Configure una regla del paso en un sistema de Cisco FirePOWER

Contenido

Introducción

Este documento describe una regla del paso, cómo crearla, y cómo activarla en una directiva de la intrusión.

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 FirePOWER 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 ftp server 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.

> Precaución: 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 pudieron ser difíciles de mantener.

> **Note**: Si usted activa la característica de la supresión para una regla, suprime las notificaciones de eventos 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.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

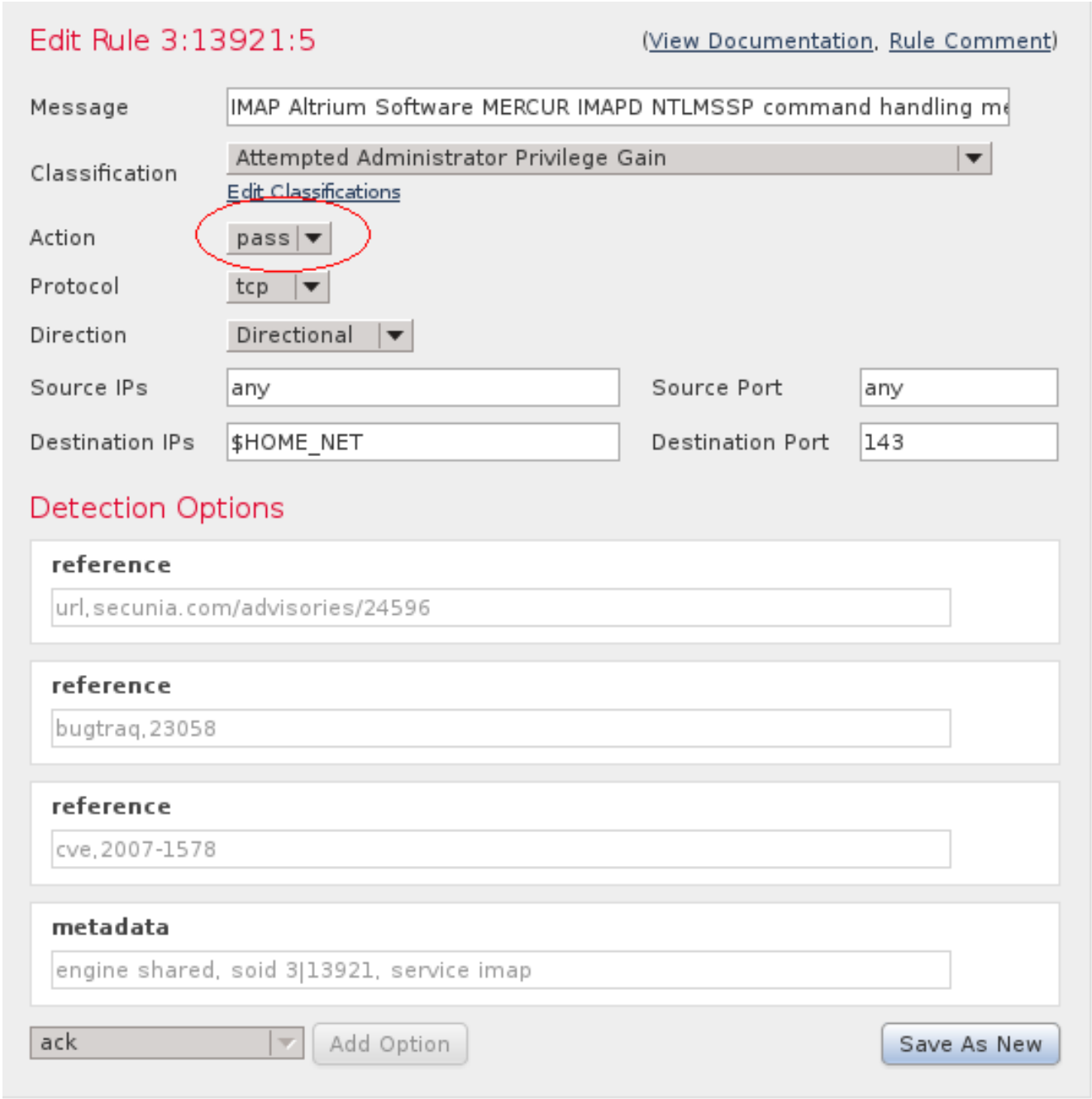
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

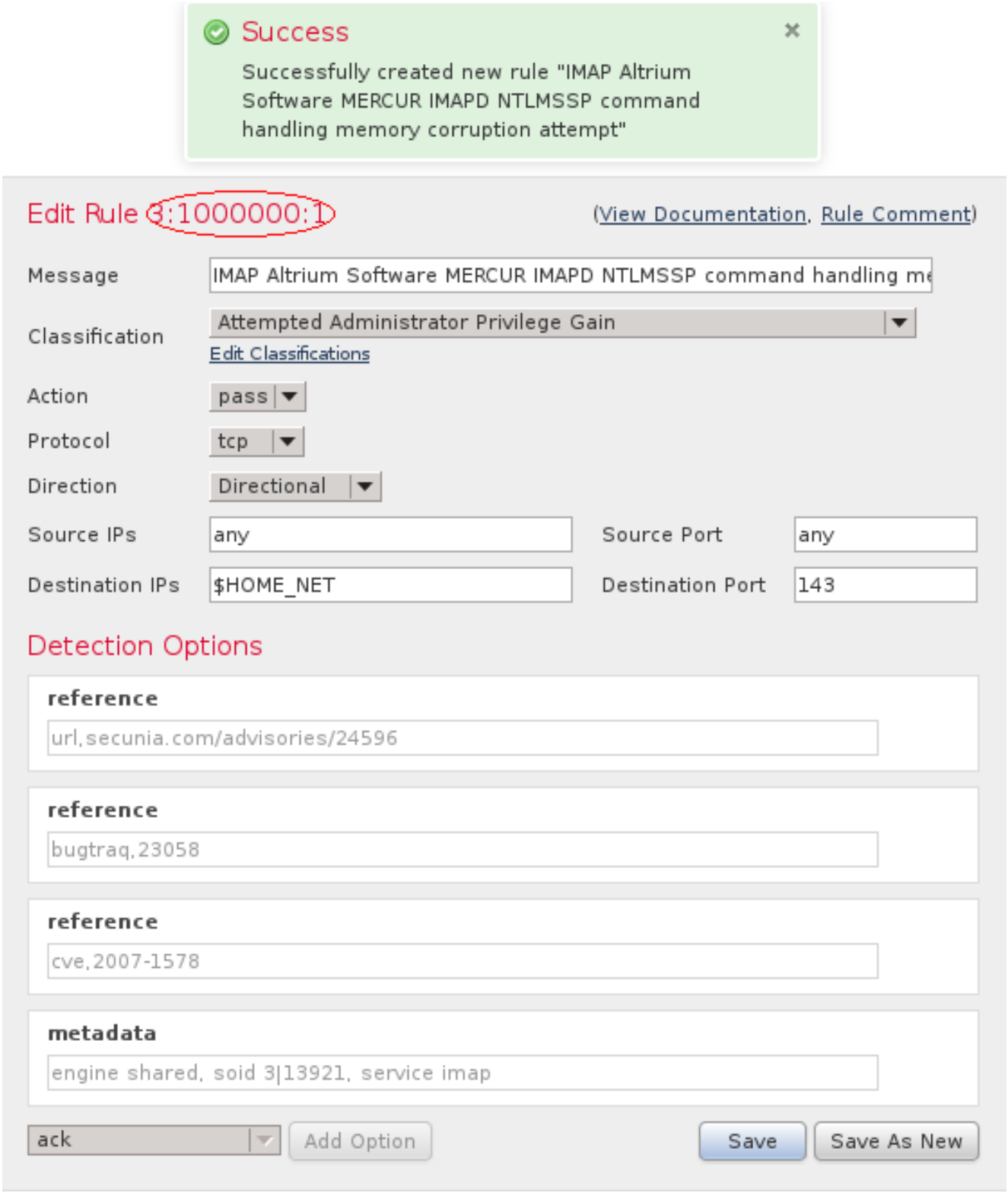
Configurar

Cree una regla del paso

1. Navegue a los **objetos > a las reglas de la intrusión**. La lista de categorías de la regla aparece.
2. Encuentre la categoría de la regla que se asocia a la regla que usted quiere filtrar. Utilice el icono de flecha para ampliar la categoría de la regla de los anuncios de la categoría y para encontrar la regla para la cual usted quiere hacer una regla del paso. Alternativamente, usted puede utilizar el cuadro de búsqueda de la regla.
3. Una vez que usted encuentra la regla deseada, haga clic el icono del lápiz al lado de él para corregir la regla.
4. Cuando usted corrige una regla, complete estos pasos: Haga clic el **botón Edit** que corresponde a la regla.En la lista desplegable de la acción, elija el **paso**.Cambie el campo IPS de la fuente y el campo del IP de destino a los host o a las redes que usted no quisiera que la regla alertara encendido.Haga clic la **salvaguardia como nueva**.



5. Observe el número de ID de la nueva regla. Por ejemplo, 1000000.



Active 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 siguientes pasos para activar una regla del paso:

1. Modifique la directiva activa de la intrusión: Navegue a las **directivas > al control de acceso > a la intrusión**.El tecleo **corrige** al lado de la directiva activa de la intrusión.
2. Agregue la nueva regla a la lista de la regla: Haga clic las **reglas** en del lado izquierdo el cristal.Ingrese la identificación de la regla que usted observó anterior en el rectángulo del

filtro.Controle 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 del lado izquierdo el cristal. Haga clic los **cambios del cometer**.

3. El tecleo **despliega** para desplegar los cambios en el dispositivo.

Verificación

Usted debe vigilar los nuevos eventos por algún tiempo para asegurarse de que no se genera ningunos eventos para esta regla específica para la fuente o la dirección IP definida del destino.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.