Centro de administración de Firepower: Vea los contadores de coincidencias de políticas de control de acceso

Contenido

Introducción

Prerequisites

Este documento describe las instrucciones para crear **flujos de trabajo personalizados en FirePower Management Center (FMC) que permiten que el sistema muestre los contadores de visitas de la política de control de acceso (ACP) a nivel global y según las normas.** Esto es útil para solucionar problemas, independientemente de si el flujo de tráfico coincide con la regla correcta. También es útil obtener información sobre el uso general de las reglas de control de acceso; por ejemplo, las reglas de control de acceso sin visitas durante un período de tiempo prolongado pueden ser indicación de que la regla ya no es necesaria y que podría eliminarse de forma segura del sistema.

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

- Virtual FirePower Management Center (FMC), versión de software 6.1.0.1 (build 53)
- FirePower Threat Defense (FTD) 4150, versión de software 6.1.0.1 (build 53)

> **Nota:** La información descrita en este documento no se aplica a FirePower Device Manager (FDM).

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.

Productos Relacionados

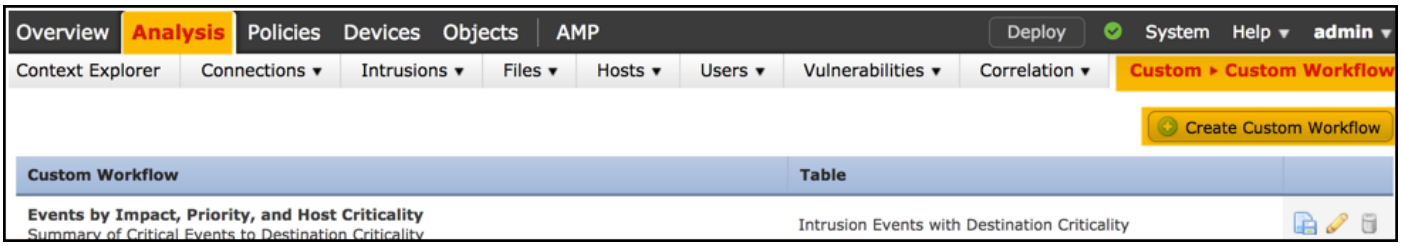
Este documento también puede utilizarse con estas versiones de software y hardware:

- FirePower Management Center (FMC), versión de software 6.0.x y posterior
- Dispositivos administrados de FirePower, versión de software 6.1.x y posterior

Configurar

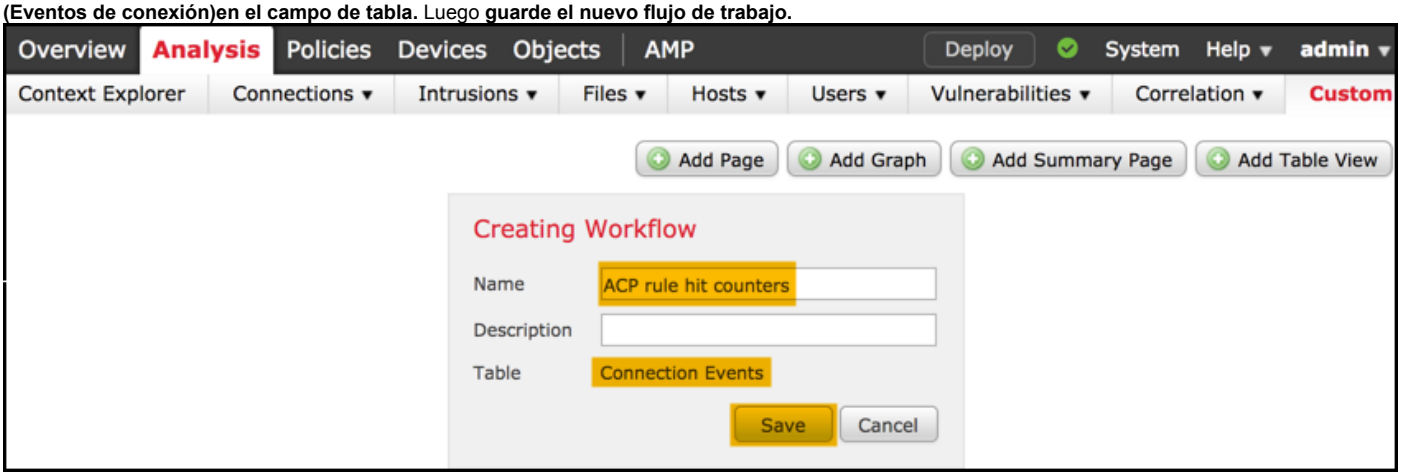
Paso 1

Para crear un flujo de trabajo personalizado, navegue hasta **Analysis > Custom > Custom Workflows > Create Custom Workflow (Análisis > Personalizar > Flujos de trabajo personalizados > Crear flujo de trabajo personalizado):**



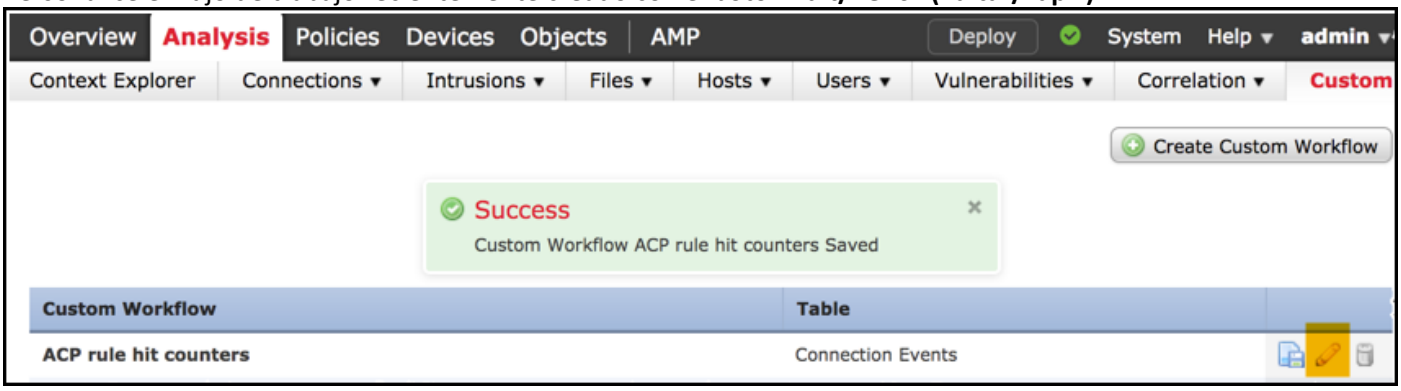
Paso 2

Defina el nombre del **flujo de trabajo personalizado, por ejemplo, contadores de visitas de la regla de la ACP, y seleccione Connection Events (Eventos de conexión)en el campo de tabla.** Luego **guarde el nuevo flujo de trabajo.**



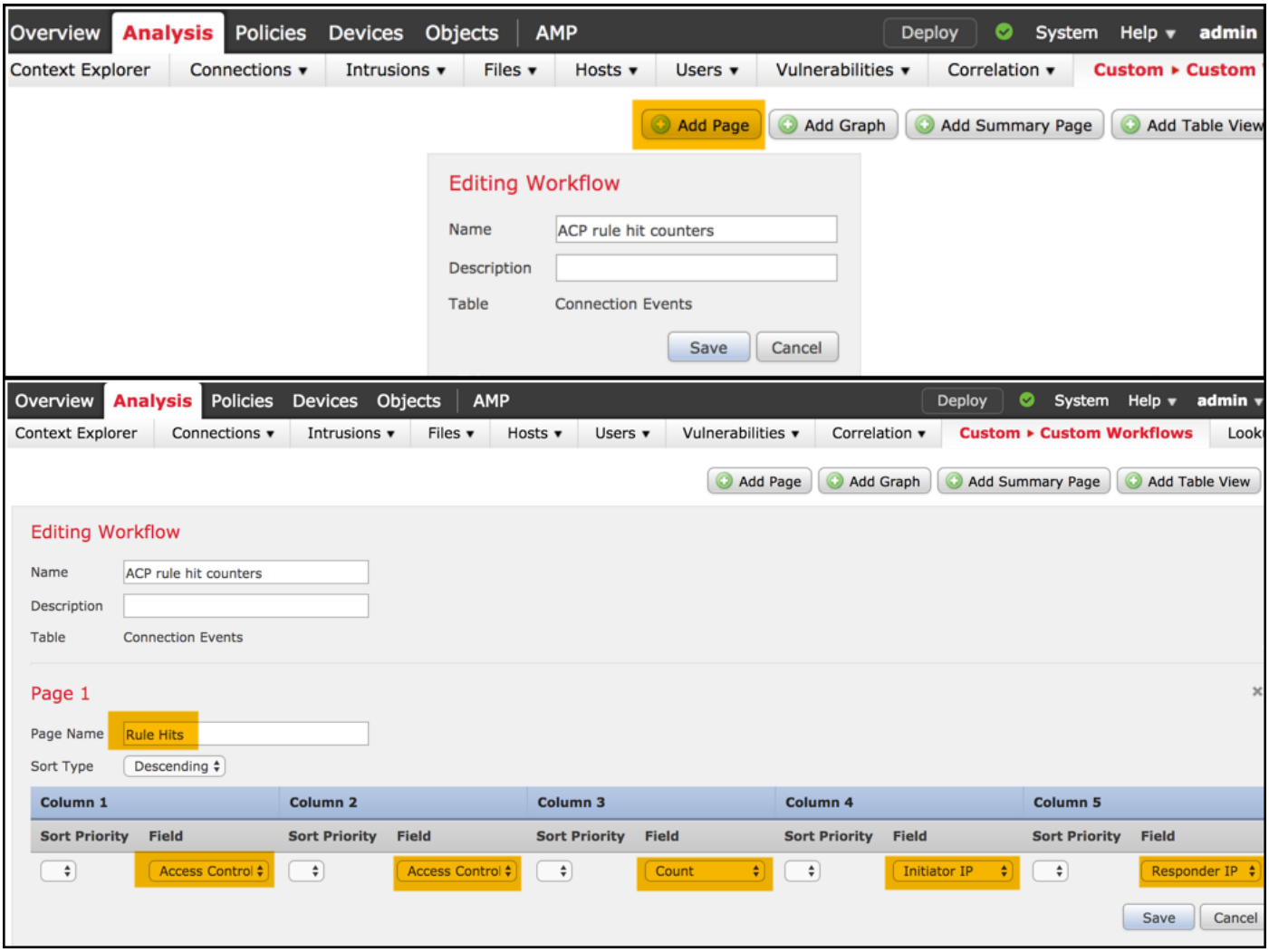
Paso 3

Personalice el flujo de trabajo recientemente creado con el botón **Edit/Pencil (Editar/Lápiz).**



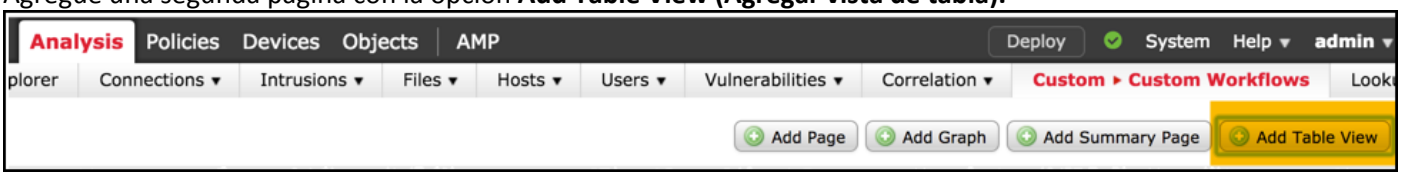
Paso 4

Agregue una página nueva para un flujo de trabajo con la opción **Add Page (Agregar página), defina su nombre y ordene los campos de la columna como Access Control Policy (Política de control de acceso), Access Control Rule (Regla de control de acceso) y los campos Count (Recuento), Initiator IP (IP del iniciador) y Responder IP (IP del transmisor).**



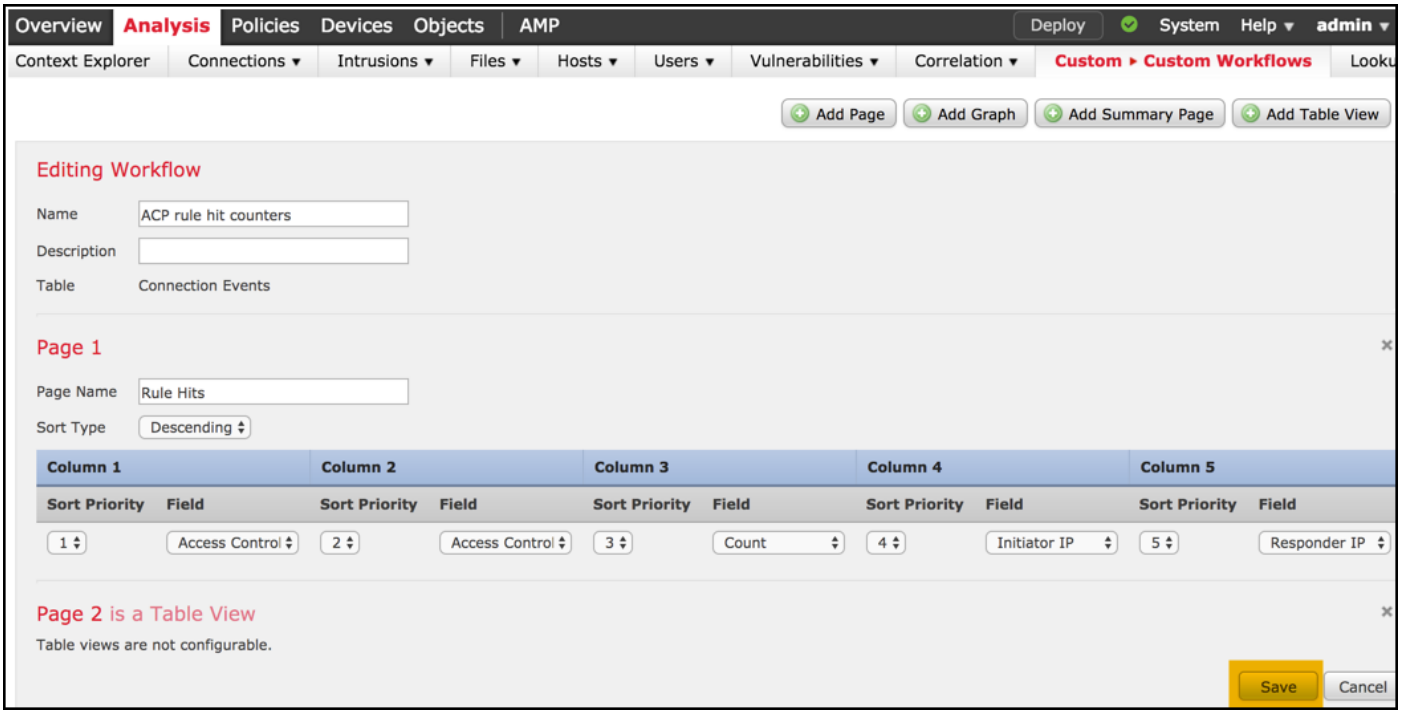
Paso 5

Agregue una segunda página con la opción **Add Table View (Agregar vista de tabla).**



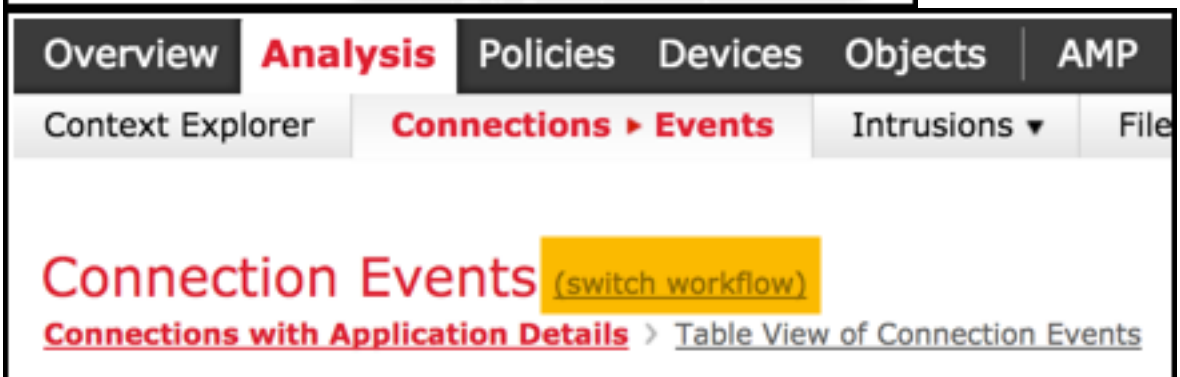
Paso 6

La **vista de tabla no se puede configurar; proceda guardando el flujo de trabajo.**

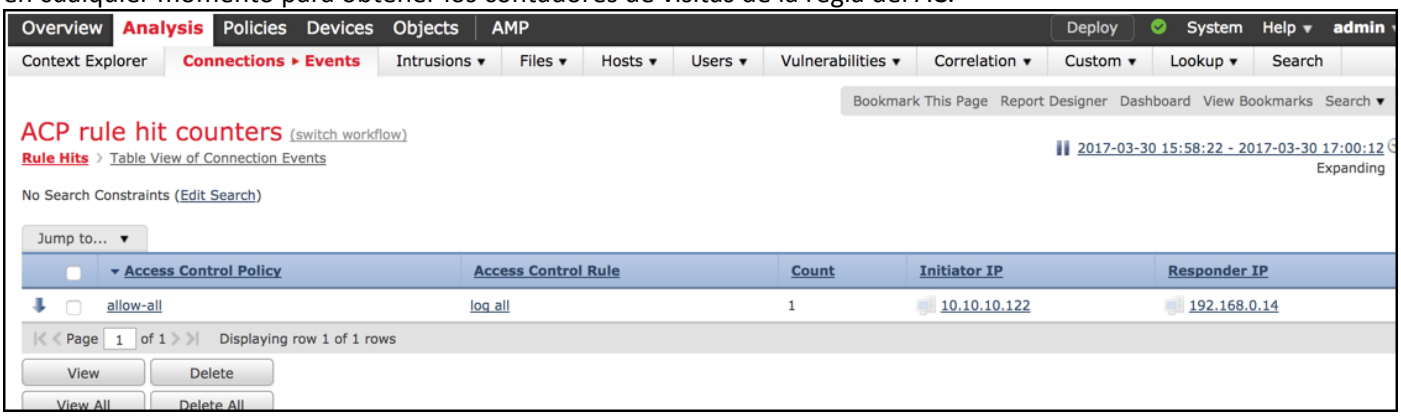


Paso 7

Navegue hasta **Analysis > Connections Events (Análisis > Eventos de conexión)**, seleccione el switch de flujo de trabajo y el flujo de trabajo recientemente creado llamado **Contador de visitas de la regla de la ACP, y espere hasta que la página se vuelva a cargar.**



Una vez que se carga la página, se muestran los contadores de visitas por cada regla de la ACP. Actualice esta vista en cualquier momento para obtener los contadores de visitas de la regla del AC.



Verificación

Una manera de confirmar los contadores de visitas de la regla de control de acceso según las normas para todo el tráfico (global) es el comando del FTD en CLISH (SHELL de la CLI) **show access-control-config, que se demuestra a continuación:**

```
> show access-control-config

==================[ allow-all ]====================
Description :
Default Action : Allow
Default Policy : Balanced Security and Connectivity
Logging Configuration
 DC : Disabled
 Beginning : Disabled
 End : Disabled
Rule Hits : 0
Variable Set : Default-Set
…(output omitted)

----------------[ Rule: log all ]------------------
Action : Allow
 Intrusion Policy : Balanced Security and Connectivity
 ISE Metadata :

 Source Networks : 10.10.10.0/24
 Destination Networks : 192.168.0.0/24
 URLs
 Logging Configuration
 DC : Enabled
 Beginning : Enabled
 End : Enabled
 Files : Disabled
Rule Hits : 3
Variable Set : Default-Set

… (output omitted)
```

Troubleshoot

Con el comando **firewall-engine-debug puede confirmar si se evaluó el flujo de tráfico conforme a la regla de control de acceso adecuada:**

```
> system support firewall-engine-debug

Please specify an IP protocol: icmp
Please specify a client IP address: 10.10.10.122
Please specify a server IP address: 192.168.0.14
Monitoring firewall engine debug messages

10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 New session
10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0
-> 0, vlan 0, sgt tag: untagged, svc 3501, payload 0, client 2000003501, misc 0, user 9999997, icmpType 8, icmpCode
0
10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 no match rule order 1, id 2017150 dst network and GEO
10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 match rule order 3, 'log all', action Allow
10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 allow action
```

Cuando compara los contadores de visitas de la regla de la ACP denominada **Registrar todo, advierte que los resultados de la línea de comandos (CLI) y la GUI no coinciden.** El motivo es que los contadores de visitas de la CLI se borran después de la implementación de cada política de control de acceso y se aplican a todo el tráfico a nivel global, no solo a una dirección IP específica. Por otro lado, la GUI de FMC conserva los contadores en la base de datos, por lo que se pueden ver los datos históricos en función de los plazos seleccionados.

Información Relacionada

- Flujos de trabajo personalizados
- Introducción a las políticas de control de acceso
- Soporte Técnico y Documentación - Cisco Systems