

# Configuración de una Regla de Paso en un Sistema Cisco Firepower

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Crear una regla de paso](#)

[Habilitar una regla de paso](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

Este documento describe una regla de paso, cómo crearla y cómo habilitarla en una política de intrusión.

Puede crear reglas de paso para evitar que los paquetes que cumplen los criterios definidos en la regla de paso activen la regla de alerta en situaciones específicas, en lugar de inhabilitar la regla de alerta. De forma predeterminada, las reglas de paso invalidan las reglas de alerta. Un sistema Firepower compara los paquetes con las condiciones especificadas en cada regla y, si los datos del paquete coinciden con todas las condiciones especificadas en una regla, la regla desencadena. Si una regla es una regla de alerta, genera un evento de intrusión. Si es una regla de paso, ignora el tráfico.

Por ejemplo, es posible que desee que una regla que busque intentos de iniciar sesión en un servidor FTP como el usuario "anonymous" permanezca activo. Sin embargo, si su red tiene uno o más servidores FTP anónimos legítimos, puede escribir y activar una regla de paso que especifique que, para esos servidores específicos, los usuarios anónimos no activarán la regla original.

**Precaución:** Cuando una regla original en la que se basa la regla de aprobación recibe una revisión, la regla de aprobación no se actualiza automáticamente. Por lo tanto, las reglas de aprobación podrían ser difíciles de mantener.

**Nota:** Si habilita la función Supresión para una regla, suprime las notificaciones de eventos para esa regla. Sin embargo, se sigue evaluando la regla. Por ejemplo, si suprime una regla de caída, los paquetes que coinciden con la regla se descartan silenciosamente.

## Prerequisites

## Requirements

No hay requisitos específicos para este documento.

## Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

### Crear una regla de paso

1. Vaya a **Objetos > Reglas de intrusión**. Aparece la lista de categorías de reglas.
2. Busque la categoría de regla asociada a la regla que desea filtrar. Utilice el icono de flecha para expandir la categoría de regla de los listados de categorías y buscar la regla para la que desea hacer una regla de paso. También puede utilizar el cuadro de búsqueda de reglas.
3. Una vez que encuentre la regla deseada, haga clic en el icono del lápiz que se encuentra junto a ella para editar la regla.
4. Cuando edite una regla, siga estos pasos: Haga clic en el botón **Edit** que corresponde a la regla. En la lista desplegable Acción, elija **pasar**. Cambie el campo IPs de origen y el campo IPs de destino a los hosts o redes en los que no desea que la regla alerte. Haga clic en **Guardar como nuevo**.

## Edit Rule 3:13921:5


[\(View Documentation, Rule Comment\)](#)

Message	IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling me		
Classification	Attempted Administrator Privilege Gain <span>▼</span>		
	<a href="#">Edit Classifications</a>		
Action	pass <span>▼</span>		
Protocol	tcp <span>▼</span>		
Direction	Directional <span>▼</span>		
Source IPs	any	Source Port	any
Destination IPs	\$HOME_NET	Destination Port	143

### Detection Options

<b>reference</b>	
<input type="text" value="url,secunia.com/advisories/24596"/>	
<b>reference</b>	
<input type="text" value="bugtraq,23058"/>	
<b>reference</b>	
<input type="text" value="cve,2007-1578"/>	
<b>metadata</b>	
<input type="text" value="engine shared, soid 3 13921, service imap"/>	
ack <span>▼</span> <input type="button" value="Add Option"/>	<input type="button" value="Save As New"/>

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

 **Success** ✕  
Successfully created new rule "IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling memory corruption attempt"

**Edit Rule** 3:1000000:1 [\(View Documentation, Rule Comment\)](#)

Message:

Classification:  ▼  
[Edit Classifications](#)

Action:  ▼

Protocol:  ▼

Direction:  ▼

Source IPs:  Source Port:

Destination IPs:  Destination Port:

### Detection Options

**reference**

**reference**

**reference**

**metadata**

▼

## Habilitar una regla de paso

Debe habilitar la nueva regla en la política de intrusiones apropiada para pasar tráfico en las direcciones de origen o de destino especificadas. Siga estos pasos para habilitar una regla de paso:

1. Modifique la política de intrusiones activa: Navegue hasta **Políticas > Control de acceso > Intrusión**. Haga clic en **Editar** junto a la política de intrusión activa.
2. Agregue la nueva regla a la lista de reglas: Haga clic en **Reglas** en el panel izquierdo. Introduzca la ID de regla que ha indicado anteriormente en el cuadro de

filtro. Marque la casilla de verificación Reglas y cambie el Estado de regla para **Generar eventos**. Haga clic en **Información de política** en el panel izquierdo. Haga clic en **Registrar cambios**.

3. Haga clic en **Implementar** para implementar los cambios en el dispositivo.

## Verificación

Debe supervisar los nuevos eventos durante algún tiempo para asegurarse de que no se generen eventos para esta regla específica para la dirección IP de origen o de destino definida.

## Troubleshoot

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