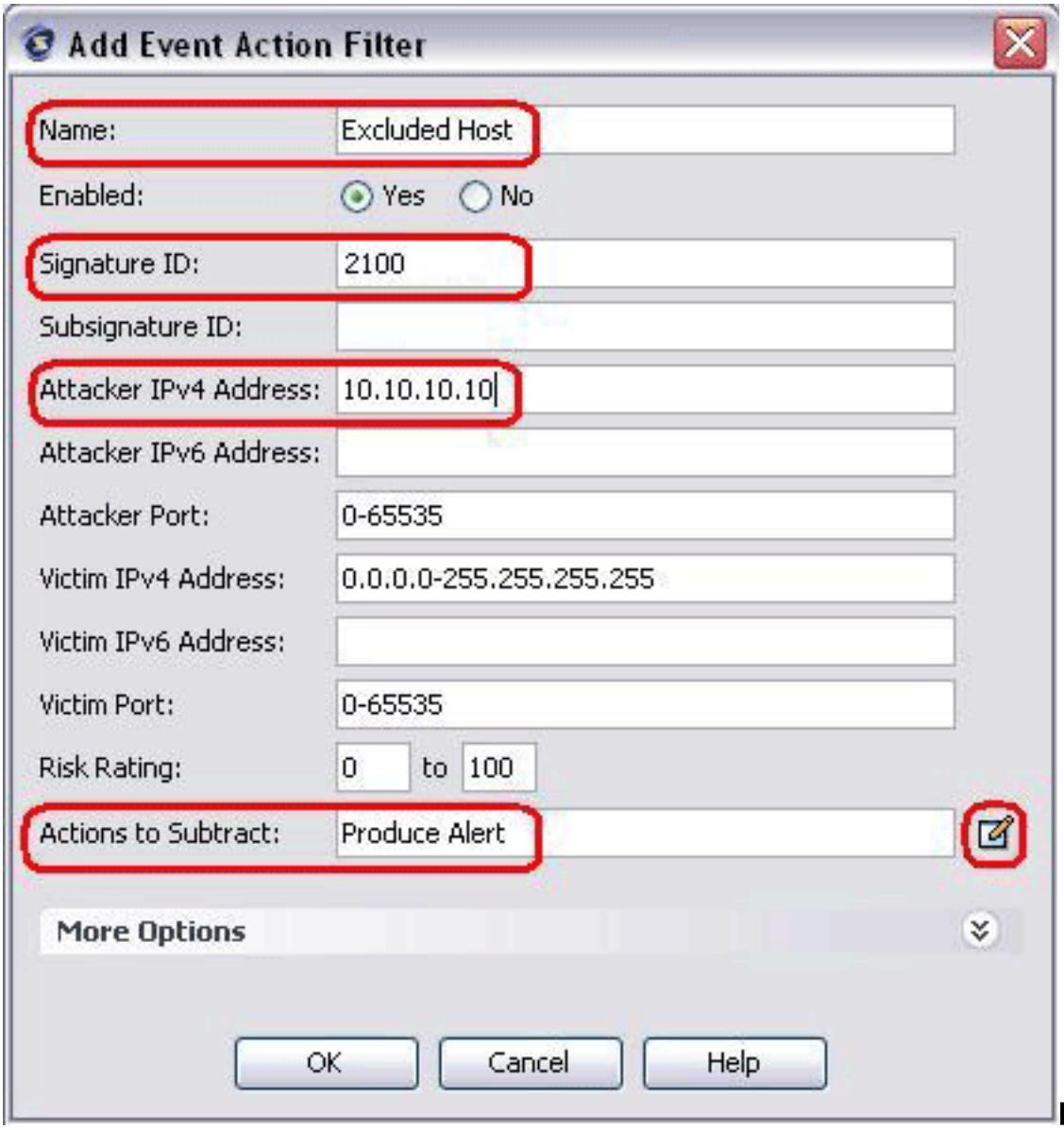
Excluir um host

Termine estas etapas a fim excluir um host específico (um endereço IP de origem) de gerar um alarme de assinatura específico:

1. Escolha a **configuração > o Corp-IPS > as políticas > as regras da ação do evento > o rules0**, e clique a aba dos **filtros da ação do evento**.



2. Clique em Add.
3. Datilografe o nome do filtro, o ID de assinatura, o endereço do IPv4 do atacante, e a ação para subtrair nos campos apropriados, e clique então a APROVAÇÃO.



Nota: Se você precisa de excluir endereços IP de Um ou Mais Servidores Cisco ICM NT múltiplos das redes diferentes, você pode usar a vírgula como um delimitador. Contudo, se você usa uma vírgula, evite o espaço de trailing após a vírgula; se não, você pôde receber um erro.**Nota:** Além, você pode usar as variáveis definidas na aba das variáveis de evento. Estas variáveis são úteis quando o mesmo valor deve ser repetido em filtros da ação do evento múltiplo. Você deve usar um sinal de dólar ($) como um prefixo à variável. A variável pode ser um destes formatos:Endereço IP de Um ou Mais Servidores Cisco ICM NT completo; por exemplo, 10.77.23.23.Escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT; por exemplo, 10.9.2.10-10.9.2.155.Grupo de escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT; por exemplo, 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11.

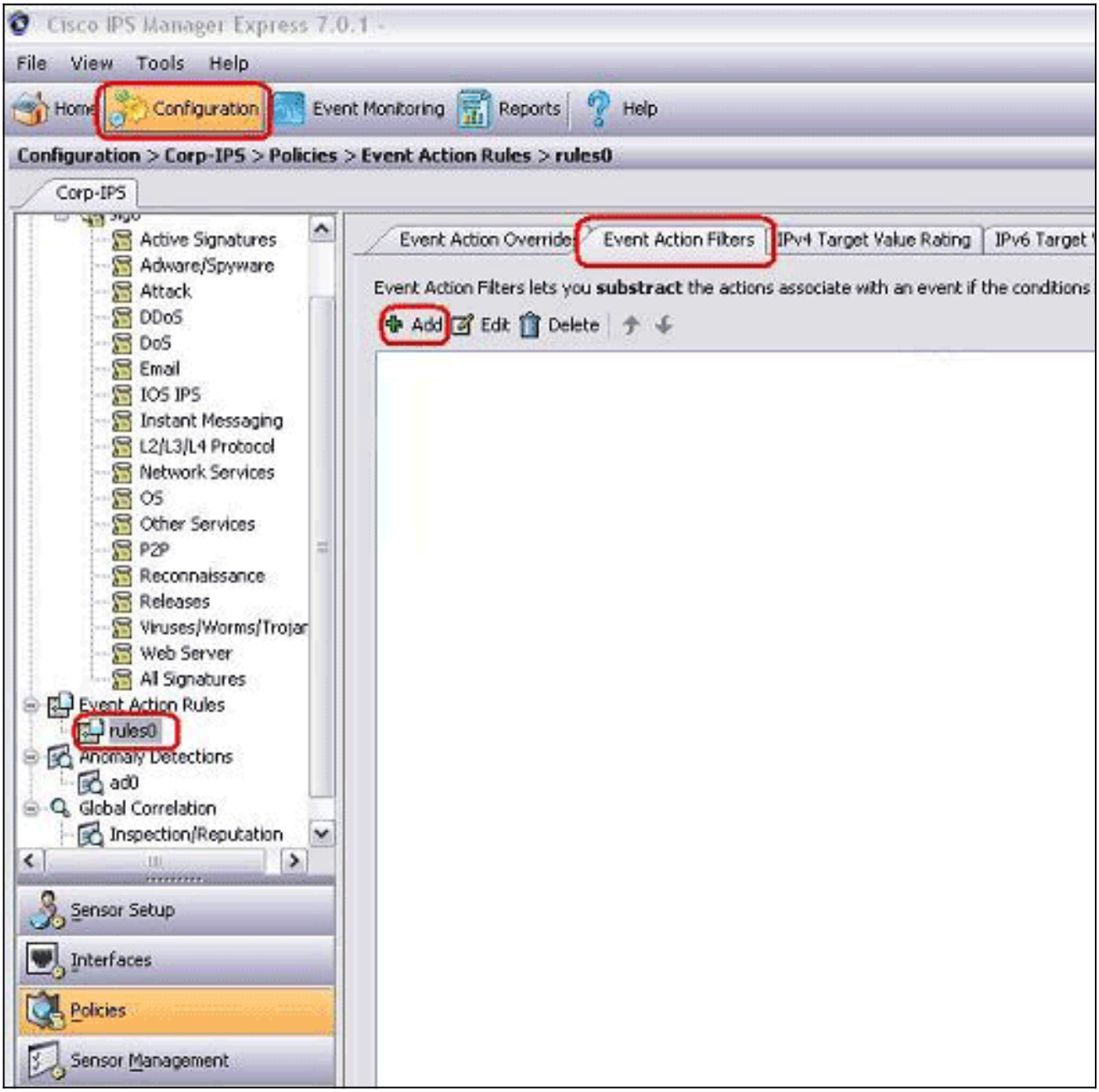
Excluir uma rede

O filtro da ação do evento igualmente exclui assinaturas específicas para atear fogo a um alarme baseado em um endereço de rede de origem ou de destino.

Termine estas etapas a fim excluir uma rede de gerar um alarme de assinatura específico:

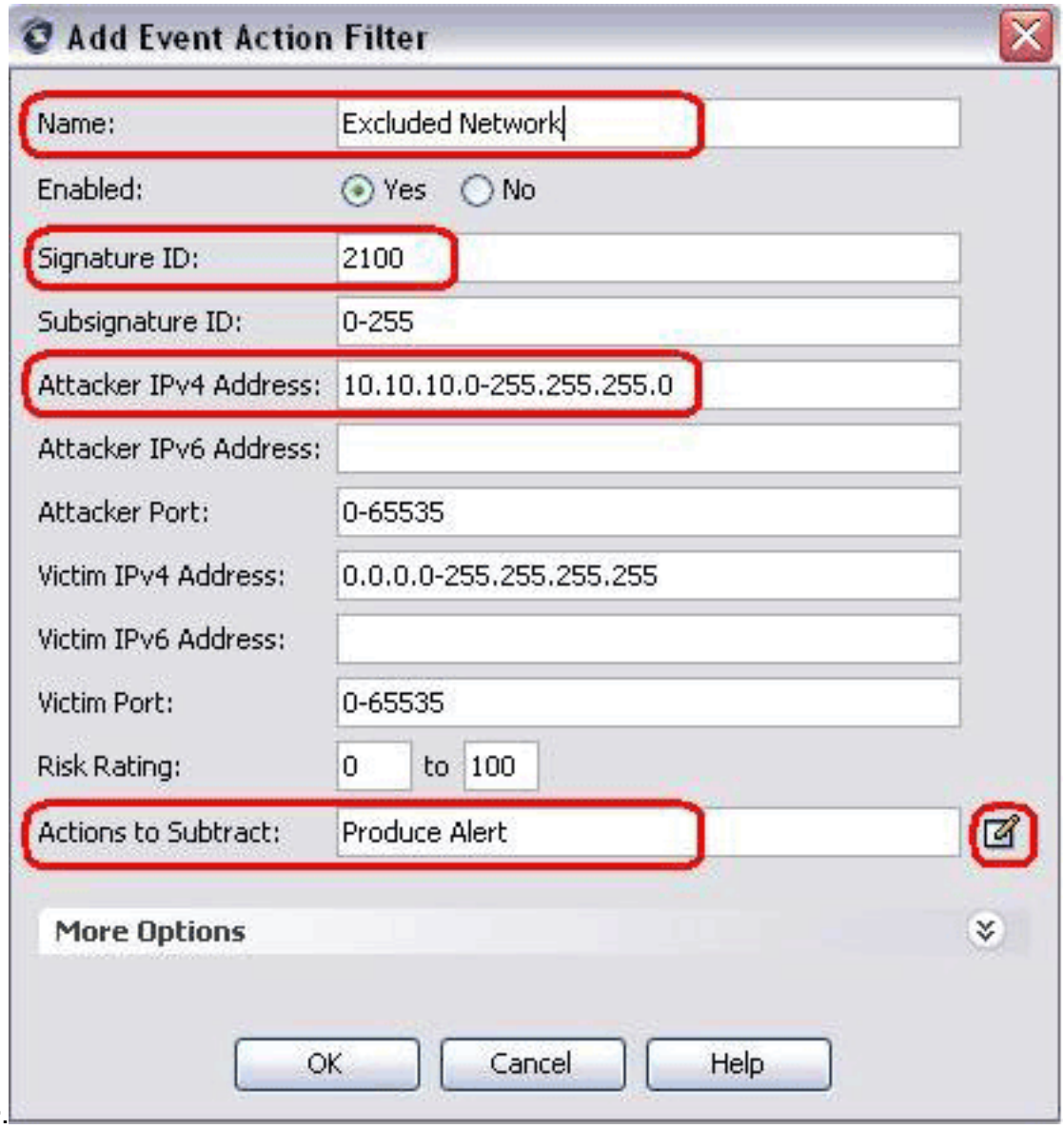
1. Clique a aba dos **filtros da ação do**

evento.



2. Clique em Add.
3. Datilografe o nome, o ID de assinatura, o endereço de rede com máscara de sub-rede, e a ação do filtro para subtrair nos campos apropriados, e clique então a

APROVAÇÃO.



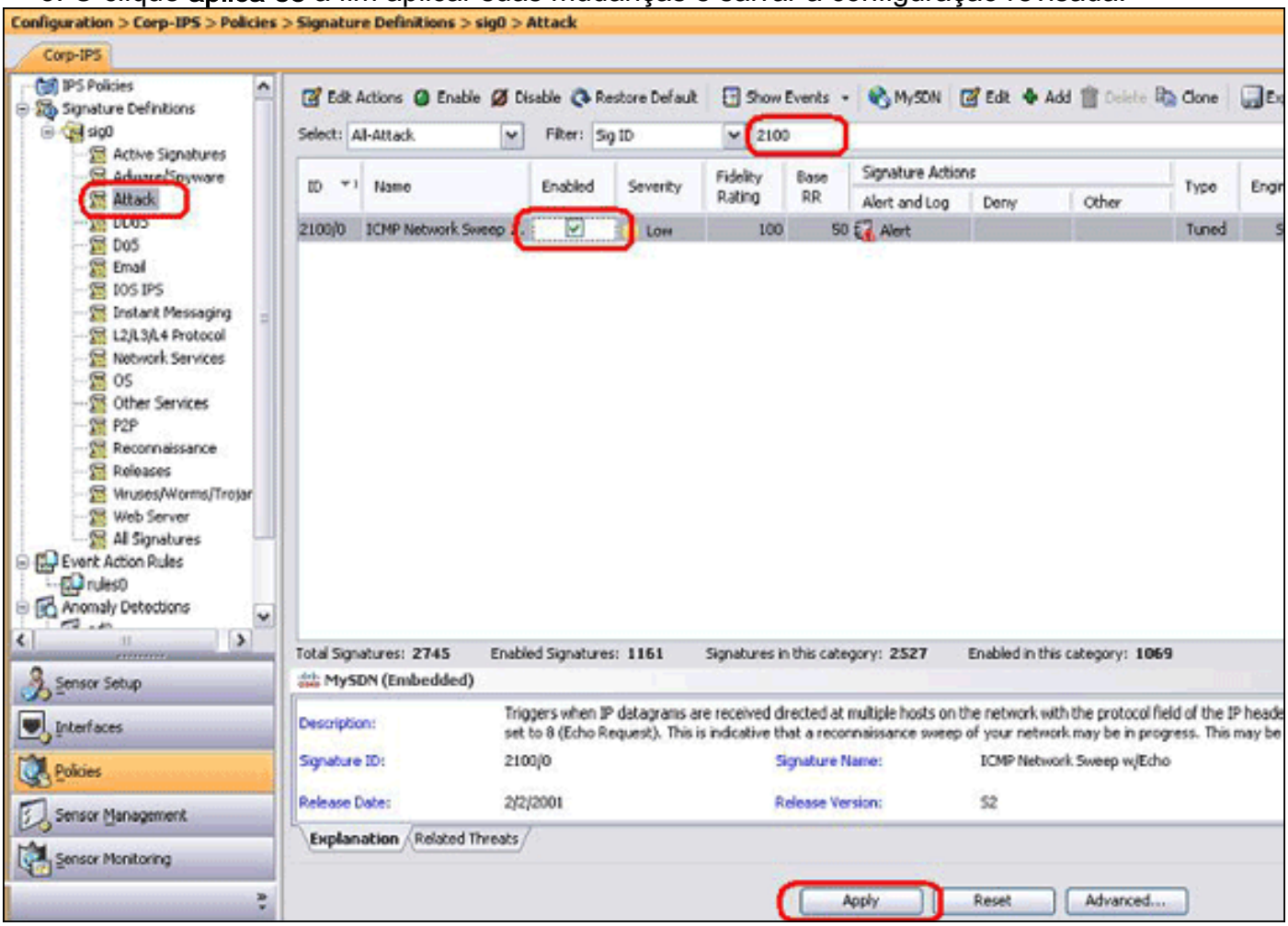
Desabilite globalmente assinaturas

Você pôde querer desabilitar uma assinatura do alarme a qualquer hora. A fim permitir, para desabilitar, e aposentar-se assinaturas, termine estas etapas:

1. Entre a IME usando uma conta com privilégios do administrador ou do operador.
2. Escolha a **configuração** > o **sensor_name** > as **políticas** > as **definições da assinatura** > o **sig0** > **todas as assinaturas**.
3. A fim encontrar uma assinatura, escolha uma opção de classificação da lista de drop-down do filtro. Por exemplo, se você está procurando por uma assinatura da varredura de rede ICMP, escolha **todas as assinaturas** sob sig0, a seguir procure-as pelo ID de assinatura ou nomeie-as. A placa sig0 refresca e indica somente aquelas assinaturas que combinam seus critérios de classificação.
4. A fim permitir ou desabilitar uma assinatura existente, escolha a assinatura, e termine estas etapas:Veja a coluna permitida para determinar o estado da assinatura. Uma assinatura que seja permitida tem a caixa de verificação verificada.A fim permitir uma assinatura que seja desabilitada, verifique a caixa de verificação **permitida**.A fim desabilitar uma assinatura que seja permitida, desmarcar a caixa de verificação **permitida**.A fim aposentar-se umas ou várias assinaturas, escolha as assinaturas, clicar com o botão direito, e clique então o

estado da mudança a > aposentado.

5. O clique **aplica-se** a fim aplicar suas mudanças e salvar a configuração revisada.



Informações Relacionadas

- Fim da venda para o diretor do Cisco Secure IDS
- Página de suporte do Cisco Secure Intrusion Detection
- Suporte Técnico e Documentação - Cisco Systems