Centro de gerenciamento da potência de fogo: Contadores de acertos da política do controle de acesso do indicador

Índice

Introdução

Pré-requisitos

Este documento descreve as instruções para criar **trabalhos feitos sob encomenda em um** centro de gerenciamento da potência de fogo (FMC) que permita que o sistema indique contadores de acertos da política do controle de acesso (ACP) na base global e da por-regra. Isto é útil de pesquisar defeitos se o fluxo de tráfego combina a regra correta. É igualmente útil obter a informação sobre o uso geral das regras do controle de acesso, por exemplo o controle de acesso ordena sem batidas por um longo período do tempo pôde ser uma indicação que a regra não está precisada anymore e pôde potencialmente com segurança ser removido do sistema.

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

- Centro de gerenciamento virtual da potência de fogo (FMC) - versão de software 6.1.0.1 (construção 53)
- Defesa da ameaça da potência de fogo (FTD) 4150 - versão de software 6.1.0.1 (construção 53)

> Nota: A informação descrita neste documento não é aplicável ao gerenciador de dispositivo da potência de fogo (FDM).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Produtos Relacionados

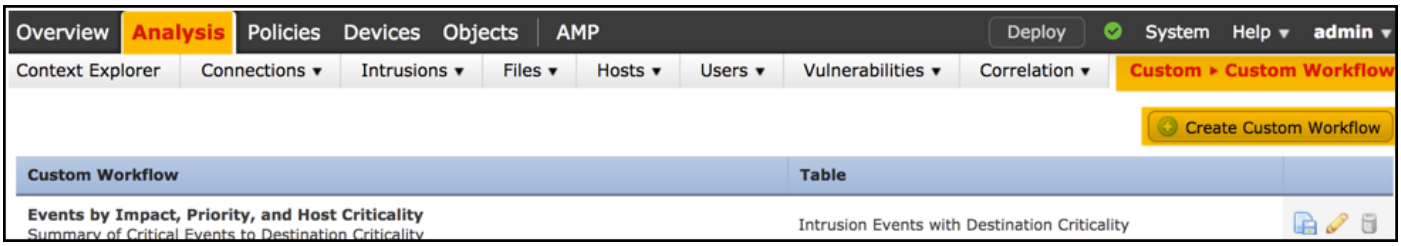
Este documento pode igualmente ser usado com estes versão de hardware e software:

- Centro de gerenciamento da potência de fogo (FMC) - versão de software 6.0.x e mais altamente
- Dispositivos controlados potência de fogo - versão de software 6.1.x e mais altamente

Configurar

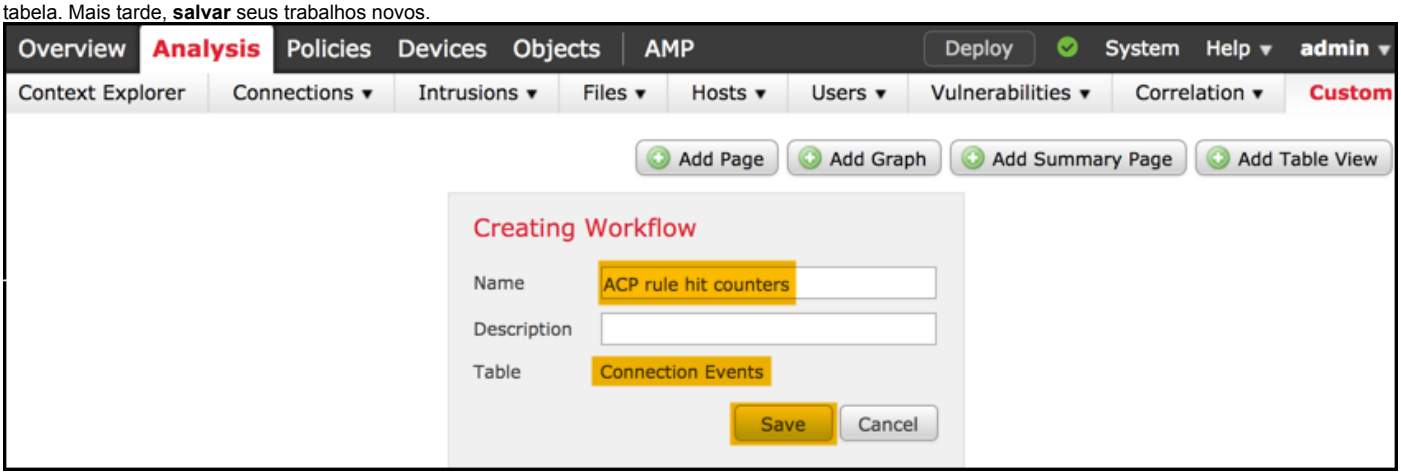
Passo 1

A fim criar uns trabalhos feitos sob encomenda, navegue à **análise > ao costume > trabalhos feitos sob encomenda > criam trabalhos feitos sob encomenda:**



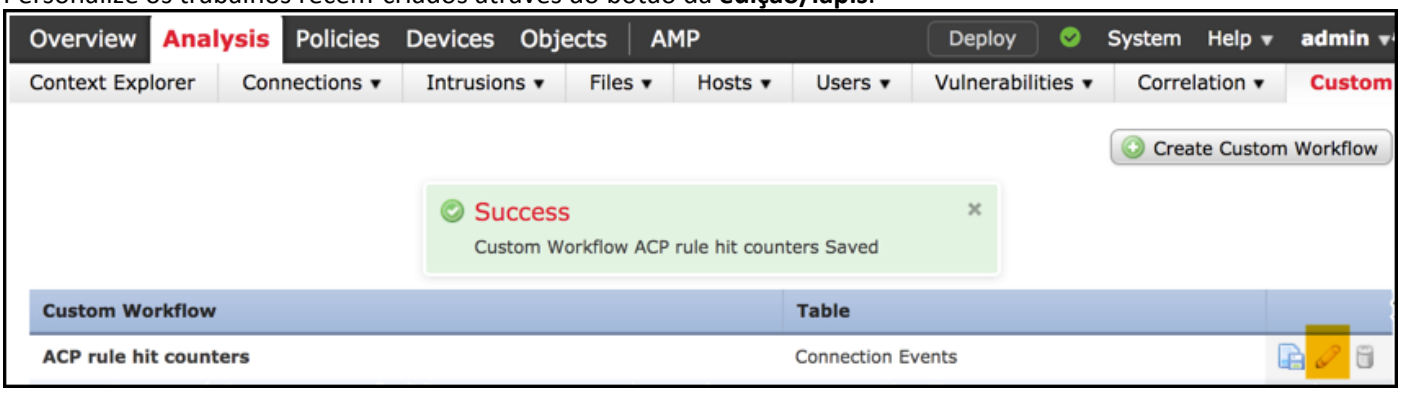
Passo 2

Defina o nome **feito sob encomenda dos trabalhos**, por exemplo **contadores de acertos da regra ACP** e **eventos de conexão** seletos em um campo da tabela. Mais tarde, **salvar** seus trabalhos novos.



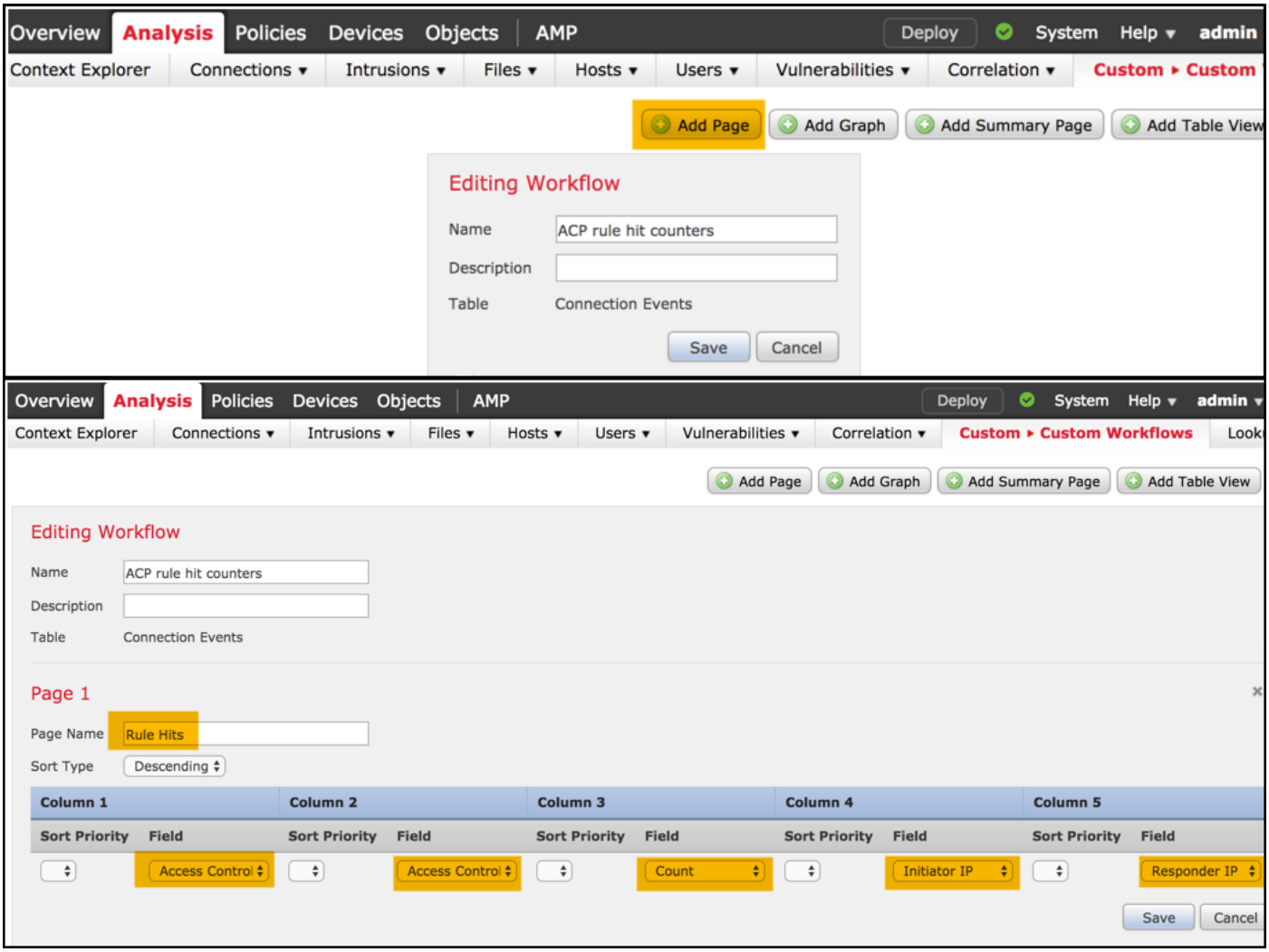
Etapa 3

Personalize os trabalhos recém-criados através do botão da **edição/lápis**.



Passo 4

Adicionar uma página nova para uns trabalhos com a opção de **página adicionar**, defina seu nome e classifique os campos da coluna pela **política do controle de acesso**, **regra do controle de acesso** e pelo **IP da contagem**, do **iniciador** e **IP do que responde** campos.

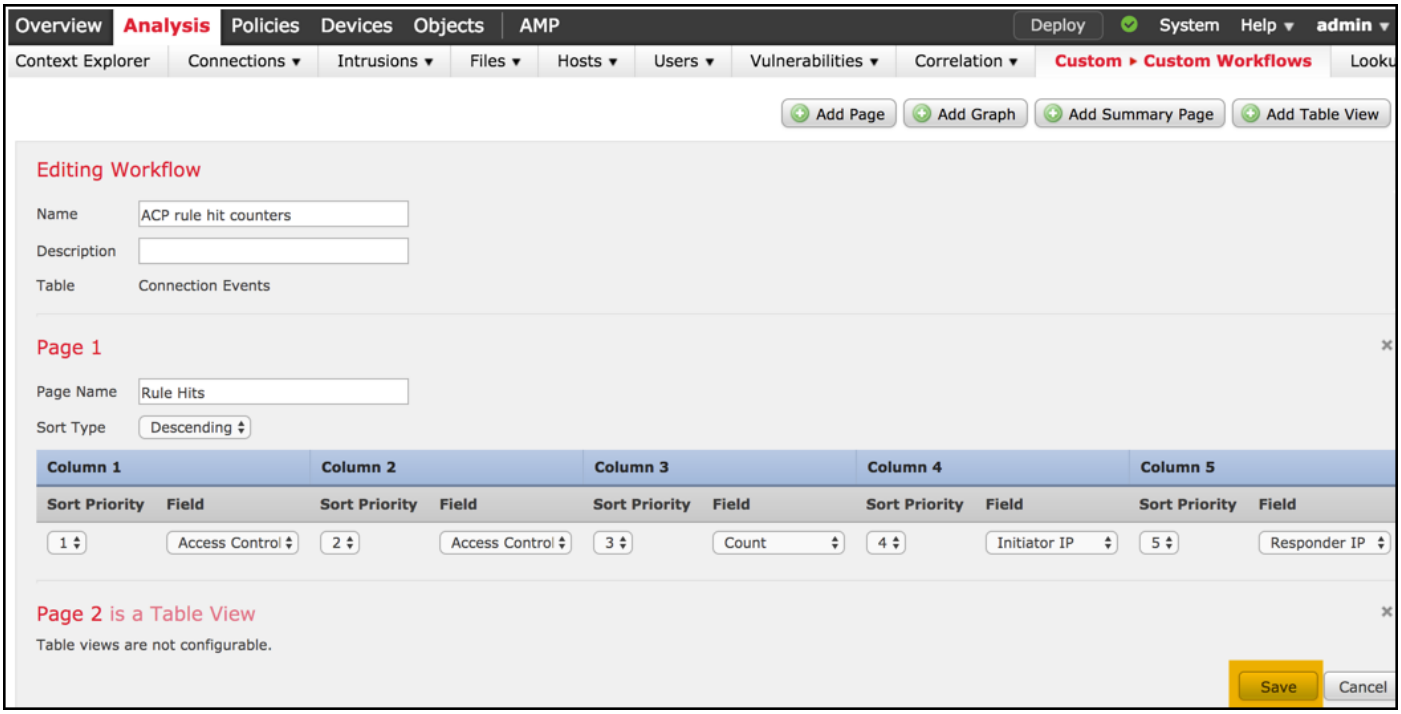


Etapa 5

Adicionar uma segunda página com a opção da **opinião da tabela adicionar**.

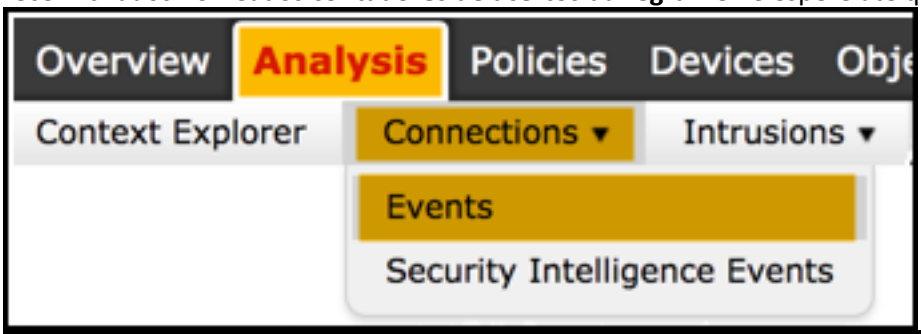
Etapa 6

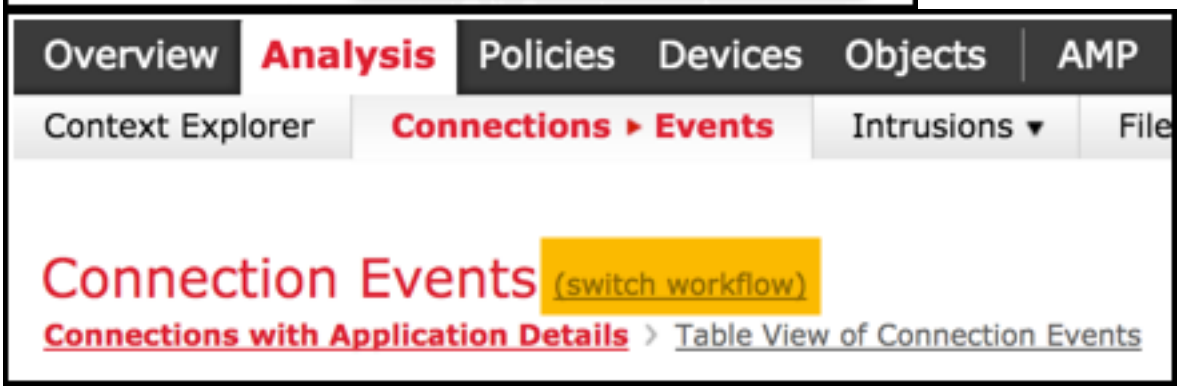
A opinião da tabela não é configurável, daqui apenas continua **salvar** seus trabalhos.



Etapa 7

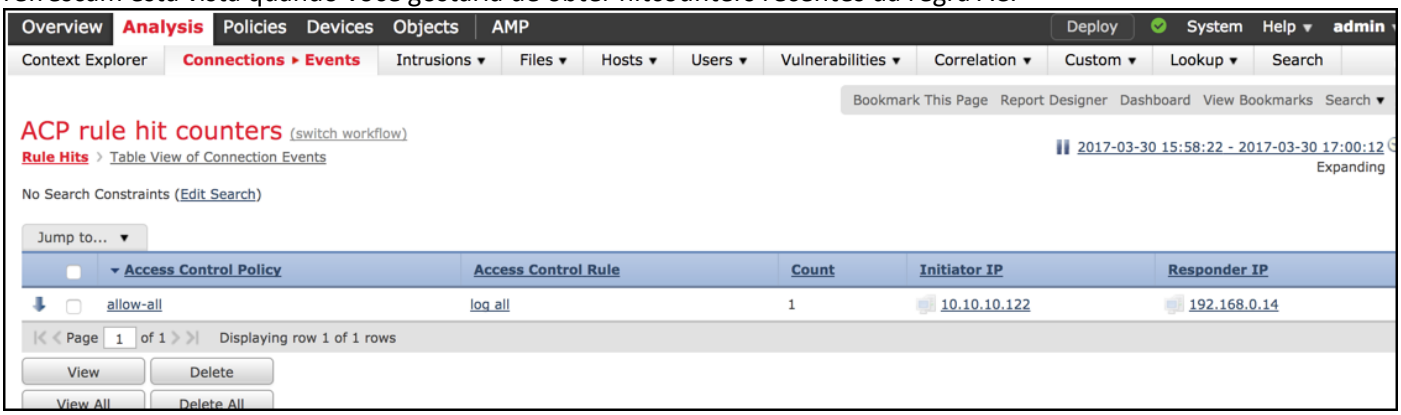
Navegue aos **eventos da análise > das conexões** e aos **trabalhos do interruptor** seleto, a seguir escolha os trabalhos recém-criados nomeados **contadores de acertos da regra ACP** e espere até que os reloads da página.





Uma vez que a página é carregada, os contadores de acertos da regra por cada regra ACP são indicados, apenas

refrescam esta vista quando você gostaria de obter hitcounters recentes da regra AC.



Verificar

Uma maneira de confirmar contadores de acertos da regra do controle de acesso na base da regra para todo o tráfego (globalmente) pode ser conseguida do comando da acesso-controle-**configuração da mostra** FTD CLISH (SHELL CLI), que é 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)
```

Troubleshooting

Com o comando Firewall-motor-**debugar** você pode confirmar se o fluxo de tráfego está avaliado contra a regra apropriada do controle de acesso:

```
> 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
```

Quando você compara os contadores de acertos para a regra ACP nomeada **log todo** você observa que a linha de comando (CLI) e as saídas GUI não combinam. A razão é que os contadores de acertos CLI estão cancelados após cada distribuição de política do controle de acesso e se aplicam a todo o tráfego globalmente e não ao endereços IP de Um ou Mais Servidores Cisco ICM NT específicos. Na outra mão, FMC GUI mantêm os contadores no base de dados, assim que podem indicar os dados históricos baseados em um tempo de frame selecionado.

Informações Relacionadas

- Trabalhos feitos sob encomenda
- Obtenção começado com políticas do controle de acesso
- Suporte Técnico e Documentação - Cisco Systems