Firepower Management Center: Exibir contadores de ocorrências de políticas do controle de acesso

Contents

Introduction

Prerequisites

Este documento descreve as instruções para criar **Fluxos de trabalho personalizados no Firepower Management Center (FMC), permitindo que o sistema exiba os contadores de ocorrências da política de controle de acesso (ACPI) de forma global e por regra.** Isso é útil para solucionar problemas, caso o fluxo de tráfego corresponda à regra correta. Também é útil obter informações sobre o uso geral das regras de controle de acesso, por exemplo, as regras de controle de acesso sem ocorrências por um período prolongado podem ser um indicação de que a regra não é mais necessária e pode ser removida com segurança do sistema.

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

- Virtual Firepower Management Center (FMC) - versão do software 6.1.0.1 (compilação 53)
- Firepower Threat Defense (FTD) 4150 - versão do software 6.1.0.1 (compilação 53)

> **Note**: As informações descritas neste documento não são aplicáveis para o 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

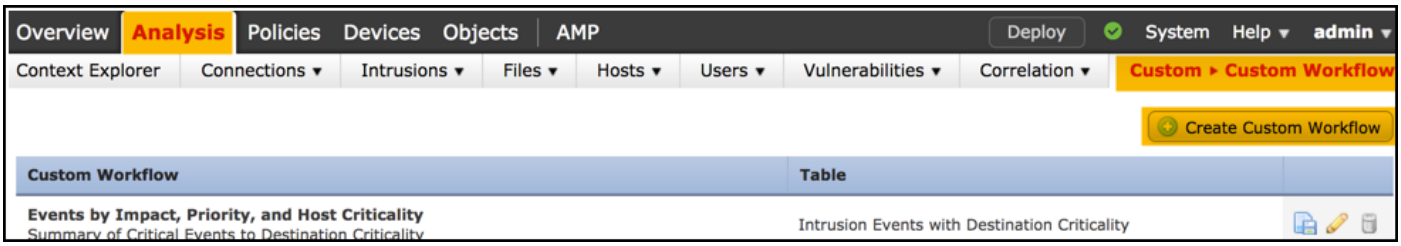
Este documento também pode ser usado com as seguintes versões de hardware e software:

- Firepower Management Center (FMC) - versão do software 6.0 e posterior
- Dispositivos gerenciados do Firepower - versão do software 6.1.x e posterior

Configurar

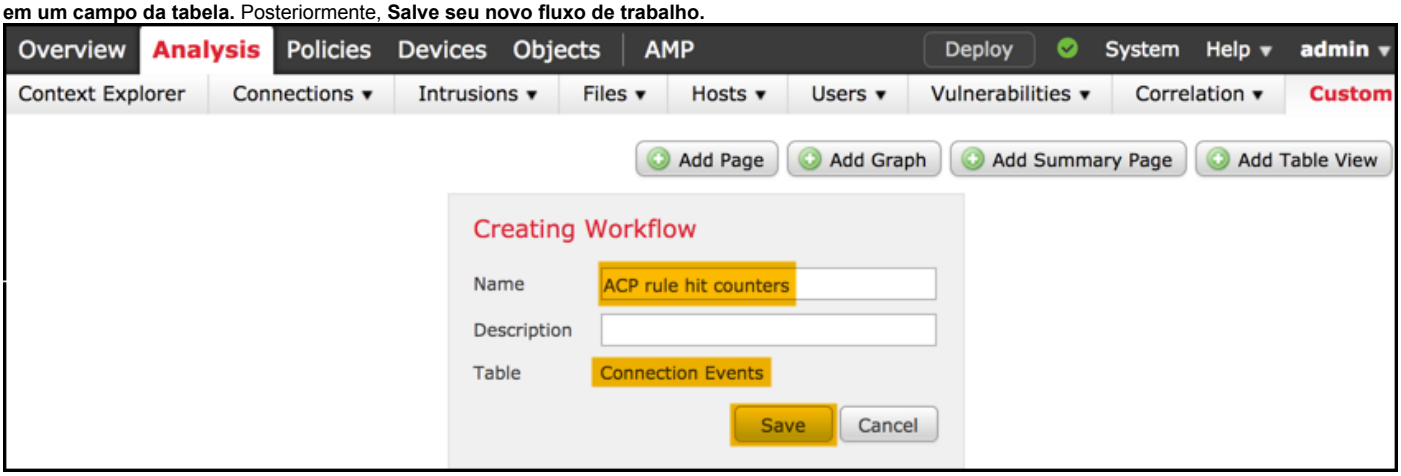
Passo 1

Para criar um fluxo de trabalho personalizado, navegue por **Analysis > Custom > Custom Workflows > Create Custom Workflow (Análise > Personalizar > Fluxos de trabalho personalizados > Criar fluxo de trabalho):**



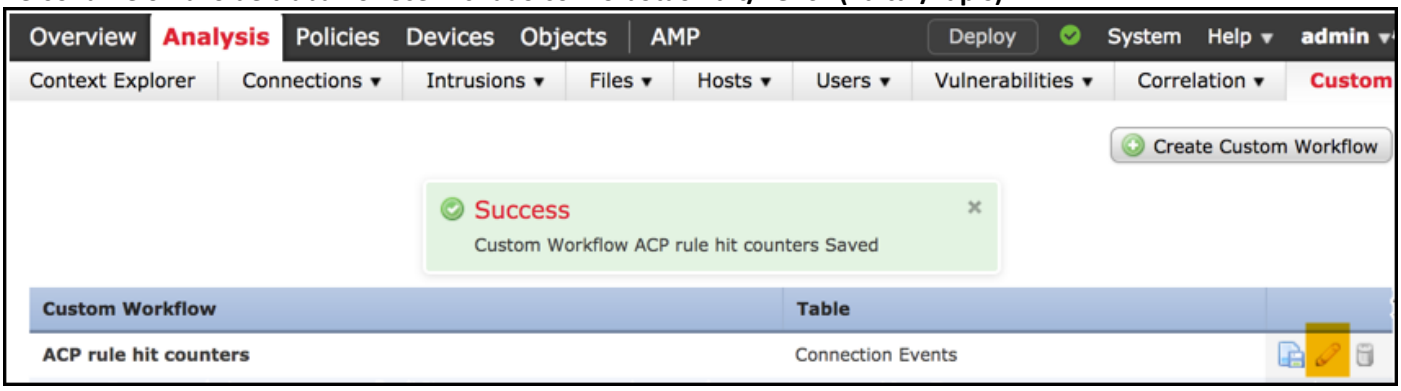
Passo 2

Defina o nome do **Fluxo de trabalho, por exemplo contadores de ocorrências de regra de ACP e selecione Connection Events (Eventos de conexão) em um campo da tabela.** Posteriormente, **Salve seu novo fluxo de trabalho.**



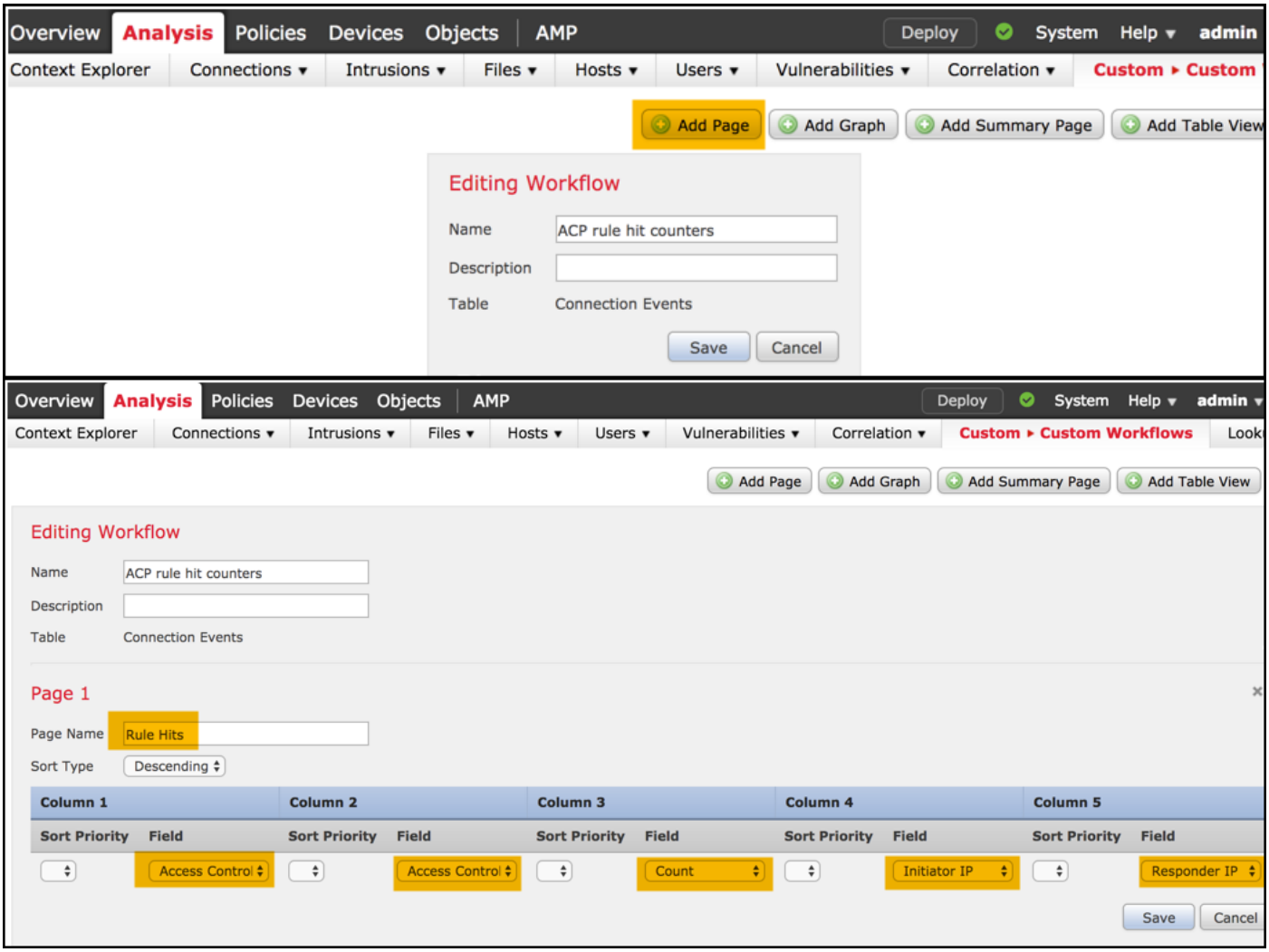
Etapa 3

Personalize o fluxo de trabalho recém-criado com o botão **Edit/Pencil (Editar/Lápis).**



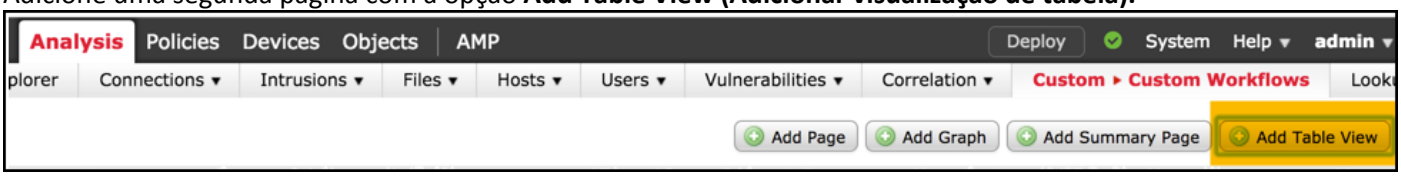
Passo 4

Adicione uma nova página para um fluxo de trabalho com a opção **Add Page (Adicionar página), defina o nome e classifique os campos da coluna em Access Control Policy** (Política de controle de acesso), **Access Control Rule (Regra de controle de acesso) e nos campos Count** (Contagem), **Initiator IP (IP iniciador) e Responder IP (IP de resposta).**



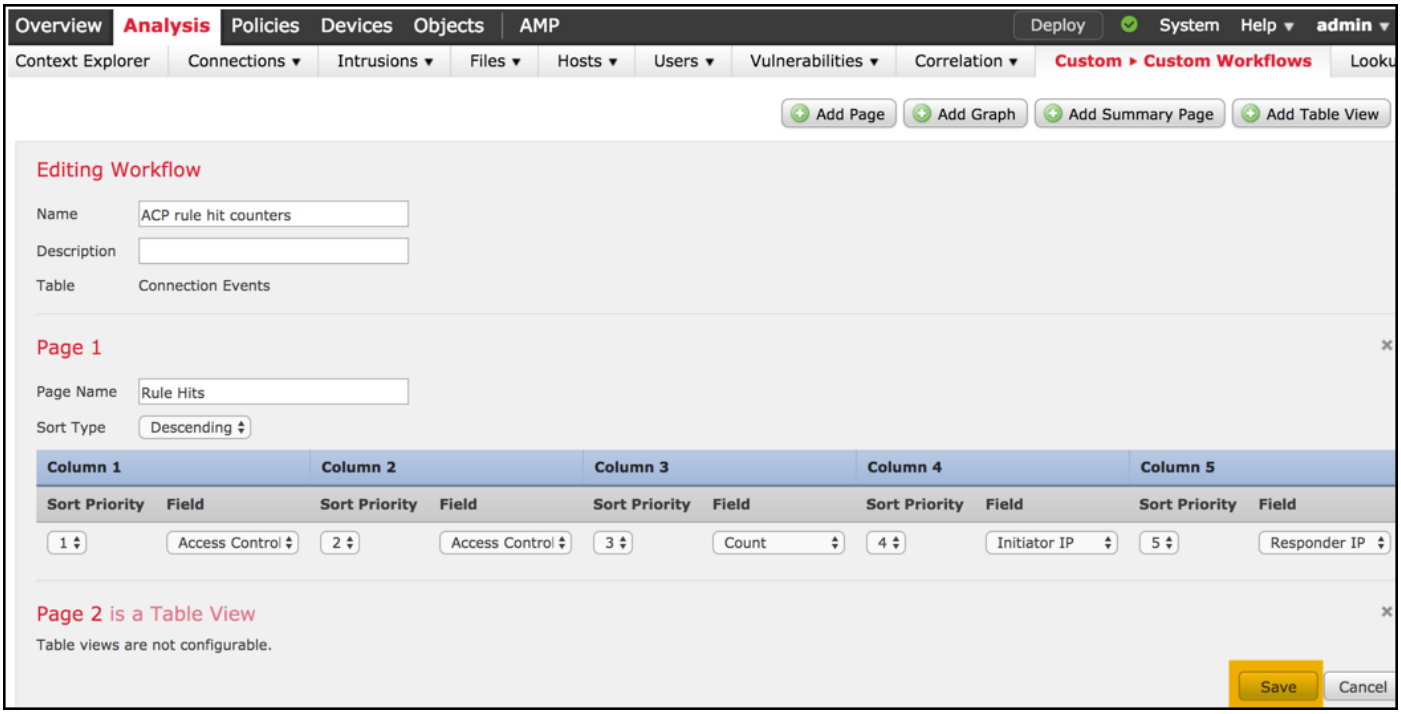
Etapa 5

Adicione uma segunda página com a opção **Add Table View (Adicionar visualização de tabela).**



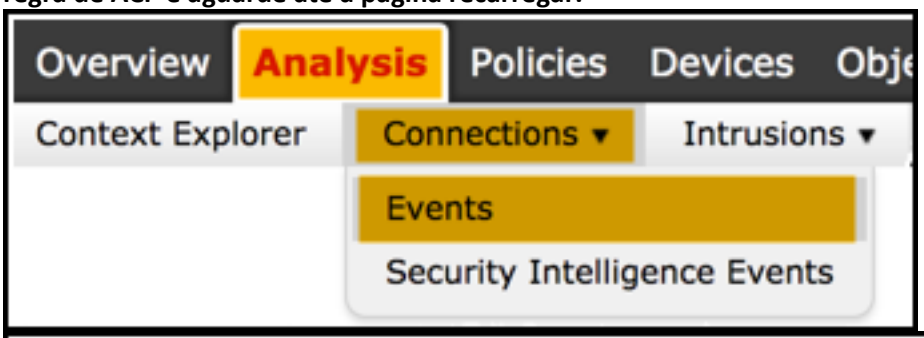
Etapa 6

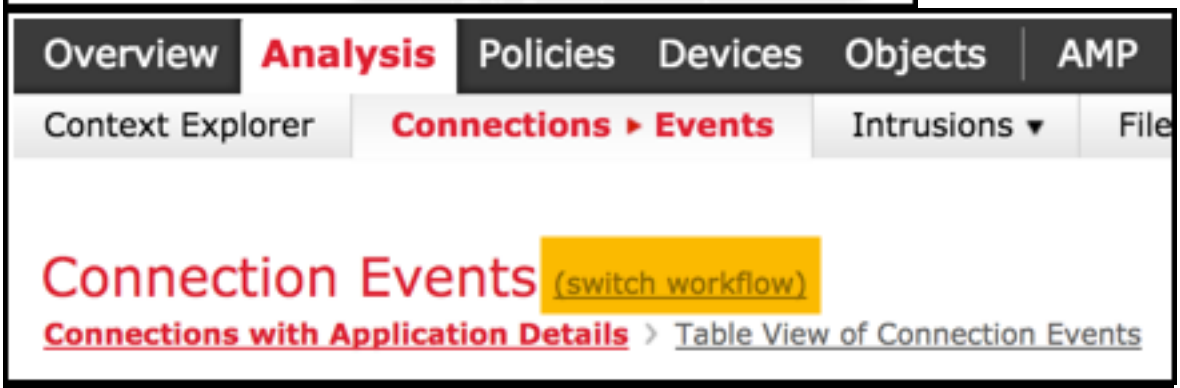
Table View (Visualização de tabela) não é configurável, portanto, apenas continue com Save para salvar o fluxo de trabalho.



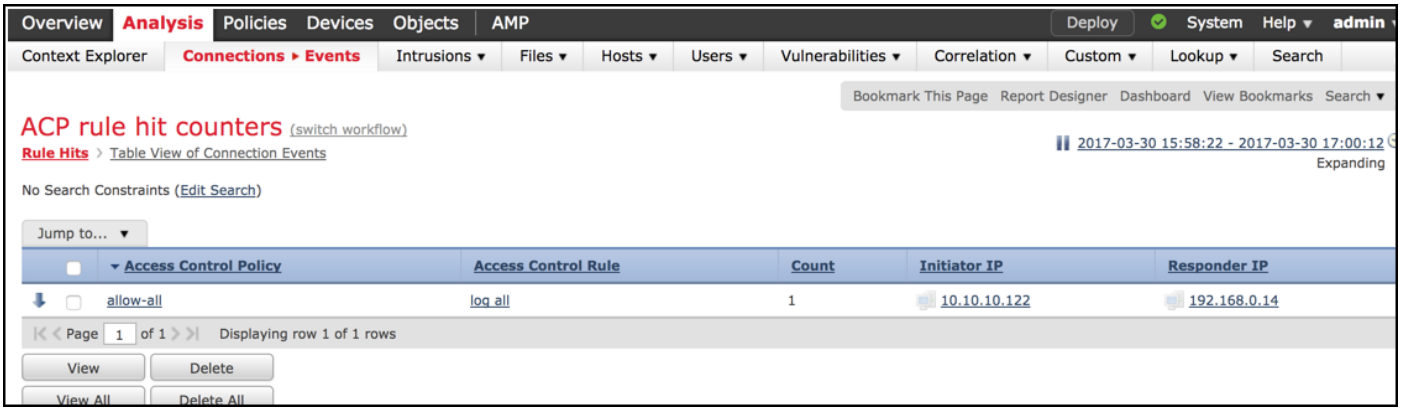
Etapa 7

Navegue até **Analysis > Connections Events** (Análise > Eventos de conexões) e selecione **Switch Workflow** (Fluxo de trabalho do switch), em seguida, escolha o fluxo de trabalho recém-criado chamado **contadores de ocorrências de regra de ACP e aguarde até a página recarregar.**





Depois que a página for carregada, os contadores de ocorrências de regra por cada regra ACP são exibidos, apenas atualize essa exibição sempre que quiser obter os contadores de ocorrências recentes da regra de controle de acesso.



Verificar

Uma forma de confirmar os contadores de ocorrências de regras de controle de acesso com base na regra para todo o tráfego (globalmente) pode ser obtida com o comando CLISH FTD (CLI SHELL) **show access-control-config demonstrado abaixo:**

```
> 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

Com o comando **firewall-engine-debug você pode confirmar se o fluxo de tráfego é avaliado em relação à regra de controle de acesso apropriada:**

```
> 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
```

Ao comparar os contadores de ocorrências para a regra de ACP chamado **log all você observa que as saídas de linha de comando (CLI) e da interface de usuário não coincidem.** O motivo é que os contadores de ocorrências da CLI são removidos após cada implantação da Política de controle de acesso e se aplicam a todo o tráfego globalmente e não a endereços IP específicos. Por outro lado, a interface de usuário do FMC mantém os contadores no banco de dados, para que possa exibir os dados históricos com base em um período determinado.

Informações Relacionadas

- Fluxo de trabalho personalizados
- Introdução às políticas de controle de acesso
- Suporte Técnico e Documentação - Cisco Systems