Firepower 管理中心：显示访问控制策略点击计数器

目录

简介

先决条件

Firepower (FMC) **Firepower (FMC) (ACP)**

要求

本文档没有任何特定的要求。

- Firepower (FMC) - 6.1.0.1 53
- Firepower (FTD) 4150 - 6.1.0.1 53

注意：本文档中所述信息不适用于 Firepower 设备管理器 (FDM)。

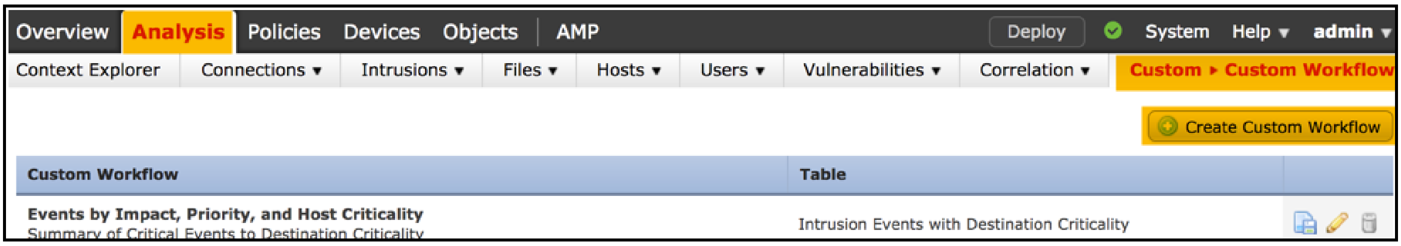
本文档也可用于以下硬件和软件版本：

- Firepower (FMC) - 6.0.x
- Firepower - 6.1.x

配置

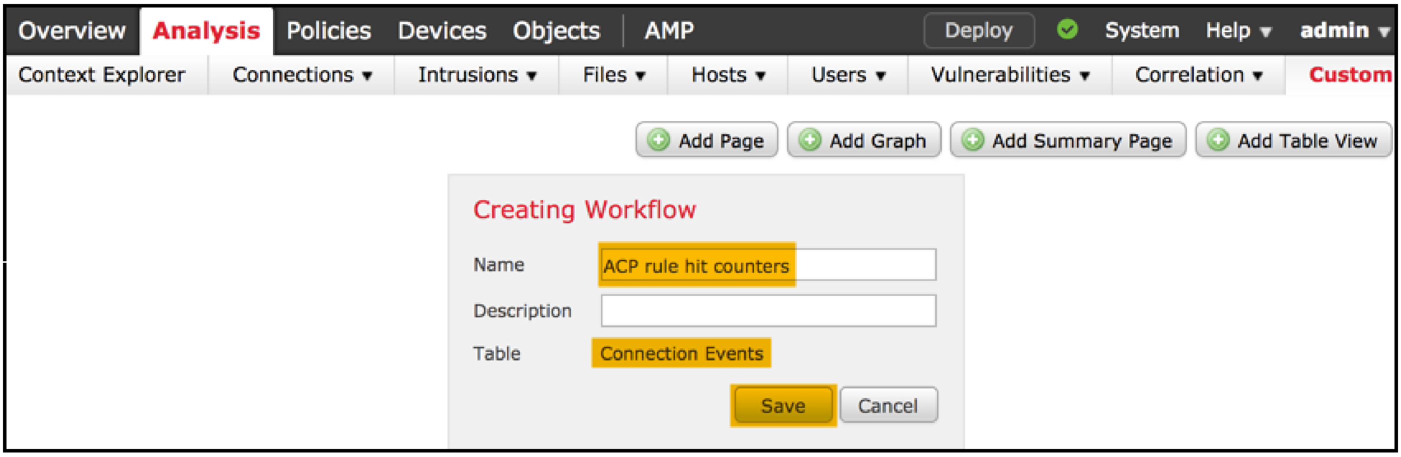
1

要创建自定义工作流程，请依次导航至**分析 > 自定义 > 自定义工作流程 > 创建自定义工作流程**：



Custom Workflow	Table
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality	Intrusion Events with Destination Criticality

2
ACP



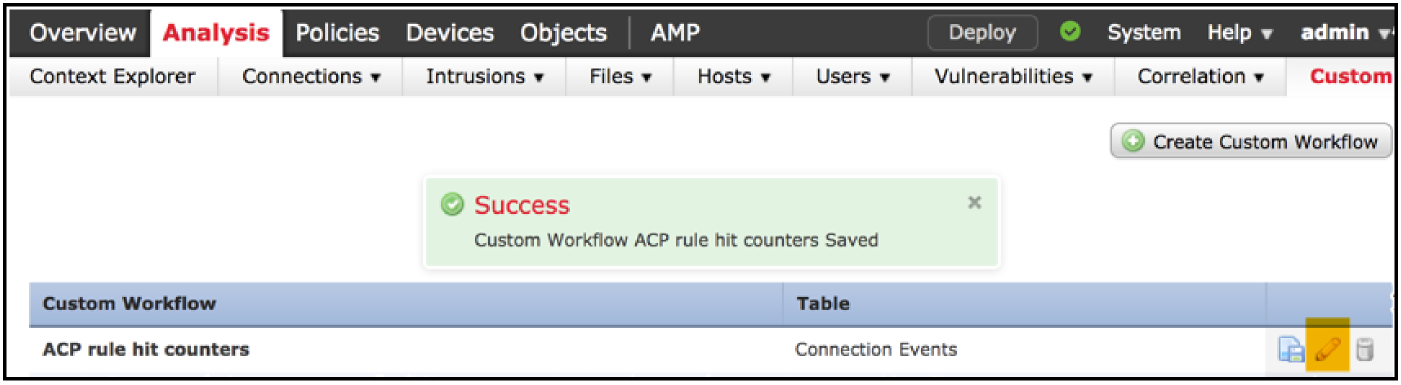
Creating Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events

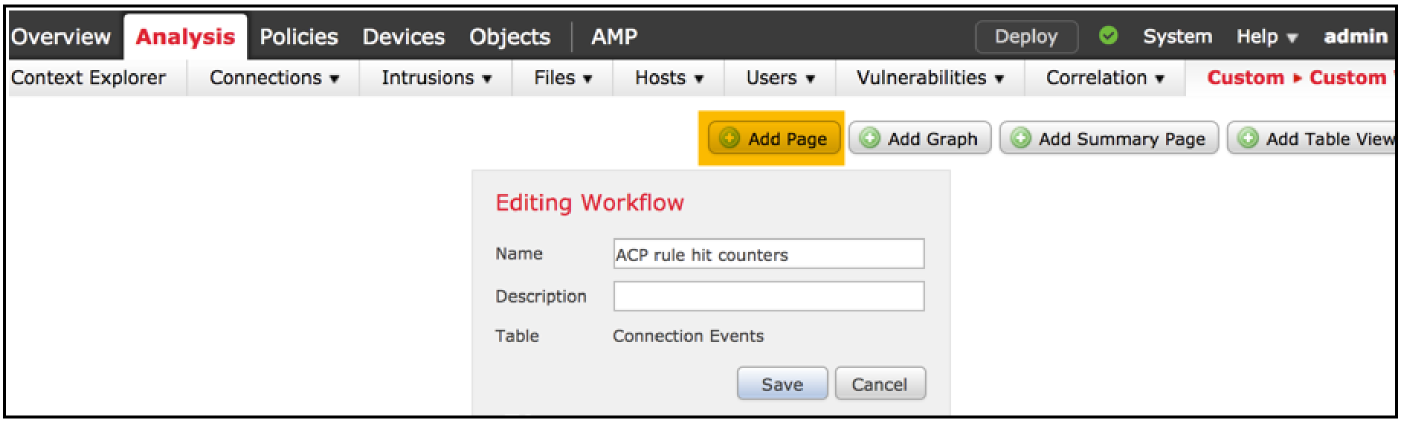
3
/



Success
Custom Workflow ACP rule hit counters Saved

Custom Workflow	Table
ACP rule hit counters	Connection Events

4
IP IP

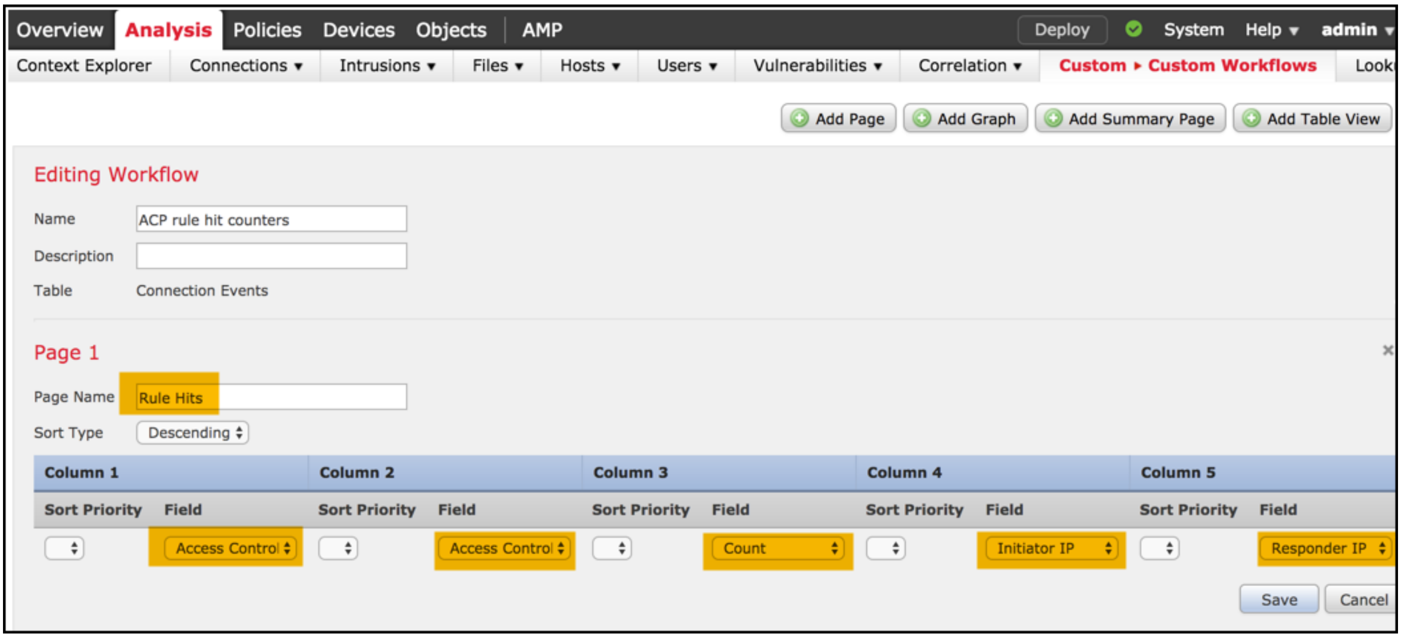


Editing Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events



Editing Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events

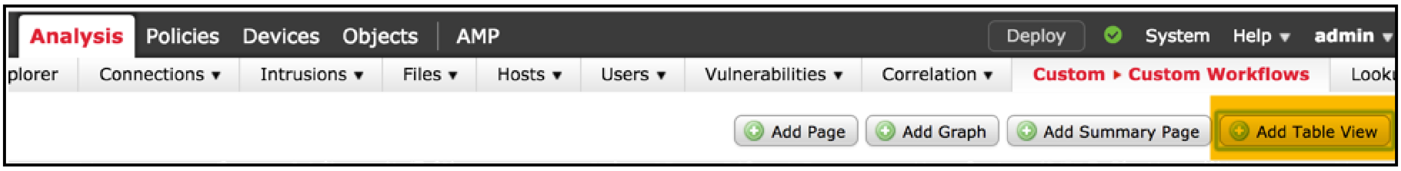
Page 1

Page Name: Rule Hits

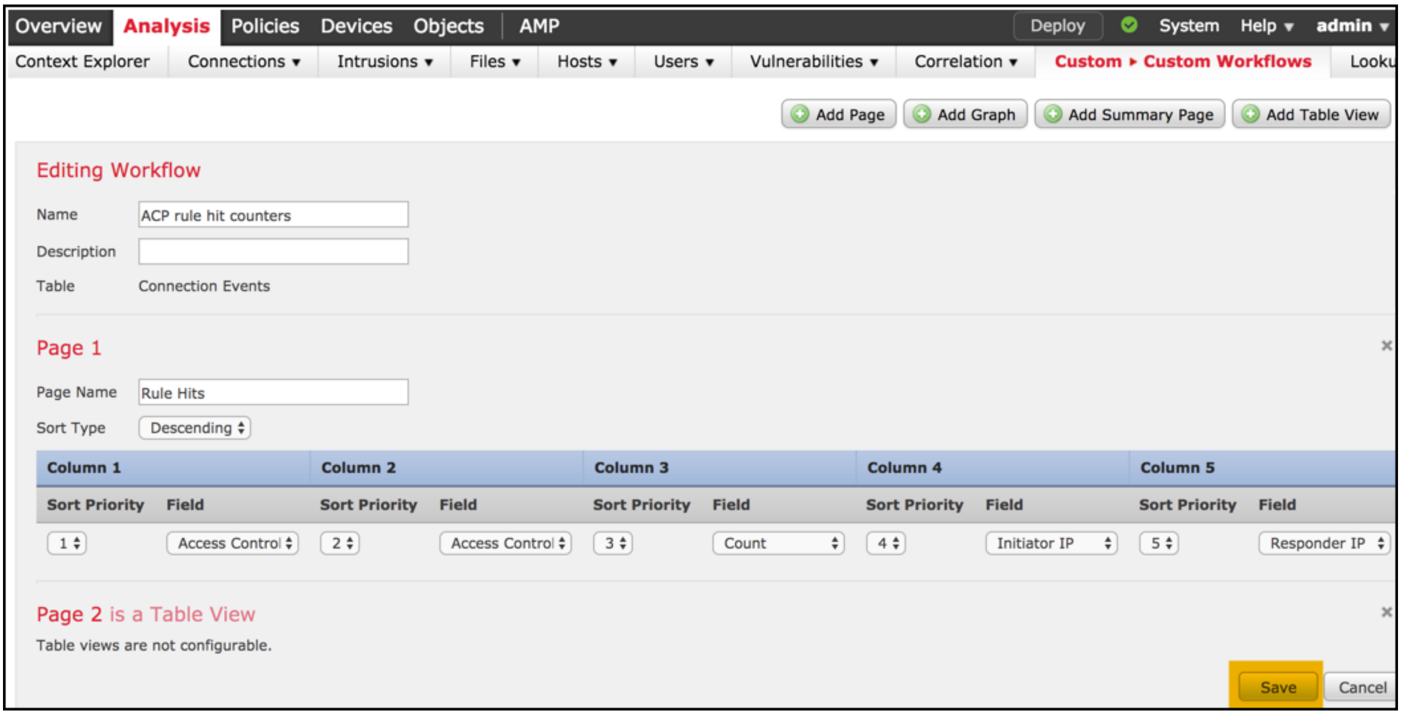
Sort Type: Descending

Column 1		Column 2		Column 3		Column 4		Column 5	
Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
	Access Control		Access Control		Count		Initiator IP		Responder IP

步驟 5



6



Editing Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events

Page 1

Page Name: Rule Hits

Sort Type: Descending

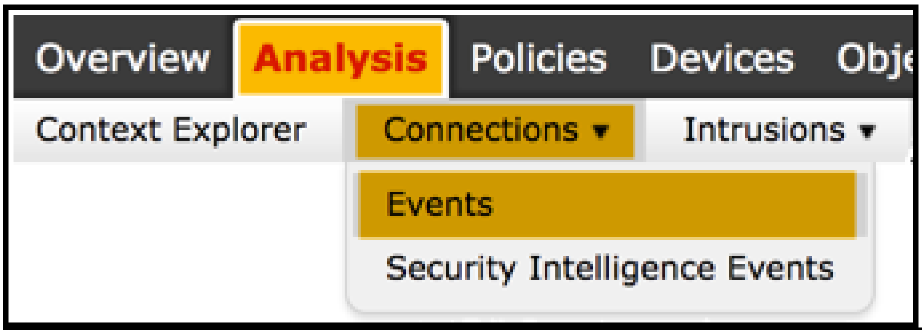
Column 1		Column 2		Column 3		Column 4		Column 5	
Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1	Access Control	2	Access Control	3	Count	4	Initiator IP	5	Responder IP

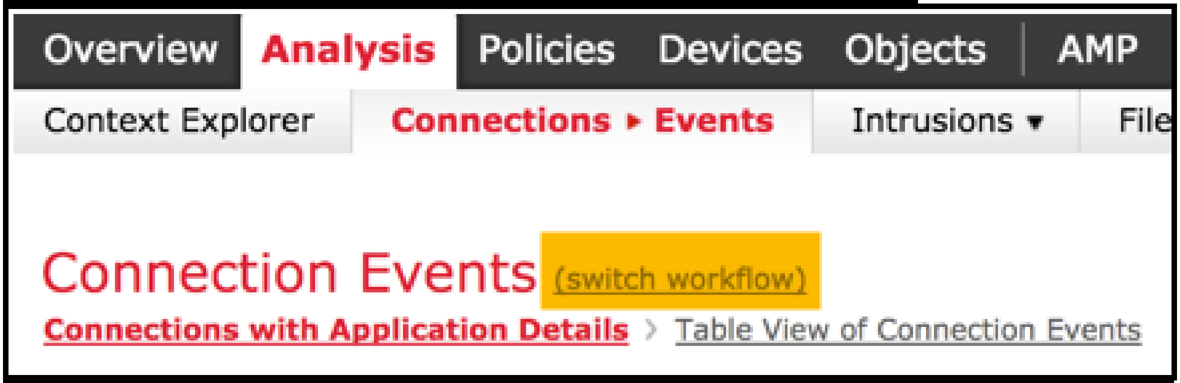
Page 2 is a Table View

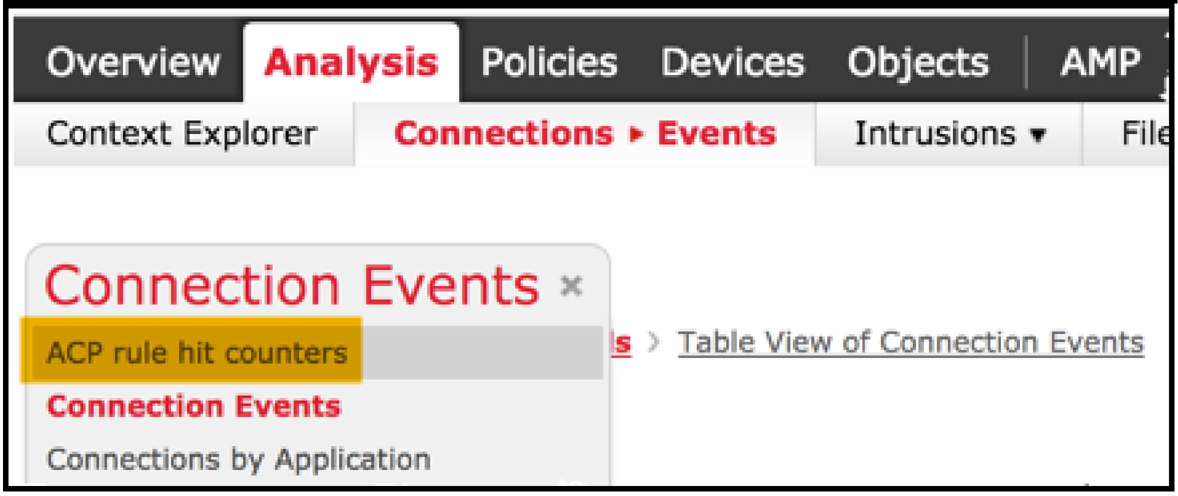
Table views are not configurable.

7

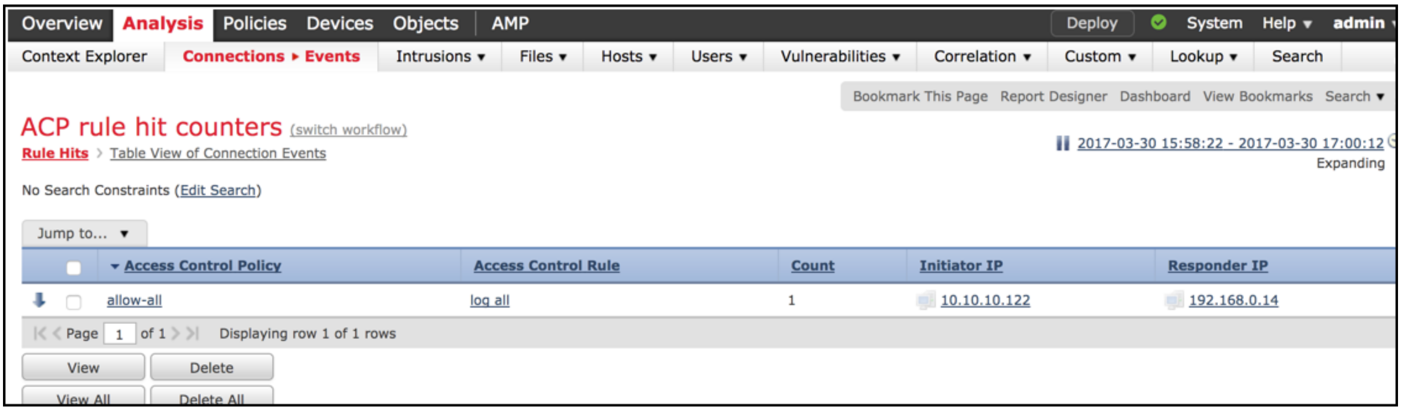
> ACP







ACP AC



ACP rule hit counters (switch workflow)
Rule Hits > Table View of Connection Events

2017-03-30 15:58:22 - 2017-03-30 17:00:12
Expanding

No Search Constraints (Edit Search)

Jump to... ▾

	Access Control Policy	Access Control Rule	Count	Initiator IP	Responder IP
□	allow-all	log all	1	10.10.10.122	192.168.0.14

Page 1 of 1 Displaying row 1 of 1 rows

验证

通过 FTD CLISH (CLI SHELL) show access-control-config 命令，可以根据规则确认所有流量（全局）的访问控制规则点击计数器，如下所示：

```
> 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)
```

故障排除

使用 firewall-engine-debug 命令，您可以确认是否根据正确的访问控制规则评估流量：

```
> 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
```

log all ACP (CLI) GUI CLI IP FMC GUI

相关信息

- [自定义工作流程]
- [访问控制策略使用入门]
- [技术支持和文档 - Cisco Systems]