Configuración de una regla del paso en un sistema de FireSIGHT

Contenido

Introducción

Usted puede crear las reglas del `paso` para prevenir los paquetes que cumplen los criterios definidos en la regla del `paso de` accionar la regla `alerta` en las situaciones específicas, bastante que inhabilitando la regla `alerta`. Por abandono, reglas de la `alerta de la` invalidación de las reglas del `paso`. Un sistema de FireSIGHT compara los paquetes contra las condiciones especificadas en cada regla y, si los datos del paquete hacen juego todas las condiciones especificadas en una regla, los activadores de la regla. Si una regla es una regla `alerta`, genera un evento de la intrusión. Si es una regla del `paso`, ignora el tráfico.

Por ejemplo, usted puede ser que quiera una regla que busca las tentativas de registrar en un servidor FTP como el usuario “anónimo” para seguir siendo activa. Sin embargo, si su red tiene uno o más servidores legítimos del Anonymous FTP, usted podría escribir y activar una regla del `paso` que especifica que, para esos servidores específicos, los usuarios anónimos no accionan la regla original.

Este documento describe cuál es una regla del `paso`, cómo crearla y cómo habilitarla en una directiva de la intrusión.

> **Caution**: Cuando una regla original que la regla del `paso` está basada encendido recibe una revisión, la regla del `paso` no se pone al día automáticamente. Por lo tanto, las reglas del `paso` pueden ser difíciles de mantener.

> **Note**: Si usted habilita la característica de la *supresión* para una regla, suprime las notificaciones de evento para esa regla. Sin embargo la regla está todavía se evalúa. Por ejemplo, si usted suprime una regla del `descenso`, los paquetes que hacen juego la regla se caen silenciosamente.

Configuración

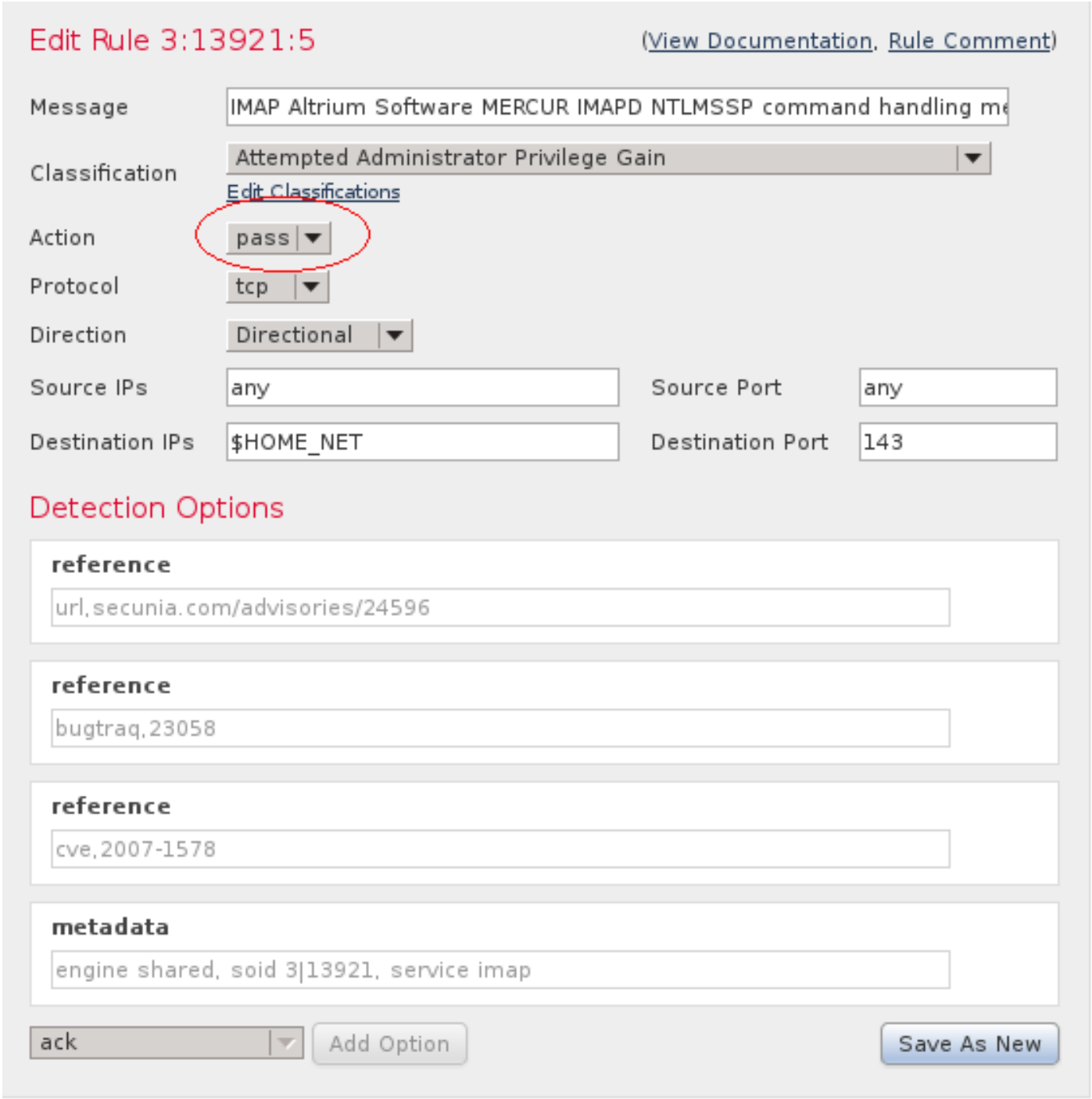
Cree una regla del paso

1. Navegue a las **directivas > al editor de la intrusión > de la regla**, para abrir el editor de la regla usando la interfaz Web

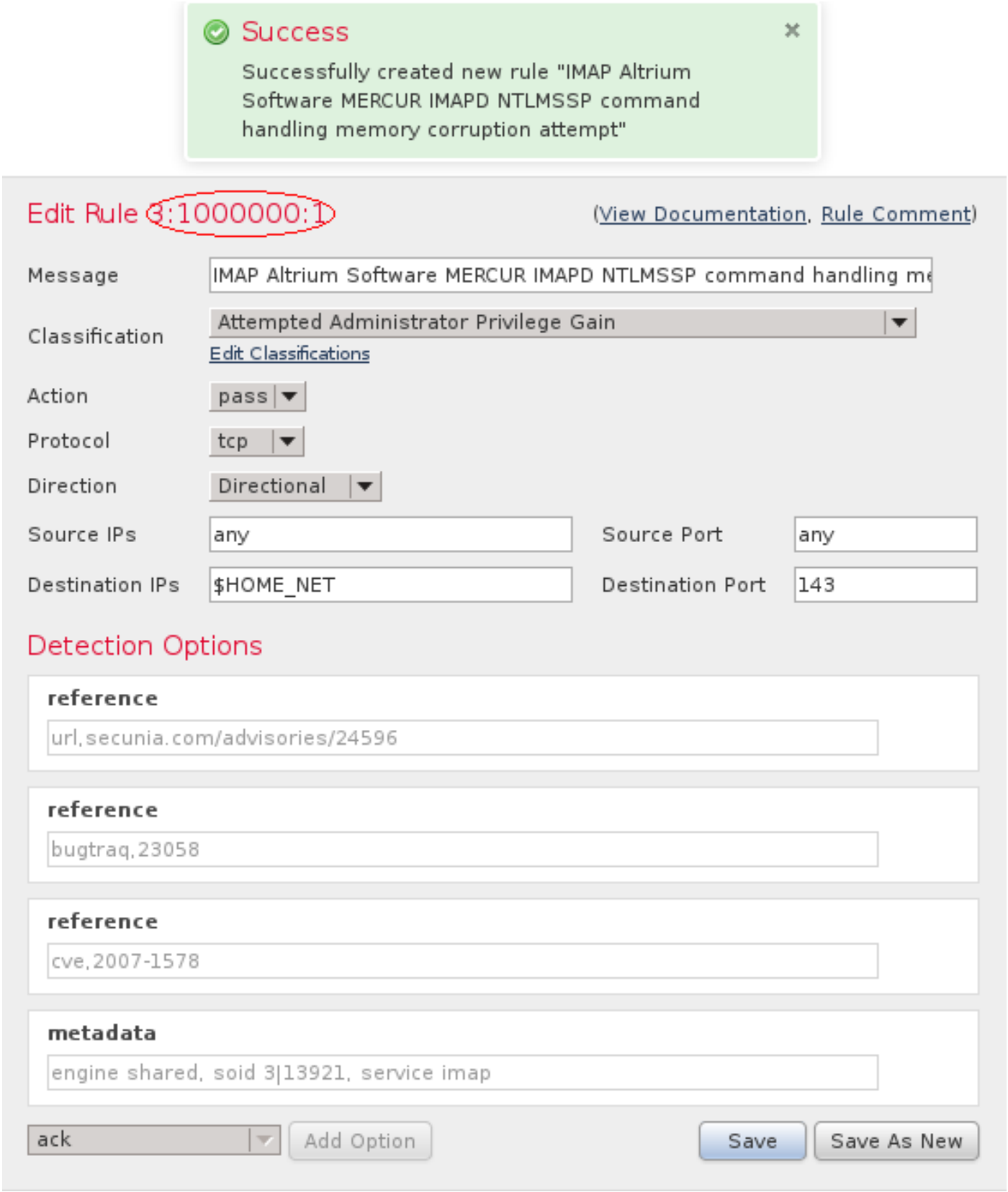
2. Encuentre la regla que usted quiere filtrar. Utilice el cuadro de búsqueda o los anuncios de la categoría para encontrar la regla para la cual usted quiere hacer una regla del `paso`.

3. Edite la regla para hacer juego sus criterios:

- Haga clic el **botón Edit** correspondiente a la regla.
- Cambie el **IP de la fuente** y el **IP de destino a los** host o a las redes que usted no quisiera que la regla alertara encendido.
- Cambie la **acción de la alerta para pasar**.



4. Haga clic la **salvaguardia como nueva**. Observe el número de ID de la nueva regla. Por ejemplo, 1000000.



Habilite una regla del paso

Usted necesita permitir a su nueva regla en la directiva apropiada de la intrusión para pasar el tráfico en las direcciones de origen o de destino que usted especificó. Siga los pasos abajo para habilitar una regla del `paso`:

1. Modifique la directiva activa de la intrusión.

- Navegue a las **directivas > a la intrusión > a la directiva de la intrusión.**
- El tecleo **edita** al lado de su directiva de trabajo.

2. Agregue la nueva regla a la lista de la regla.

- Haga clic las **reglas** en el cristal del lado izquierdo.
- Ingrese la regla ID que usted observó anterior en el rectángulo del filtro.
- Seleccione la casilla de verificación de las reglas, y cambie el estado de la regla **para generar los eventos**.
- Haga clic la **información de política** en el cristal del lado izquierdo. Haga clic el botón de los **cambios del cometer**.

3. Haga clic el botón de la **directiva de la aplicación** al lado de la directiva de la intrusión. Seleccione sus dispositivos y el tecleo **reaplica**.

Verificación

Usted debe monitorear los nuevos eventos por algún tiempo para no aseegurarse ningún evento se genera para esta regla específica para la fuente definida o el IP de destino.