

Configuración para ver los cambios en una política de control de acceso

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo ver/verificar los cambios realizados en una política de control de acceso (ACP). Esto también se aplica para determinar los cambios realizados en la configuración de la interfaz.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower

Componentes Utilizados

La información de este documento se basa en Firepower Management Center 6.1.0.5 y superiores.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

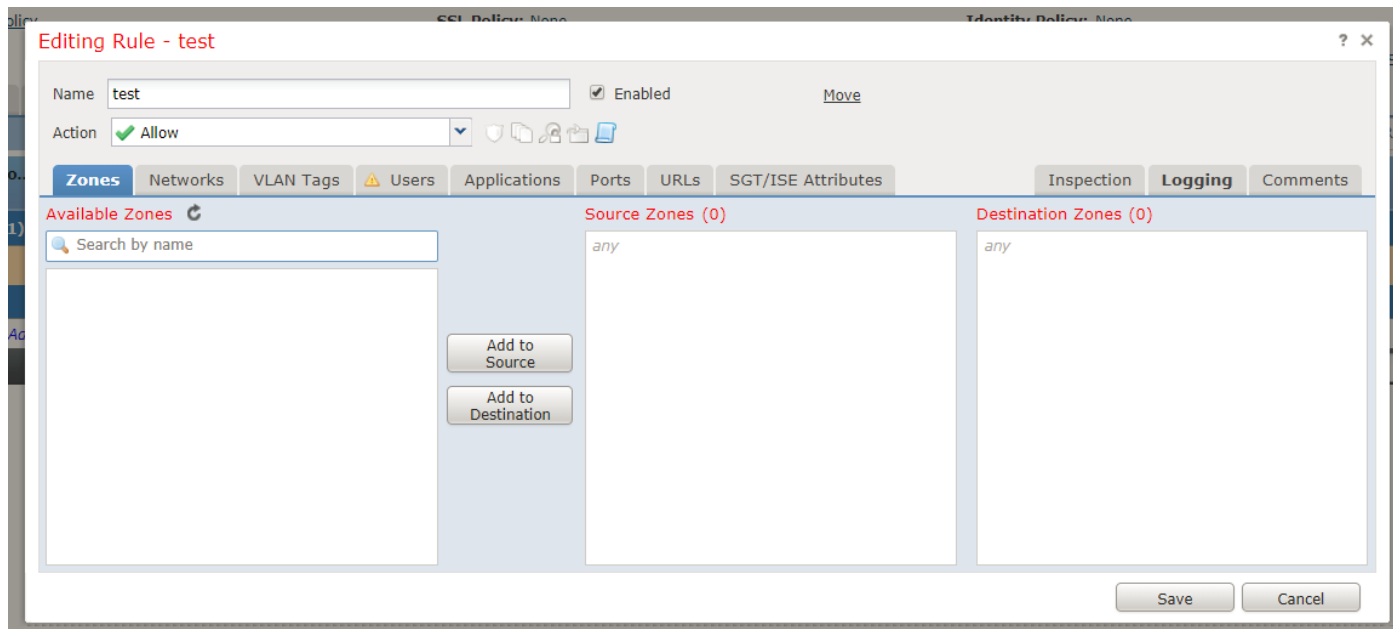
Configuraciones

Paso 1. Inicie sesión en la GUI del Firepower Management Center con privilegios de administrador.

Paso 2. Navegue hasta **Políticas > Control de acceso** y haga clic para editar (o incluso crear) una directiva nueva.

Ejemplo:

Realice algunos cambios en la política. Por ejemplo, agregue una nueva regla, como se muestra en la imagen:



Paso 3. A continuación, guarde los cambios de política.

Paso 4. Ahora, navegue hasta **Sistema > Supervisión > Auditoría** y busque el registro del cambio que acaba de realizar. Aparece como se muestra en esta imagen:



Paso 5. Ahora puede ver un registro, como se muestra en la imagen anterior, en su primera línea **Guardar política <Policy_name>** junto con un icono junto a él (resaltado).

Paso 6. Haga clic en el icono y se redirigirá a una página diferente que muestra los cambios/adiciones/modificaciones detallados realizados en la política.

Policy-Test (2018-01-10 03:48:53/admin)	
Policy Information	
Last Modified	2018-01-10 03:48:53

Policy-Test (2018-01-10 03:51:15/admin)	
Policy Information	
Last Modified	2018-01-10 03:51:15
Mandatory Rule	
Rule 1	
Name	test
Enabled	True
Action	PERMIT
Variable Set	Default Set
Log at Beginning of Connection	True
Log at End of Connection	False
Log File Events	False
Send Events to Defense Center	True

Verificación

Estos registros están disponibles en el punto en que los registros de auditoría no se borran.

Troubleshoot

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