Firepower管理中心：顯示訪問控制策略命中計數器

目錄

簡介

必要條件

Firepower(FMC)(ACP)(

需求

本文件沒有特定需求。

- Firepower(FMC) — 6.1.0.153
- Firepower(FTD)4150 — 6.1.0.153

附註：本文檔中描述的資訊不適用於Firepower裝置管理器(FDM)。

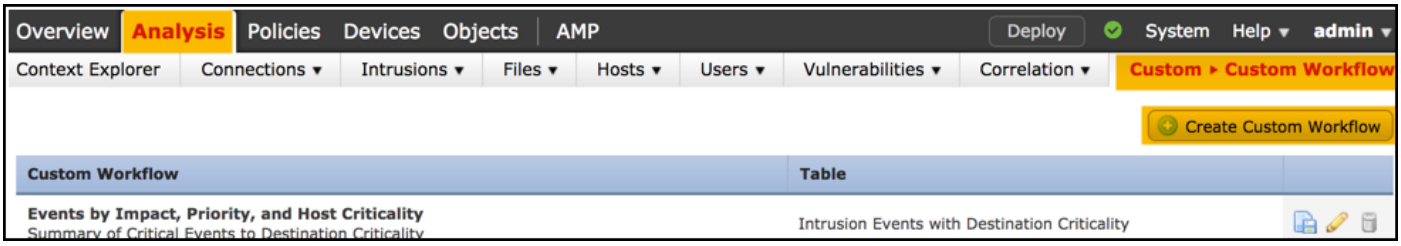
本文件也適用於以下硬體和軟體版本：

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

設定

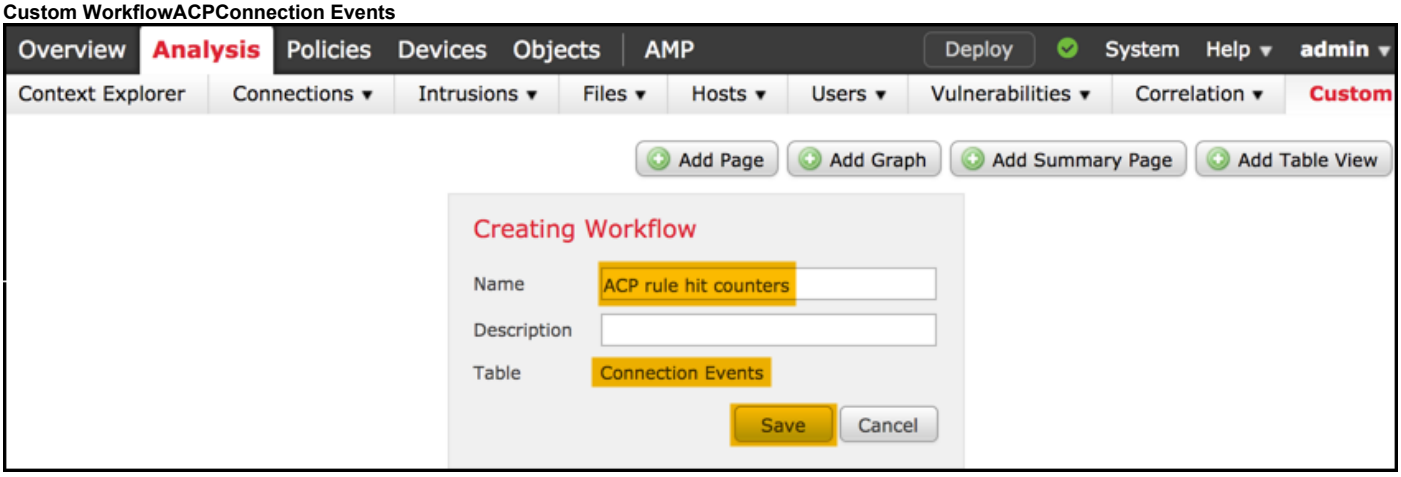
1

要建立自定義工作流程，請導航到**分析>自定義>自定義工作流程>建立自定義工作流程**：



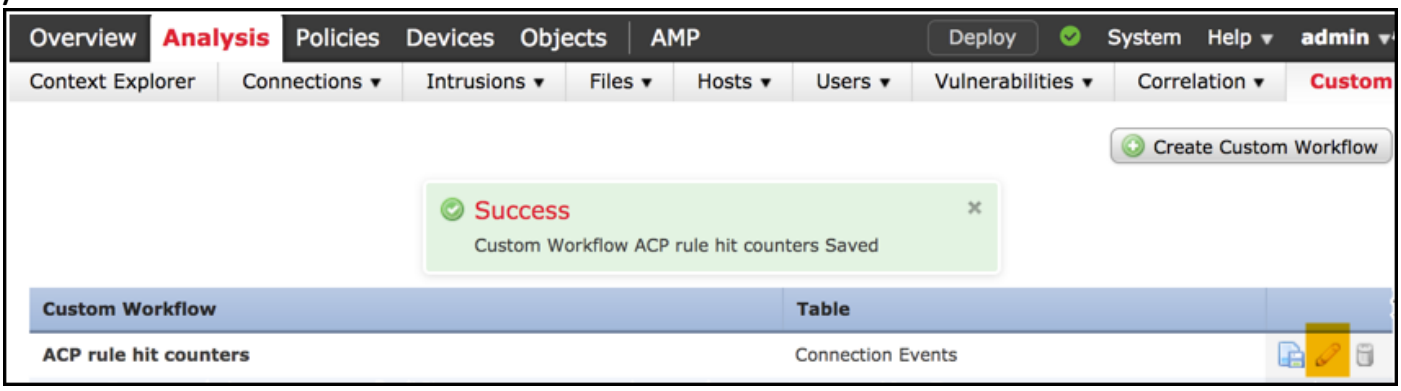
2

Custom WorkflowACPConnection Events



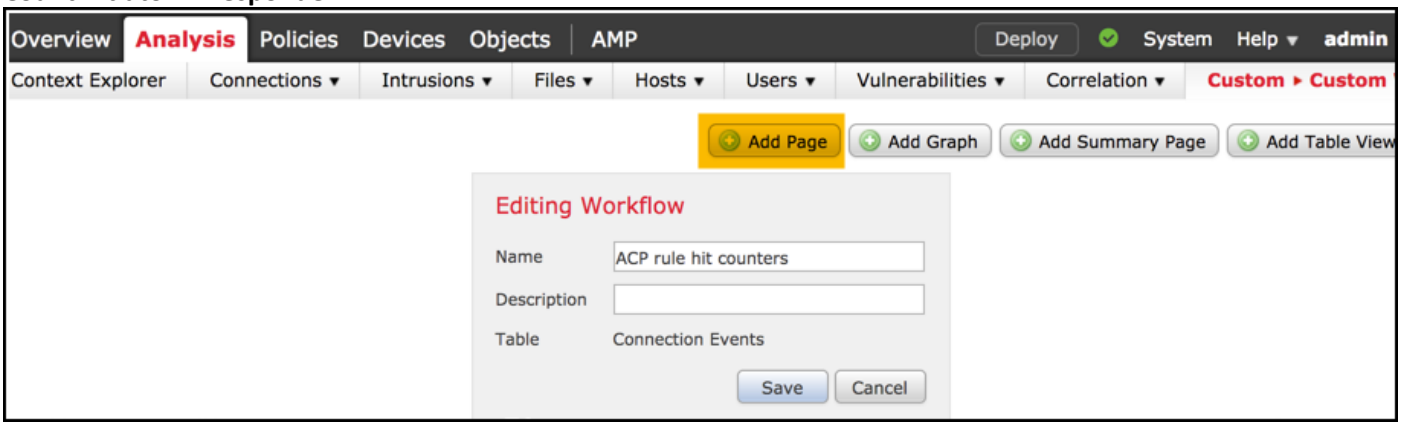
3

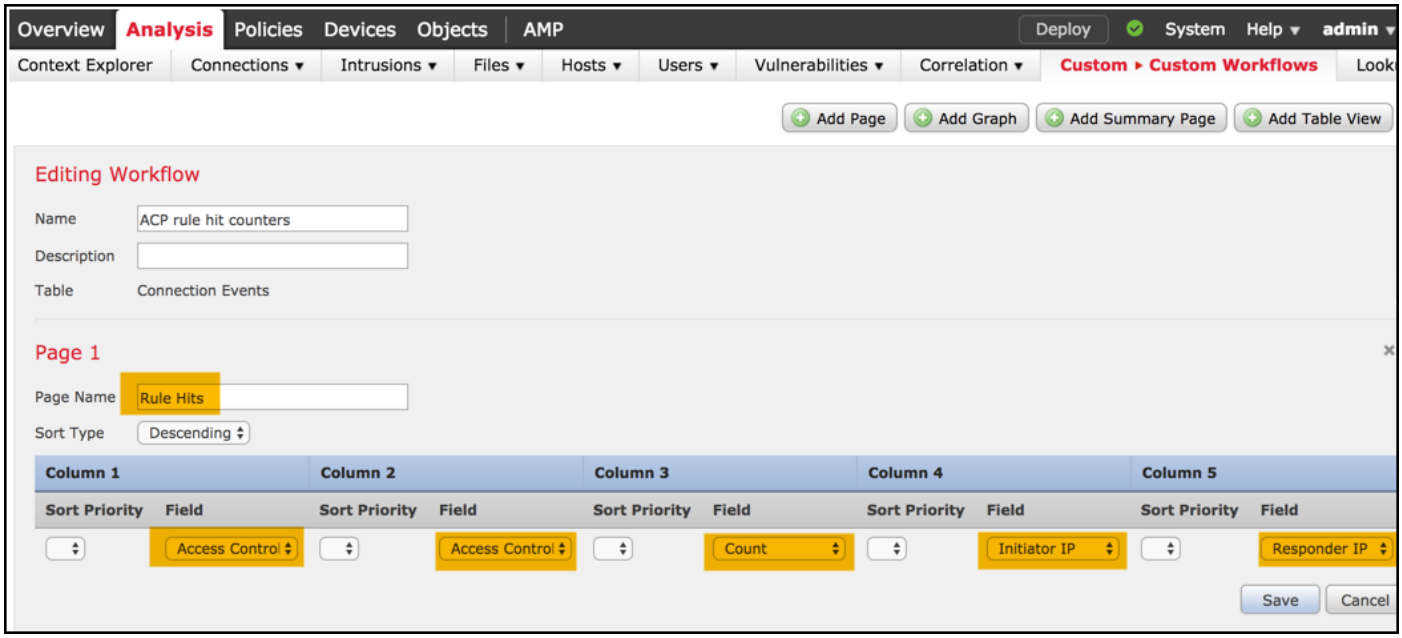
/



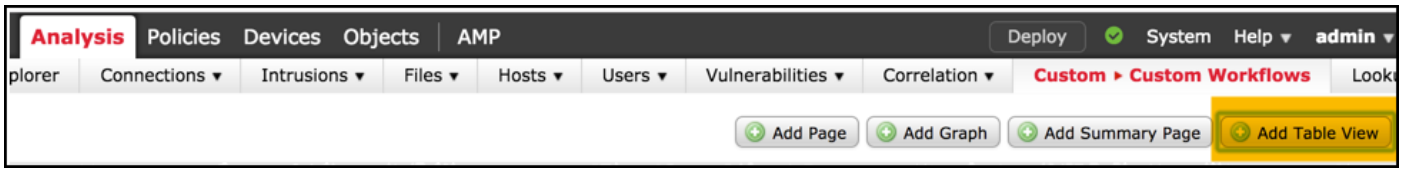
4

CountInitiator IPResponder IP



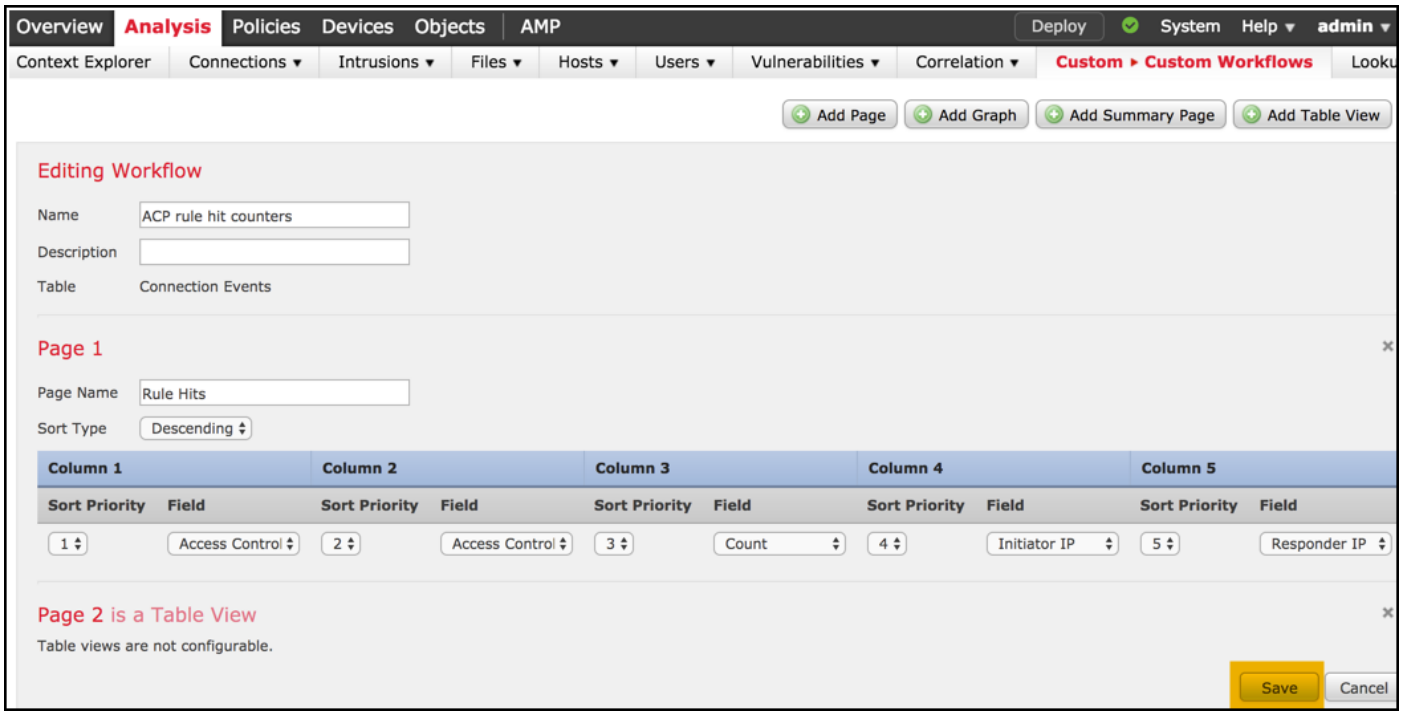


步驟5



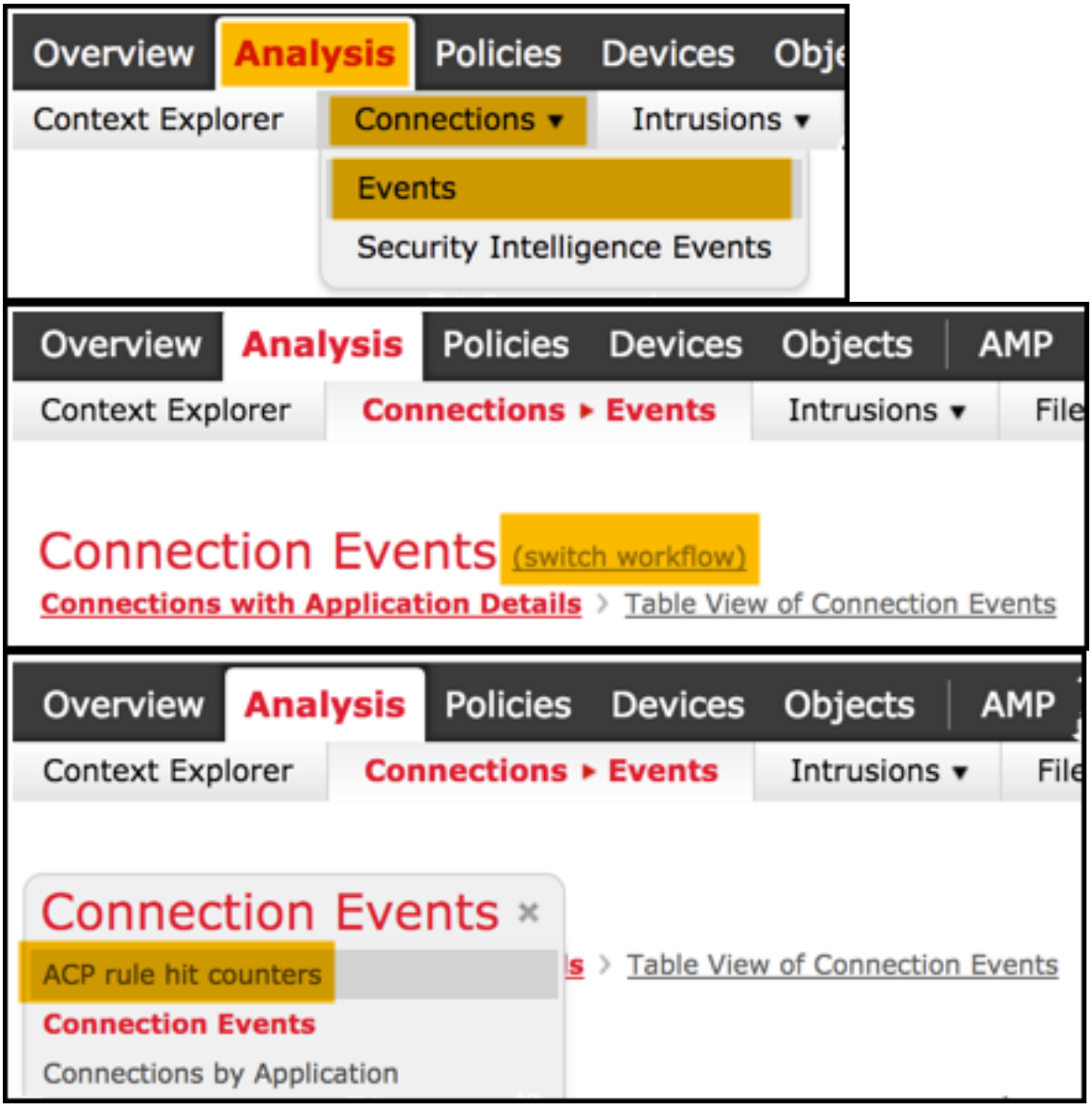
6

Table ViewSave

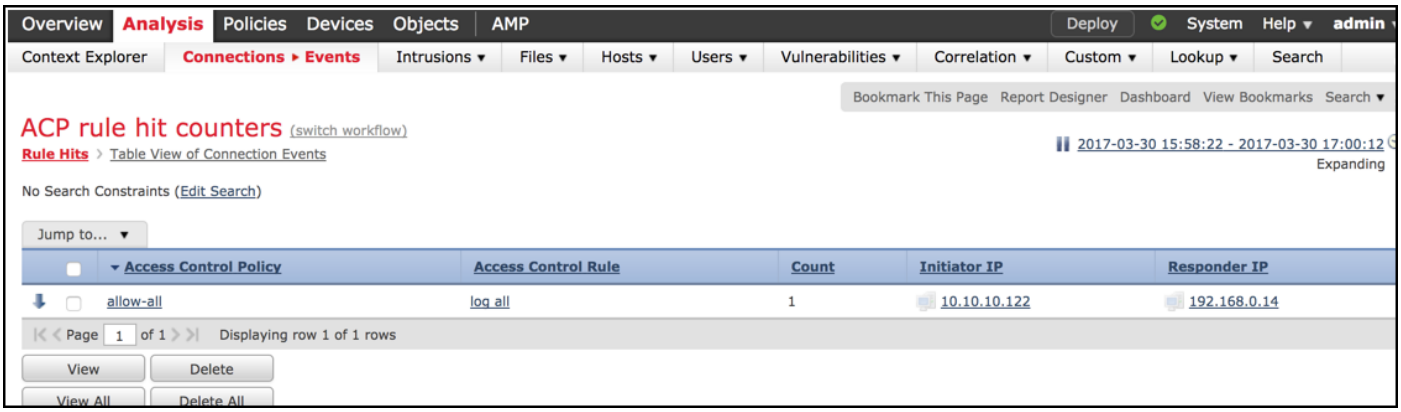


7

Analysis > Connection Eventsswitch workflowACP



ACPAC



驗證

通過FTD CLISH(CLI SHELL)**show access-control-config**命令，可以獲得根據規則（全域性）確認所有流量的訪問控制規則命中計數器的方法，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)
```

疑難排解

使用**firewall-engine-debug**命令，可以確認是否根據正確的訪問控制規則評估流量：

```
> 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
```

logACP(CLI)GUICLIIPFMC GUI

相關資訊

- 自定義工作流程
- 訪問控制策略入門
- 技術支援與文件 - Cisco Systems