Firepower管理中心：显示访问控制策略命中计数器

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

先决条件

Firepower(FMC)()

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：在本文描述的信息不是可适用的对Firepower设备管理器(FDM)。

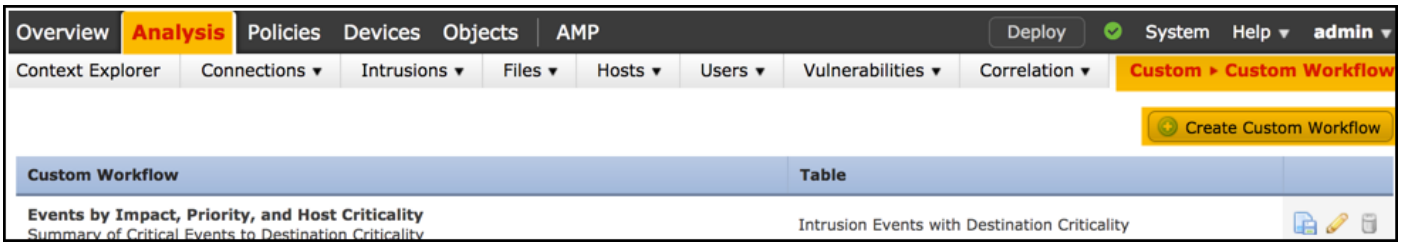
本文档也可用于以下硬件和软件版本：

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

配置

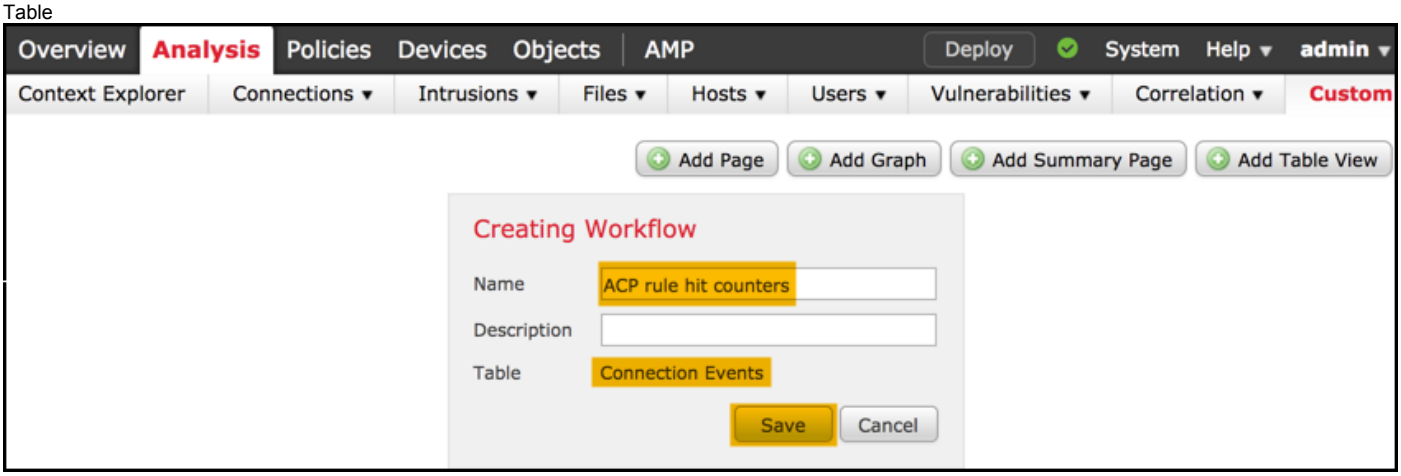
步骤 1

为了创建自定义工作流，请导航对**分析>自定义>自定义工作流>创建自定义工作流：**



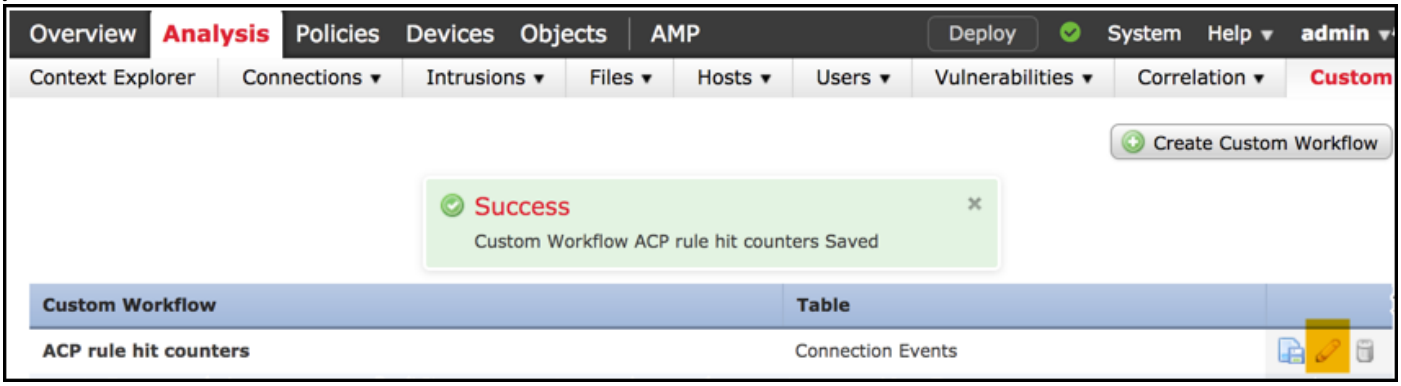
2

Table



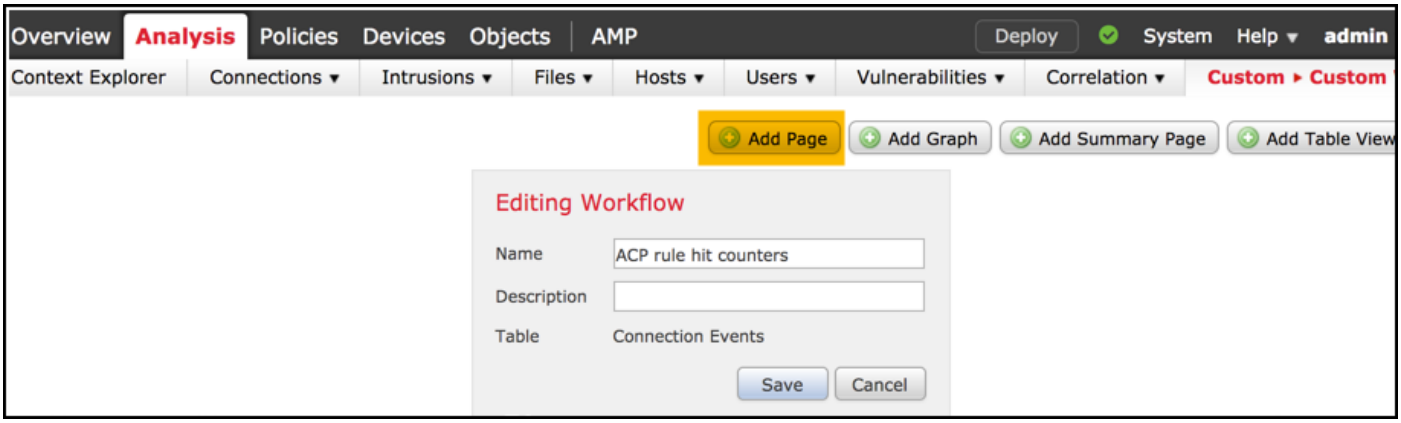
3

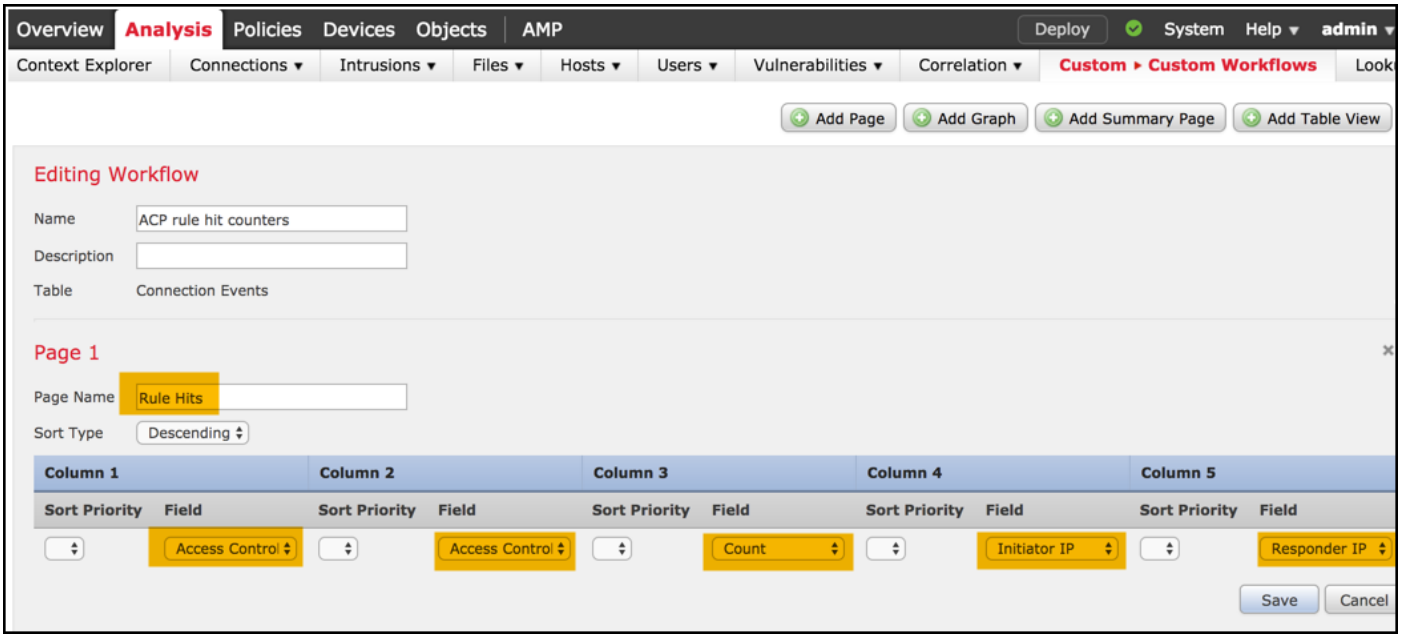
/



4

AddIPIP

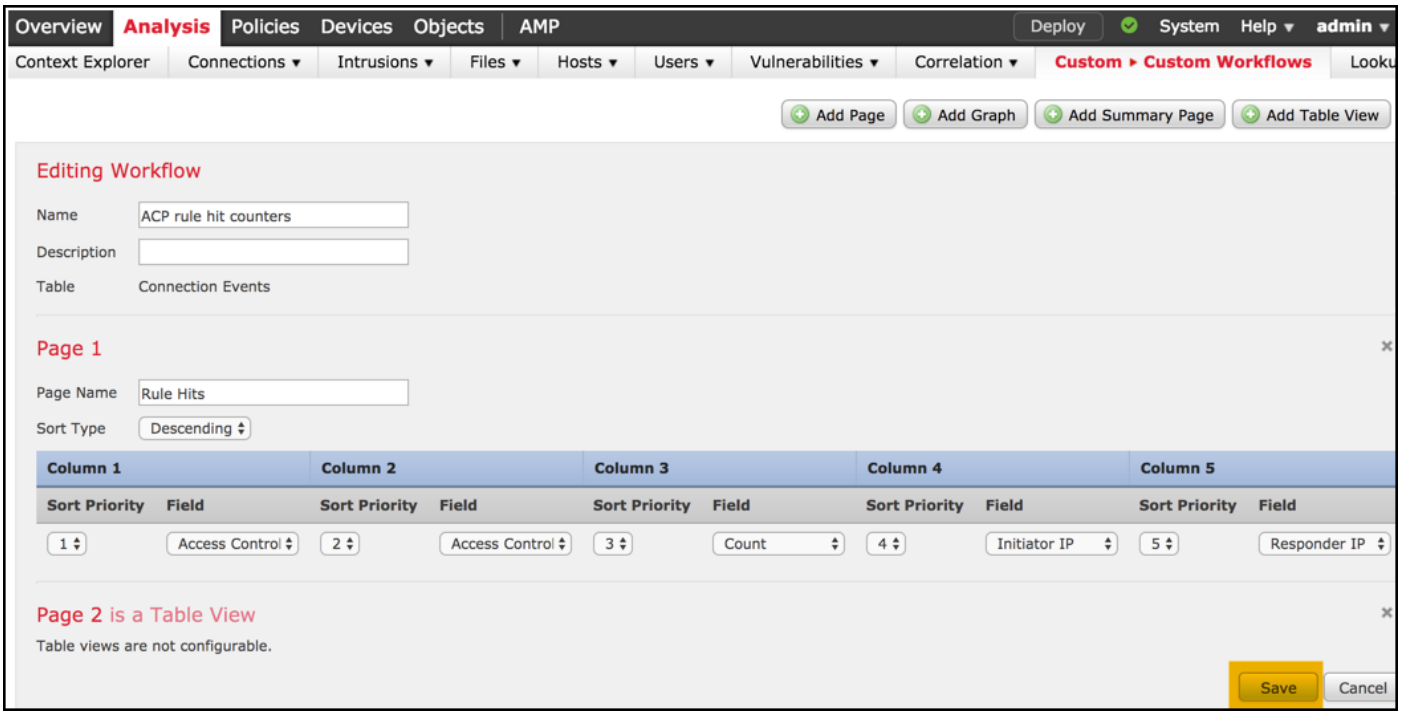



Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View
Editing Workflow
Name
ACP rule hit counters
Description
Table
Connection Events
Page 1
Page Name
Rule Hits
Sort Type
Descending
Column 1
Column 2
Column 3
Column 4
Column 5
Sort Priority
Field
Access Control
Count
Initiator IP
Responder IP
Save
Cancel

步骤 5

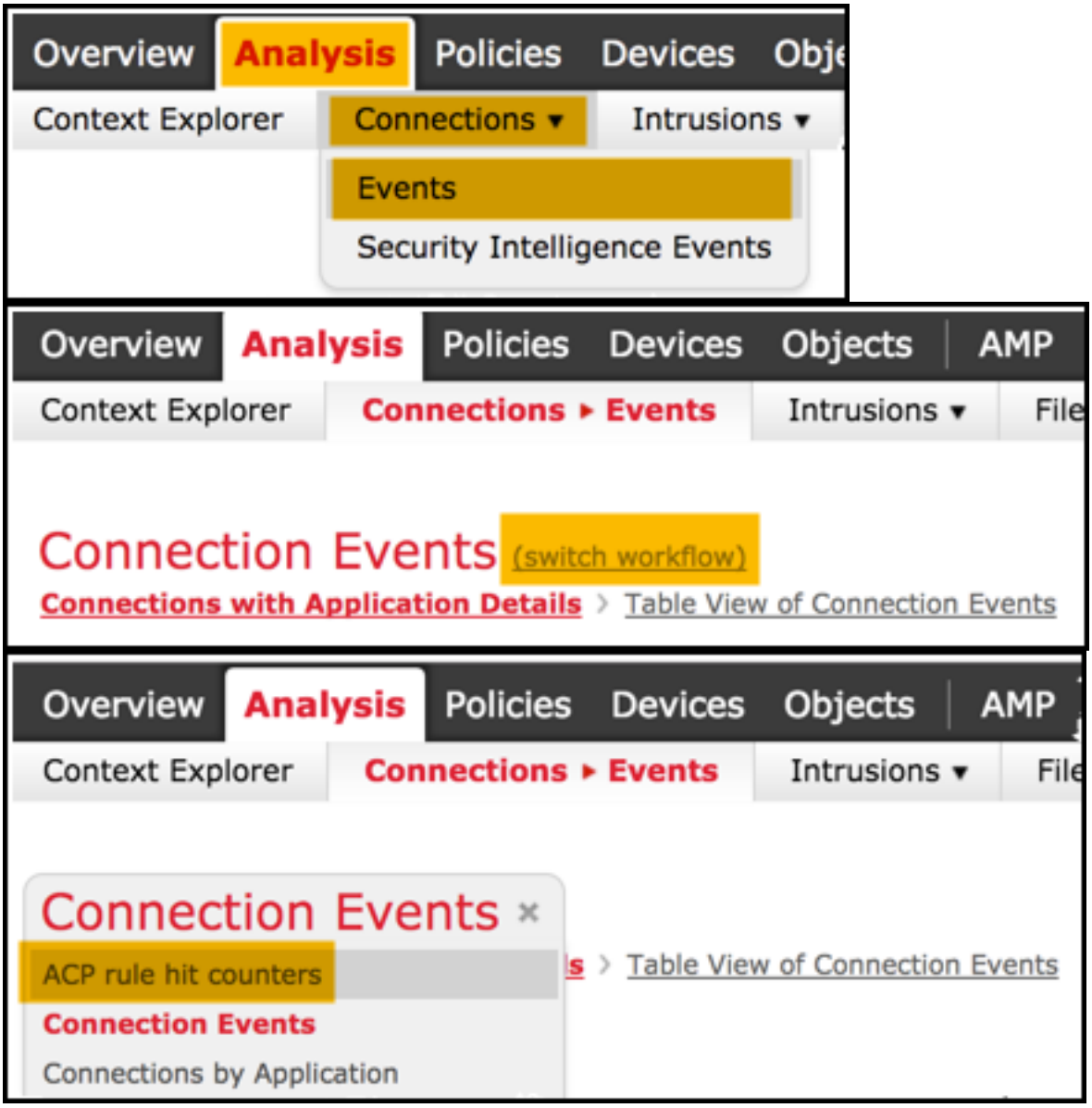

Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View

6

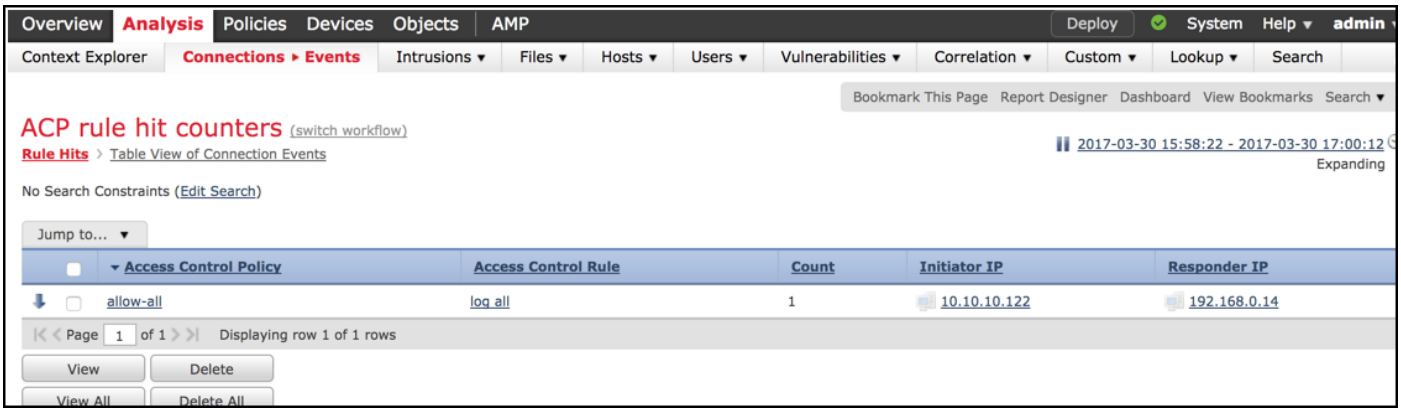

Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View
Editing Workflow
Name
ACP rule hit counters
Description
Table
Connection Events
Page 1
Page Name
Rule Hits
Sort Type
Descending
Column 1
Column 2
Column 3
Column 4
Column 5
Sort Priority
Field
Access Control
Count
Initiator IP
Responder IP
Page 2 is a Table View
Table views are not configurable.
Save
Cancel

7

>



AChitcounters



验证

方式确认访问控制根据规则基本类型的规则命中计数器为所有流量(全局)可以从FTD CLISH (CLI SHELL)达到**显示访问控制设置**命令，如下被展示：

```
> 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

用防火墙引擎**调试**命令您能确认通信流是否被评估适当的访问控制规则：

```
> 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
```

ACPLine(CLI)GUICLIIP FMC GUI

相关信息

- 自定义工作流
- 开始与访问控制策略
- 技术支持和文档 - Cisco Systems