# Configure Firesight Management Center para mostrar los recuentos de visitas por regla de acceso

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Configuraciones Verificación Troubleshoot

### Introducción

Este documento describe cómo configurar la página personalizada de flujo de trabajo/visor de eventos para representar los recuentos de aciertos de conexión por nombre de regla de acceso. La configuración muestra un ejemplo básico del campo de nombre de regla asociado a los recuentos de visitas y cómo agregar campos adicionales si es necesario.

### Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower
- · Conocimiento de la navegación básica en el Firesight Management Center

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower Management Center versión 6.1.X y posterior
- Aplicable a los sensores de Firepower/Threat Defense gestionados

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

#### Configuraciones

Paso 1. Inicie sesión en Firesight Management Center con privilegios de administrador.

Una vez que el login se realiza correctamente, navegue hasta **Analysis > Custom > Custom Workflows**, como se muestra en la imagen:

Overview Analysis Policies Devices Objects AMP Intelligence						Syste	m Help 🖷	admin <del>v</del>					
Context Explorer	Connections •	Intrusions 🔻	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Custom + Custom Workflows	Lookup 🔻	Search			
												reate Custo	m Workflow
Custom Workflow								Table					
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality Intrusion Events with Destination Criticality									🕞 🥒 🗊				
Events with Destination, Impact, and Host Criticality Current Events by Time, Impact, and Host Criticality Intrusion Events with Destination Criticality									🕞 🥒 🗊				
Hosts with Servers Default Workflow Hosts with Servers								🔒 🥒 🗎					
Intrusion Events with Destination Criticality Default Workflow Intrusion Events with Destination Criticality								🔒 🥔 🗎					
Intrusion Events with Source Criticality Default Workflow Intrusion Events with Source Criticality								🕞 🥔 🗐					
Server and Host Details Network Server Information with Server OS						Hosts with Servers	Hosts with Servers				🔒 🥒 🖯		

Paso 2. Haga clic en **Crear flujo de trabajo personalizado** y elija los parámetros como se muestra en la imagen:



Paso 3. Seleccione el campo de tabla como **Eventos de conexión** e introduzca un nombre de flujo de trabajo y haga clic en **Guardar**. Una vez guardado el flujo de trabajo, haga clic en **Agregar página** como se muestra en la imagen:

Creatin	g Wa	orl	kflow							
Name	Н		Access Control Policy							
Descriptio	n		Access Control Rule Action							
Table	Co	Application Protocol Application Protocol Business Relevance								
Page 1			Application Protocol Category Application Protocol Risk Application Protocol Tag							×
Page Nam	e H		Application Risk Business Relevance							
Sort Type		1	Client Client Business Relevance							
Column	1		Client Category Client Risk		Column 3		Column 4		Column 5	
Sort Pri	ority		Client Tag	d	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1 \$		~	Count     DNS Query	cess Control 🗘	•	\$	•	\$	<b>\$</b>	\$
			DNS Record Type DNS Response DNS Sinkhole Name							Save Cancel
			DNS TTL							

**Nota:** La primera columna debe ser Count y, a continuación, en la columna adicional, puede elegir entre los campos disponibles en la lista desplegable. En este caso, la primera columna es Count y la segunda columna es Access Control Rule (Regla de control de acceso).

Paso 4. Una vez agregada la página de flujo de trabajo, haga clic en Guardar.

Para ver los recuentos de aciertos, navegue hasta **Análisis > Conexiones > Eventos** y haga clic en **Flujos de Trabajo del Switch**, como se muestra en la imagen:

Overview Analysis Policies	s Devices	Objects	AMP Intell	igence					
Context Explorer Connections	s ► Events	Intrusions 🔻	Files 🔻	Hosts 🔹	Users • Vulne	rabilities 🔻	Correlation •		
Connection Events ×									
Connection Events	s > Table View of Connection Events								
Connections by Application									
Connections by Initiator									
Connections by Port									
Connections by Responder	ast Actio	n <u>Reason</u>	Initiator Initiato	Initiator	Responder IP	Responder	Ingress		
Connections over Time	acket		IP	Country		Country	Security Zone		
Hit-Counts	Allow		10.1.1.5		52.39.210.199	USA			
Traffic by Application	Allow		10 1 1 5		10 76 77 50				
Traffic by Initiator	Allow		<u> 10.1.1.5</u>		<u>10.76.77.50</u>				
Traffic by Port	Allow		<u> 10.1.1.5</u>		<u>10.76.77.50</u>				
Traffic by Responder	Allow		<u> 10.1.1.5</u>		<u>52.39.210.199</u>	USA			
Traffic over Time • Unique Initiators by Responder	Allow		<u>10.1.1.5</u>		<u>10.106.38.75</u>				
Unique Responders by Initiator	Allow		<u>10.1.1.5</u>		<u>10.106.38.75</u>				
2017-07-19 08:47:13	Allow		<u>10.1.1.5</u>		<u>10.76.77.50</u>				
↓ _ <u>2017-07-19 08:47:08</u>	Allow		<u>10.1.1.5</u>		<u>10.76.77.50</u>				
2017-07-19 08:47:08	Allow		<u>10.1.1.5</u>		172.217.7.238	USA			

caso, Hit-Counts), como se muestra en la imagen:

Hit-Counts (switch workflow) Hit-Counts Based on Access Control		■ <u>2017-07-19 07:36:06 - 2017-07-19 08:52:39</u> Expanding
No Search Constraints (Edit Search)		
Jump to 🔻		
▼ Count	Access Control Rule	
4 🗋 66	Default-Allow	
		Displaying row 1 of 1 rows  < < Page 1 of 1 >>

### Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

### Troubleshoot

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