Configuração de uma regra da passagem em um sistema de FireSIGHT

Índice

Introdução

Você pode criar regras da `passagem` para impedir os pacotes que encontram os critérios definidos na regra da `passagem de` provocar a regra `alerta em` situações específicas, um pouco do que desabilitando a regra `alerta`. À revelia, as regras da `passagem` cancelam regras `alertas`. Um sistema de FireSIGHT compara pacotes contra as circunstâncias especificadas em cada regra e, se os dados do pacote combinam todas as circunstâncias especificadas em uma regra, nos disparadores da regra. Se uma regra é uma regra `alerta`, gerencie um evento da intrusão. Se é uma regra da `passagem`, ignora o tráfego.

Por exemplo, você pôde querer uma regra que procurasse tentativas de registrar em um servidor FTP como o usuário “anônimo” para permanecer ativa. Contudo, se sua rede tem uns ou vários server legítimos do Anonymous FTP, você poderia escrever e ativar uma regra da `passagem` que especificasse que, para aqueles server específicos, os usuários anônimos não provocam a regra original.

Este documento descrevem o que é uma regra da `passagem`, como criá-la e como permiti-la em uma política da intrusão.

> **Caution**: Quando uma regra original que a regra da `passagem` está baseada sobre recebe uma revisão, a regra da `passagem` não está atualizada automaticamente. Consequentemente, as regras da `passagem` podem ser difíceis de manter.

> **Note**: Se você permite a característica da *supressão* para uma regra, suprime as notificações de evento para essa regra. Contudo a regra é é avaliada ainda. Por exemplo, se você suprime uma regra da `gota`, os pacotes que combinam a regra são deixados cair silenciosamente.

Configuração

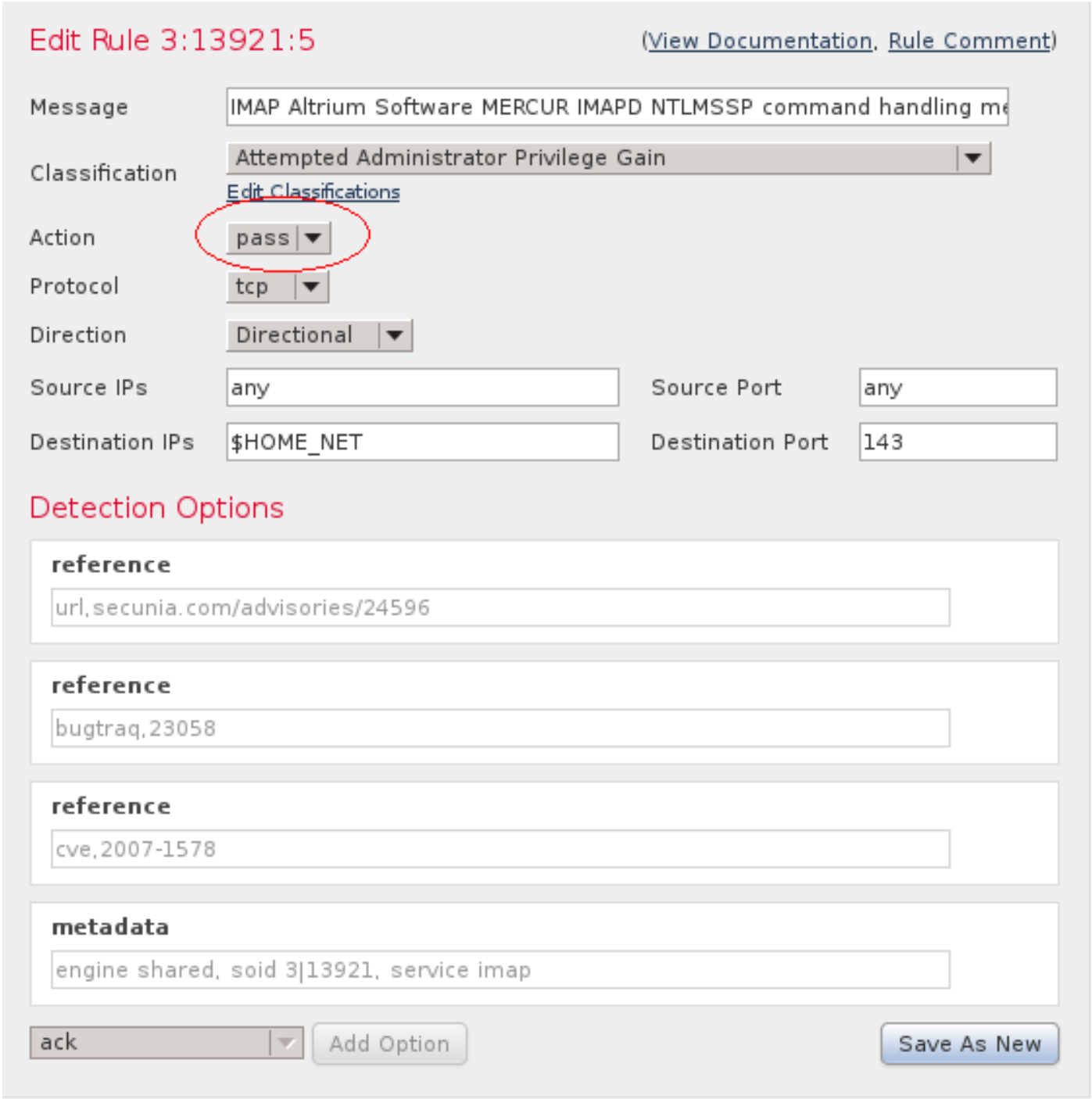
Crie uma regra da passagem

1. Navegue às **políticas > ao editor da intrusão > da regra**, para abrir o editor da regra usando a interface da WEB

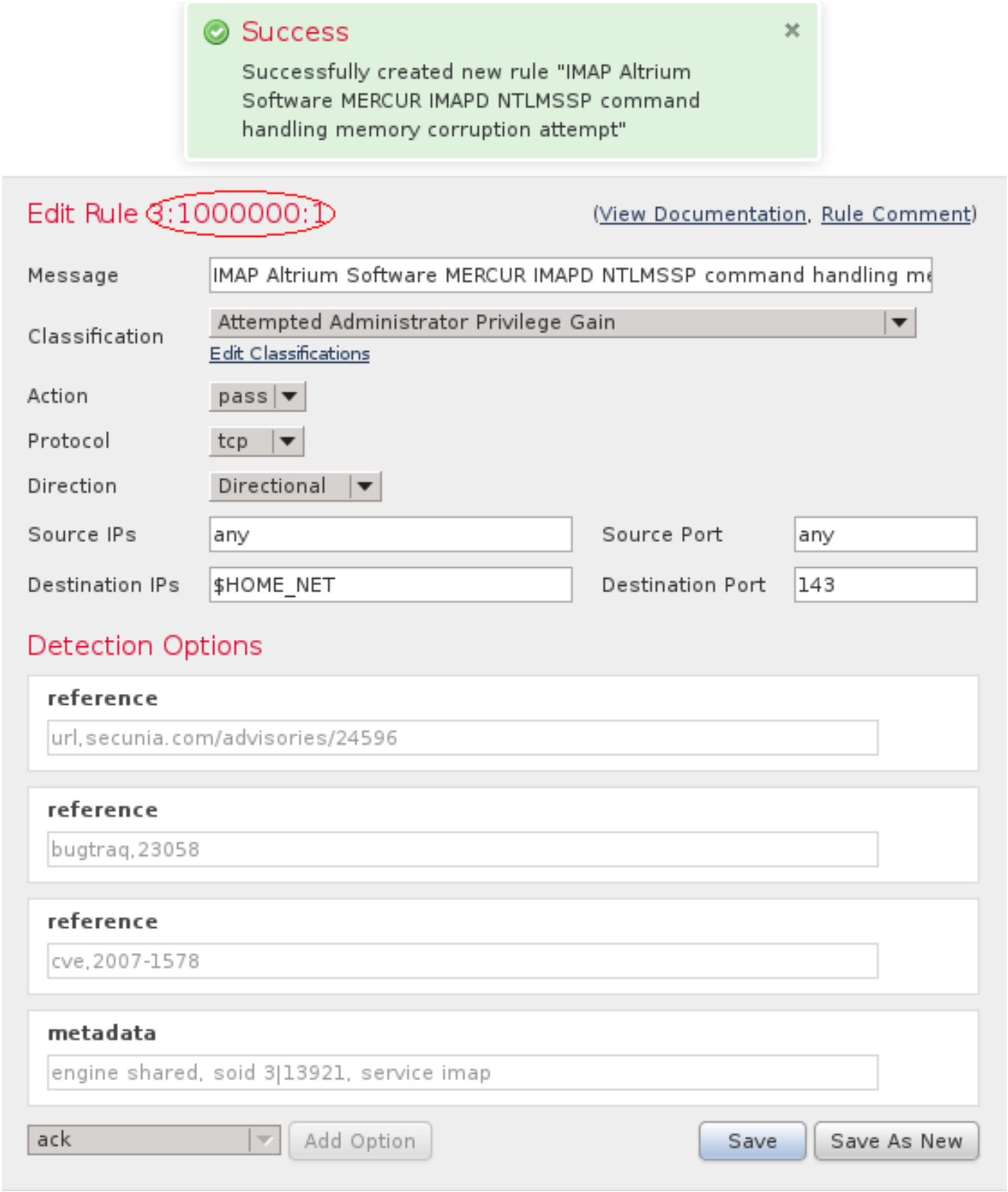
2. Encontre a regra que você quer filtrar. Use a caixa da busca ou as listas da categoria para encontrar a regra que você quer fazer uma regra da `passagem` para.

3. Edite a regra para combinar seus critérios:

- Clique o **botão Edit que** corresponde à regra.
- Mude o **IP da fonte** e o **IP de destino aos** anfitriões ou às redes que você não quer a regra alertar sobre.
- Mude a **ação do alerta para passar**.



4. Clique a **salvaguarda como nova**. Note o número de ID da regra nova. Por exemplo, 1000000.



Permita uma regra da passagem

Você precisa de permitir sua regra nova na política apropriada da intrusão a fim passar o tráfego nos endereços de origem ou de destino que você especificou. Siga as etapas abaixo para permitir uma regra da `passagem`:

1. Altere a política ativa da intrusão.

- Navegue às **políticas > à intrusão > à política da intrusão.**
- O clique **edita** ao lado de sua política de trabalho.

2. Adicionar a regra nova à lista da regra.

- Clique **regras na** placa do lado esquerdo.
- Incorpore a regra ID que você notou mais cedo na caixa do filtro.
- Selecione a caixa de verificação das regras, e mude o estado da regra **para gerar eventos**.
- Clique a **informação sobre a política na** placa do lado esquerdo. O clique **compromete o** botão das **mudanças**.

3. Clique o botão da **política da aplicação** ao lado da política da intrusão. Selecione seus dispositivos e o clique **reaplica**.

Verificação

Você deve monitorar os eventos novos para que algum dia certifique-se que nenhum evento está gerado para esta regra específica para a fonte definida ou o IP de destino.