Firepower 管理中心：显示访问控制策略点击计数器

Contents

Introduction

Prerequisites

Firepower（FMC）Firepower（FMC）(ACP)

Requirements

There are no specific requirements for this document.

Components Used

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

Note:本文档中所述信息不适用于 Firepower 设备管理器 (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.

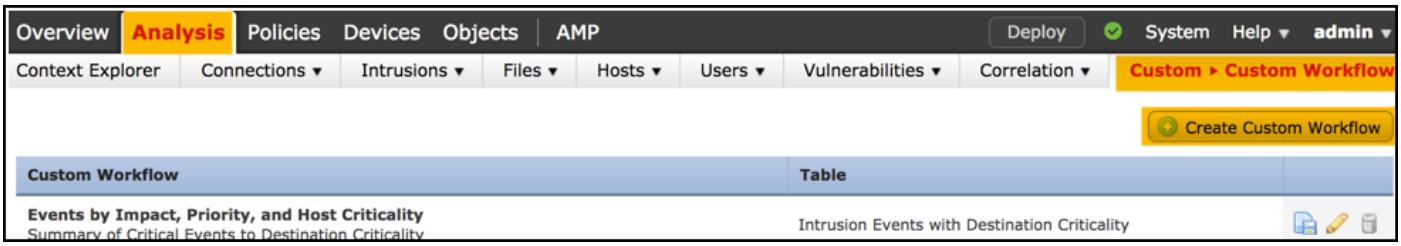
本文档还可与以下硬件和软件版本一起使用：

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

Configure

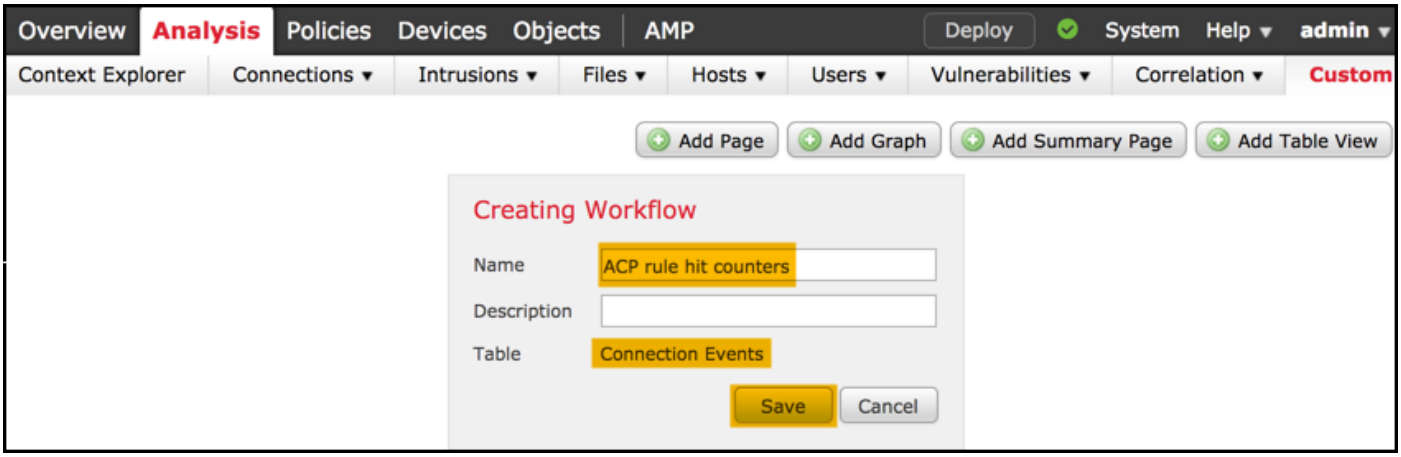
第 1 步

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**：



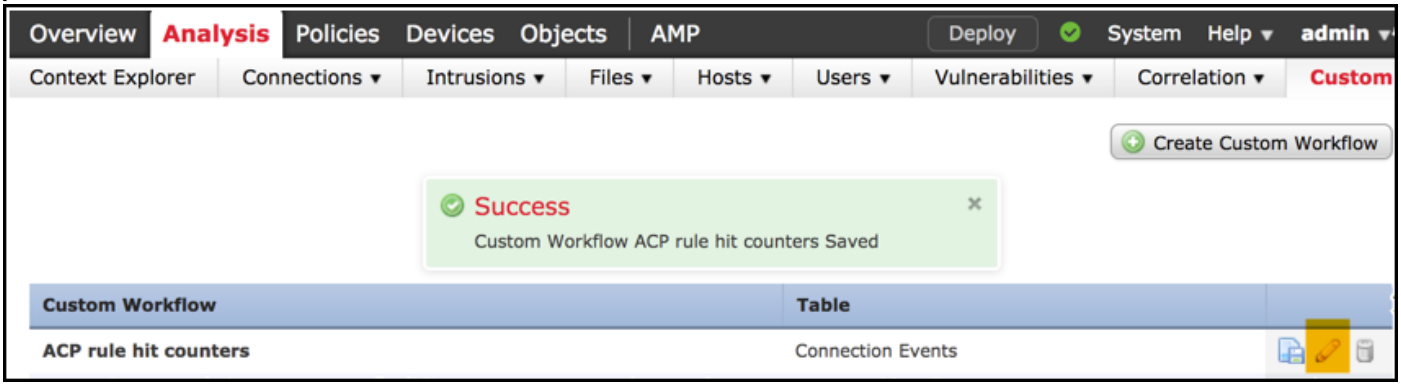
2

ACP



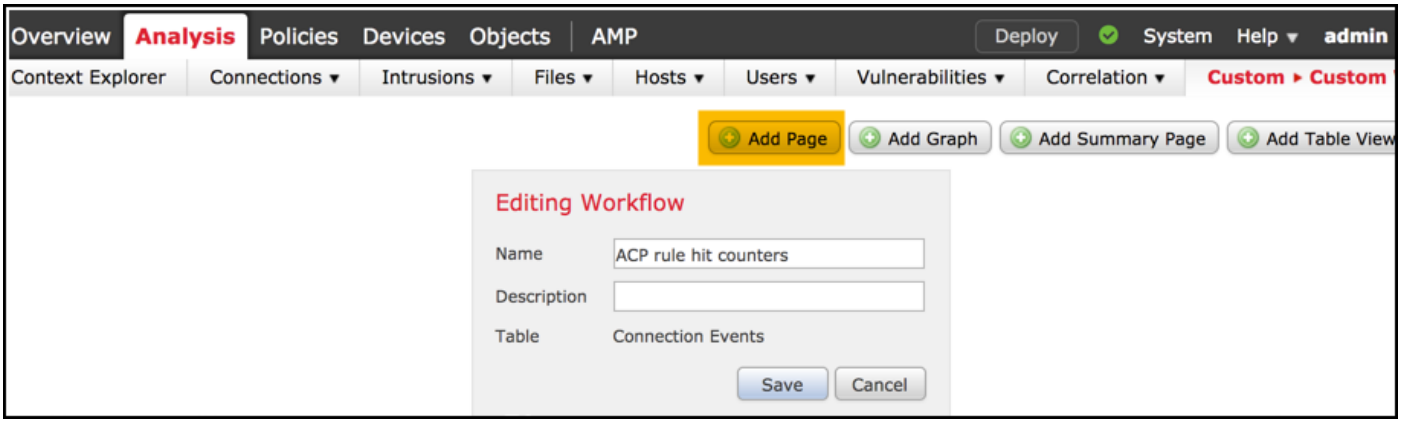
3

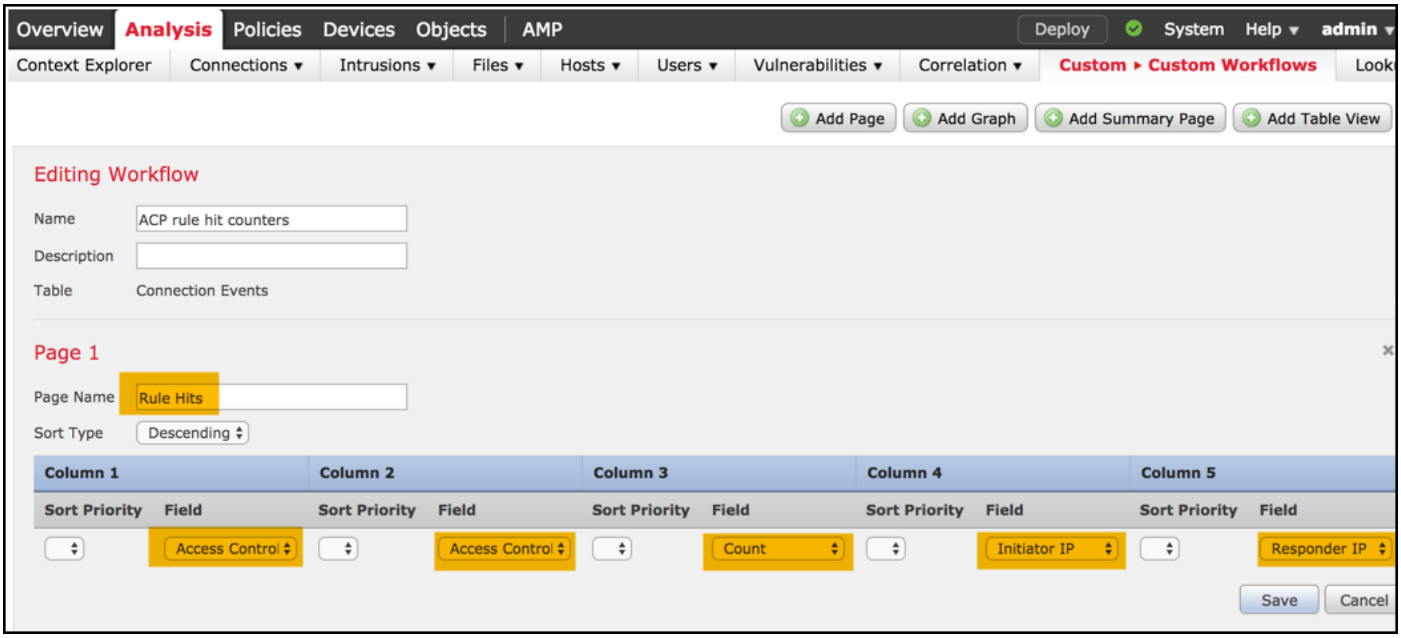
/



4

IP IP

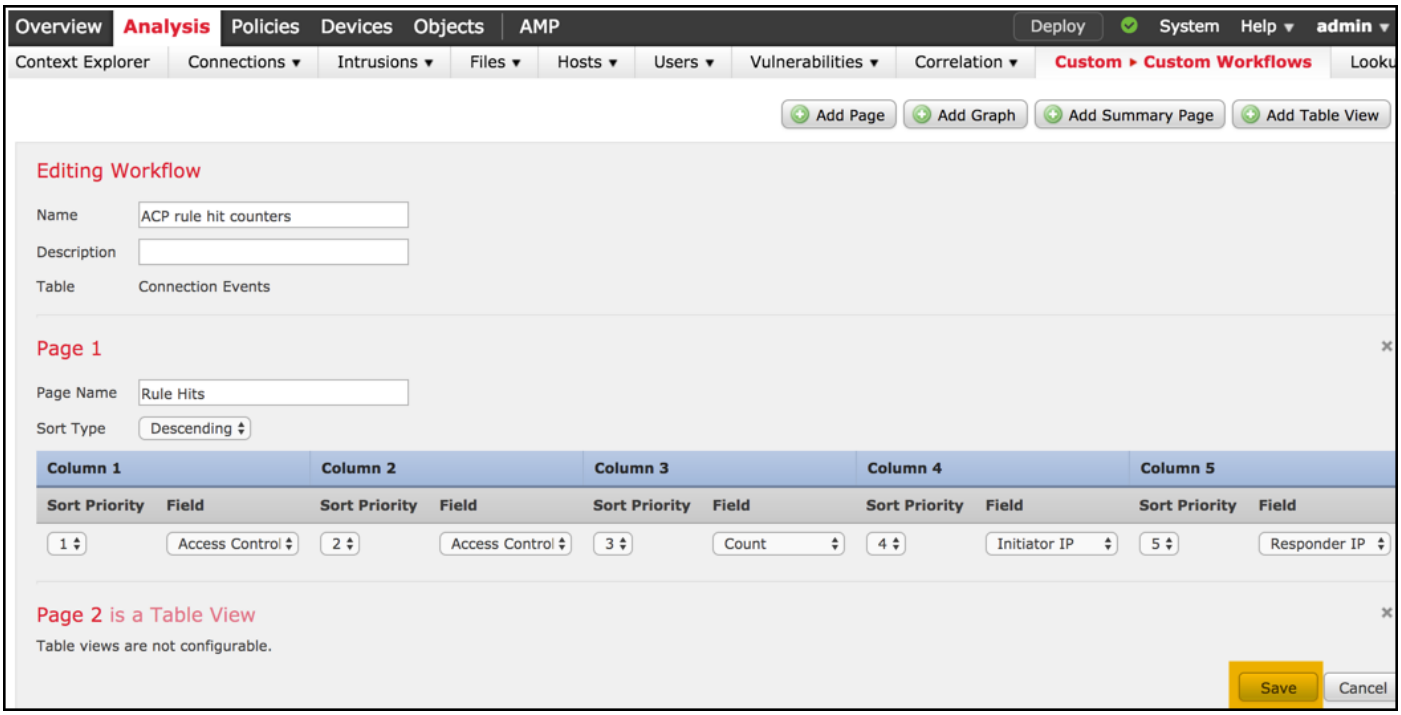



Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View
Editing Workflow
Name
ACP rule hit counters
Description
Table
Connection 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

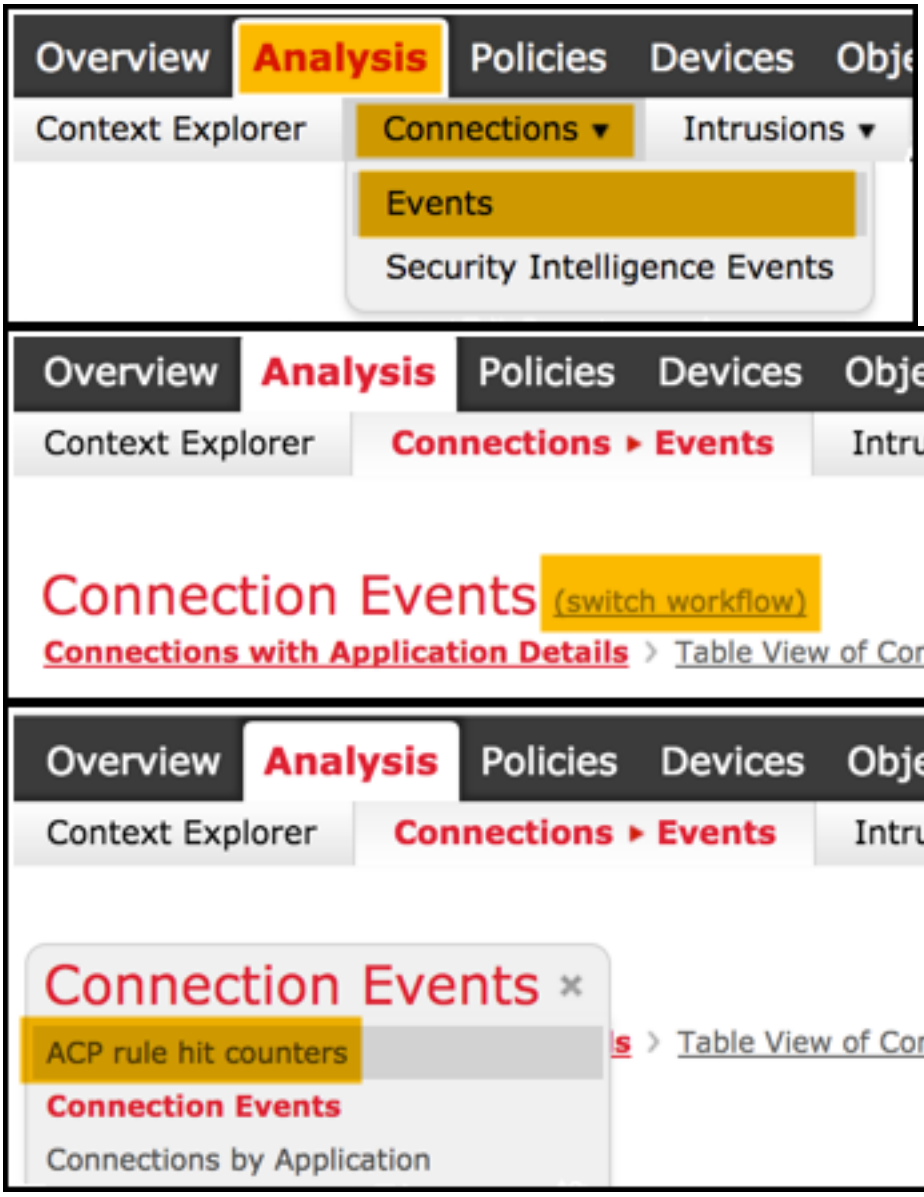

Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View

6

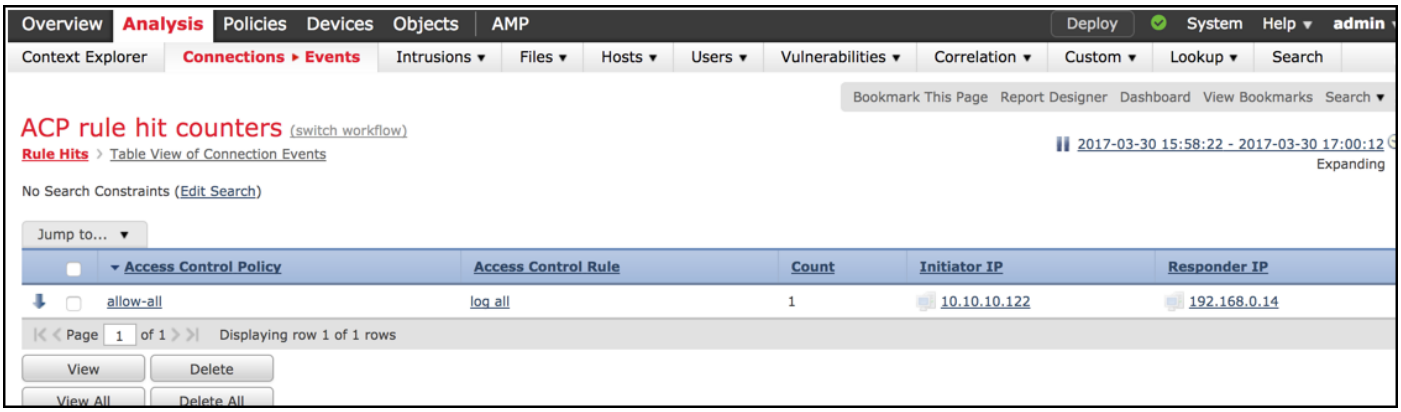

Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View
Editing Workflow
Name
ACP rule hit counters
Description
Table
Connection 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

> **ACP**



ACP AC



Verify

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)
```

Troubleshoot

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
- Technical Support & Documentation - Cisco Systems