Opções para reduzir eventos da intrusão do falso positivo

Índice

Introdução

Um sistema da prevenção de intrusão pode gerar alertas excessivos em uma determinada regra do Snort. Os alertas podiam ser positivo ou falso positivo verdadeiro. Se você está recebendo muitos alertas do falso positivo, há diversas opções disponíveis para que você reduza-os. Este artigo fornece um sumário das vantagens e desvantagem de cada opção.

Opções para reduzir alertas do falso positivo

> Nota: Estas opções não são geralmente a melhor escolha, elas podem ser a única solução sob circunstâncias específicas.

1. Relate ao Suporte técnico de Cisco

Se você encontra uma regra do Snort que provoque alertas no tráfego benigno, relate-o por favor ao Suporte técnico de Cisco. Uma vez que relatado, um engenheiro de suporte ao cliente escala a edição à equipe de investigação da vulnerabilidade (VRT). VRT pesquisa melhorias possíveis à regra. As regras melhoradas estão tipicamente disponíveis ao repórter assim que estiverem disponíveis, e são adicionadas igualmente à atualização oficial seguinte da regra.

2. Confie ou permita a regra

A melhor opção para permitir o tráfego confiado passar através de um dispositivo de Sourcefire

sem inspeção está permitindo a **confiança** ou **permitir a** ação sem uma política associada da intrusão. Para configurar uma confiança ou permitir a regra, navegue **regra ao > Add das políticas > do controle de acesso**.

> Nota: Trafique a confiança de harmonização ou permita as regras que não são configuradas para combinar usuários, aplicativos, ou as URL terão o impacto mínimo no desempenho geral de um dispositivo de Sourcefire porque tais regras podem ser processadas no hardware da potência de fogo.

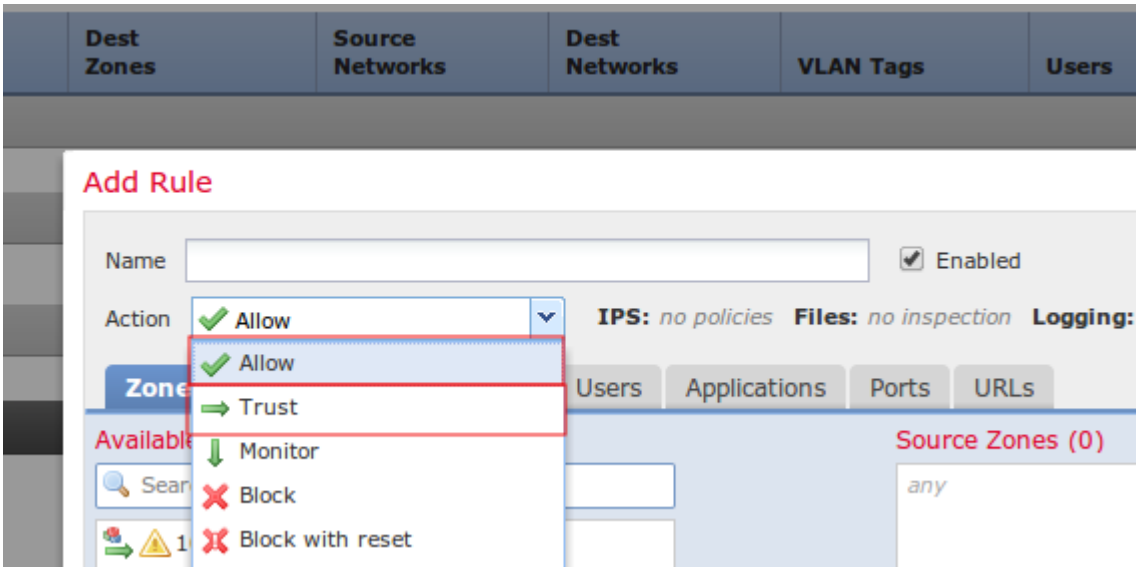

Figura: Configuração de uma regra da confiança

3. Regras desnecessárias do desabilitação

Você pode desabilitar as regras do Snort que visam vulnerabilidades velhas e remendadas. Melhora o desempenho e reduz falsos positivos. Usar recomendações de FireSIGHT pode ajudar com esta tarefa. Adicionalmente, as regras que gerenciem frequentemente os alertas de baixa prioridade ou os alertas que não são acionáveis podem ser bons candidatos para a remoção de uma política da intrusão.

4. Limite

Você pode usar o **ponto inicial** para reduzir o número de eventos da intrusão. Esta é uma boa opção a configurar quando uma regra é esperada provocar regularmente um número limitado de eventos no tráfego normal, mas poderia ser uma indicação de um problema se mais do que um determinado número de pacotes combinam a regra. Você pode usar esta opção para reduzir o número de eventos provocados por regras ruidosas.

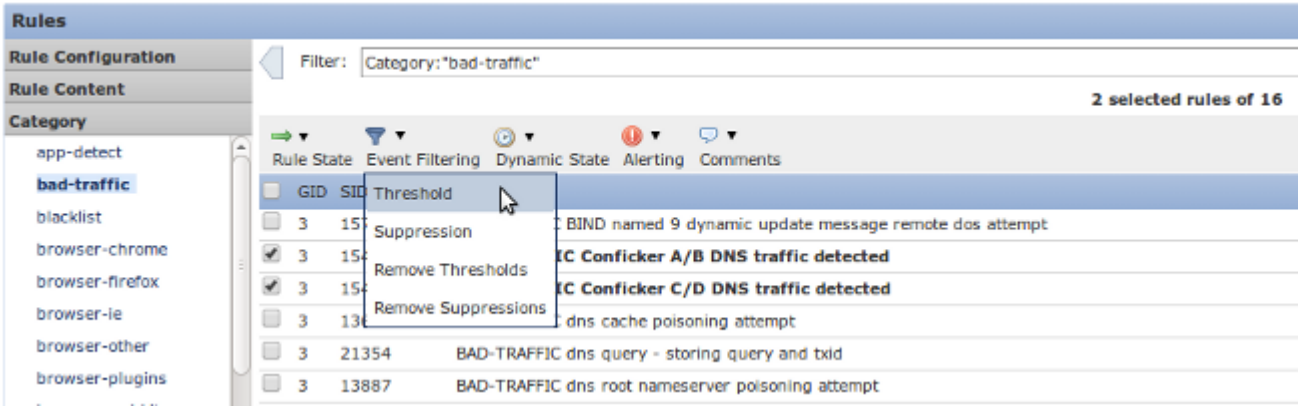

Figura: Configuração do ponto inicial

5. Supressão

Você pode usar a **supressão** para eliminar completamente a notificação dos eventos. É similar configurado à opção do **ponto inicial**.

> Cuidado: A supressão pode conduzir problemas de desempenho, porque quando nenhum evento for gerado, o Snort ainda tem que processar o tráfego.

> Nota: A supressão não impede regras da gota do tráfego deixando cair, assim que o tráfego pode silenciosamente ser deixado cair quando combina com a regra da gota.

6. Regras do caminho rápido

Similar para confiar e permitir regras de uma política do controle de acesso, as regras do caminho rápido enlatam igualmente a inspeção dos desvios. O Suporte técnico de Cisco geralmente não recomenda usar regras do caminho rápido porque são configurados no indicador **avançado da** página do **dispositivo** e pode facilmente ser negligenciado quando as regras do controle de acesso forem quase sempre suficientes.

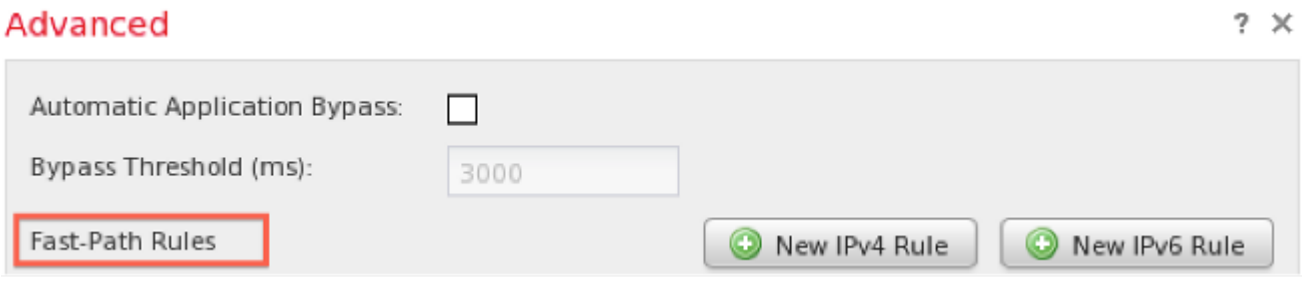

Figura: O caminho rápido ordena a opção no indicador avançado.

A única vantagem a usar regras do caminho rápido é que podem segurar um volume de tráfego máximo maior. As regras do caminho rápido processam o tráfego a nível de hardware (conhecido como NMSB) e podem teoricamente segurar até o 200 Gbps do tráfego. Ao contrário, as regras com **confiança** e **permitem** ações são promovidas ao motor do fluxo de rede (NFE) e podem segurar um máximo do 40 Gbps do tráfego.

Nota: As regras do caminho rápido estão somente disponíveis em dispositivos do 8000 Series e no 3D9900.

7. Passe regras

A fim impedir uma regra específica da provocação no tráfego de um determinado host (quando o outro tráfego desse host precisar de ser inspecionado), use um tipo regra da *passagem do* Snort. De fato, esta é a única maneira de realizá-la. Quando as regras da passagem forem eficazes, podem ser muito difíceis de manter porque as regras da passagem são escritas manualmente. Adicionalmente, se as regras originais de regras da passagem são alteradas por uma atualização da regra, todas as regras relacionadas da passagem precisam de ser atualizadas manualmente. Se não podem tornar-se ineficazes.

8. Variável SNORT_BPF

A variável de `Snort_BPF em uma` política da intrusão permite determinado tráfego de contornear a inspeção. Quando esta variável era uma das primeiras escolhas em versões de software legado, o Suporte técnico de Cisco recomenda usar uma regra da política do controle de acesso para contornear a inspeção, porque é mais granulado, mais visível, e muito mais fácil configurar.