Firepower Management Center：アクセス コントロール ポリシー ヒット カウンタの表示

内容

概要

前提条件

ACP Firepower Management CenterFMC

要件

このドキュメントに特有の要件はありません。

- Firepower Management CenterFMC- 6.1.0.1 53
- Firepower Threat DefenseFTD4150 - 6.1.0.1 53

注：このドキュメントで説明する情報は、Firepower Device Manager（FDM）には当てはまりません。

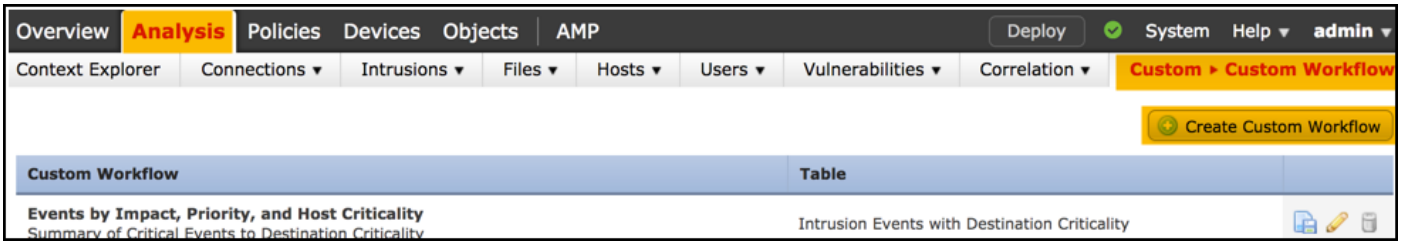
このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Firepower Management CenterFMC- 6.0.x
- Firepower - 6.1.x

設定

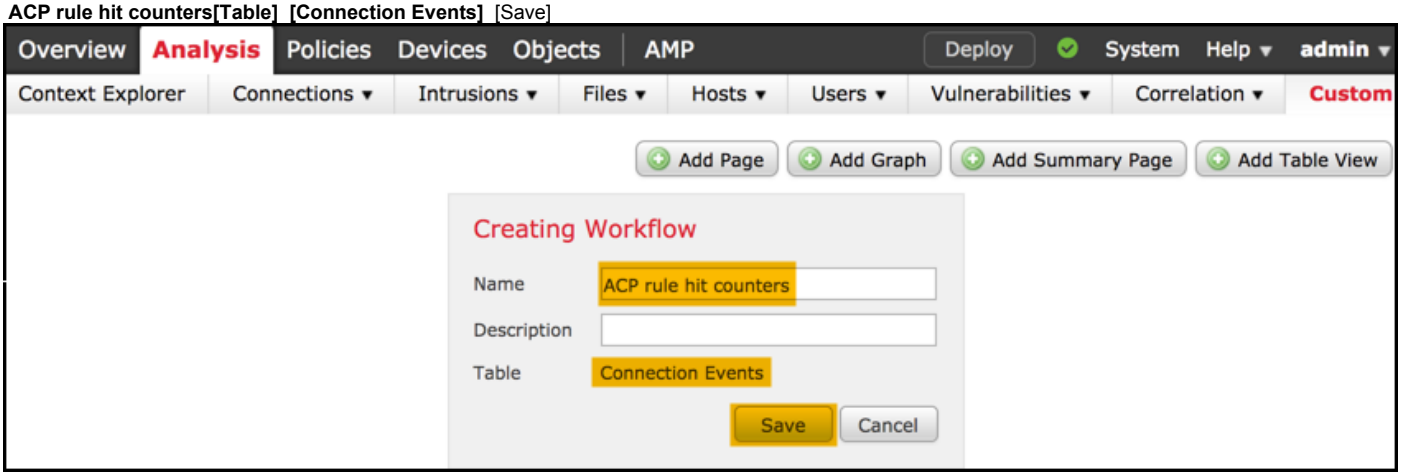
1

カスタム ワークフローを作成するには、[分析（Analysis）] > [カスタム（Custom）] > [カスタム ワークフロー（Custom Workflows）] > [カスタムワークフローの作成（Create Custom Workflow）] の順に移動します。



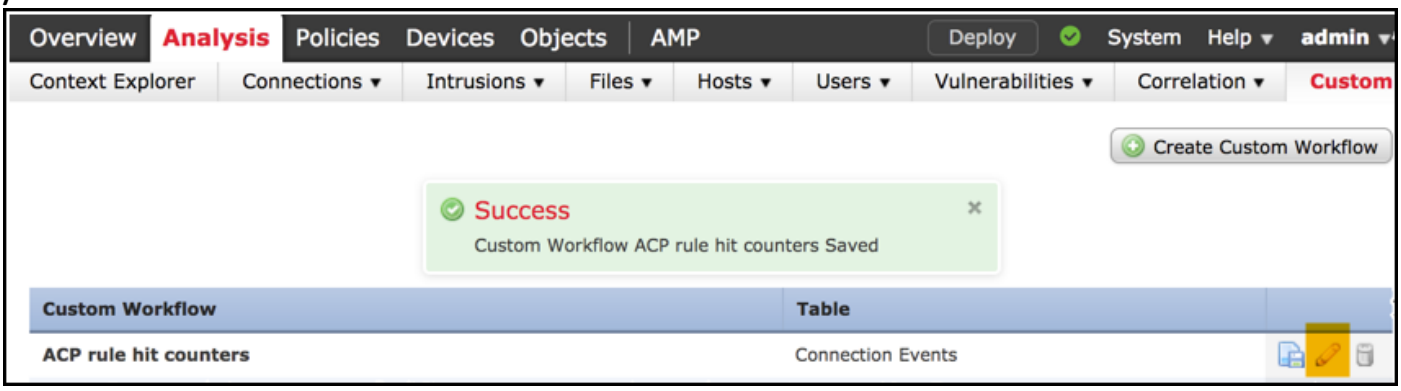
2

ACP rule hit counters[Table] [Connection Events] [Save]



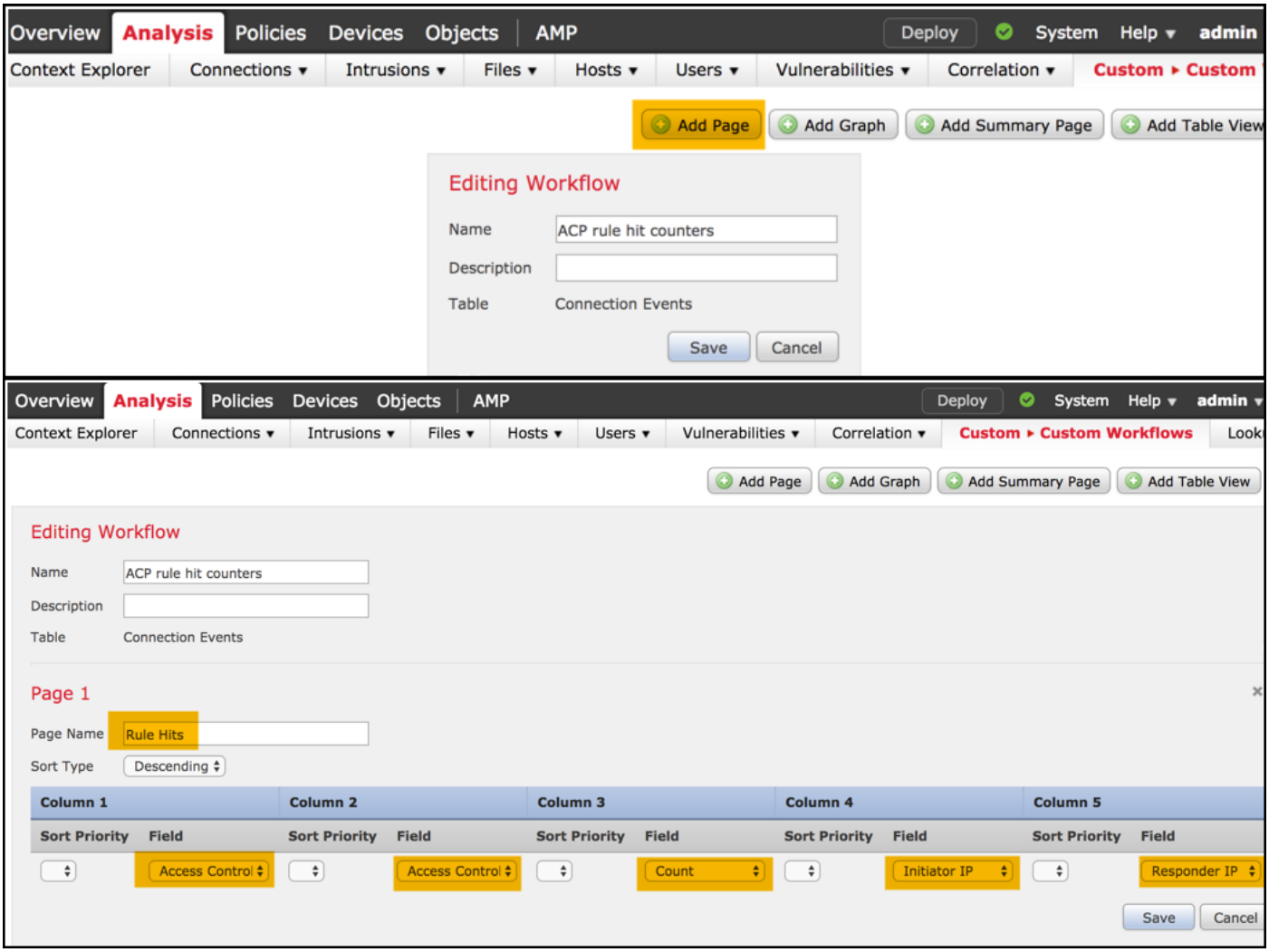
3

/



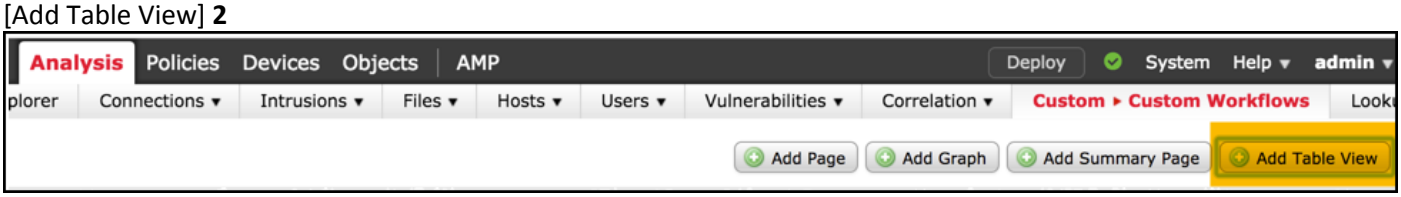
4

[Add Page] **[Access Control Policy] [Access Control Rule]** [Count][IPInitiator IP][IPResponder IP]



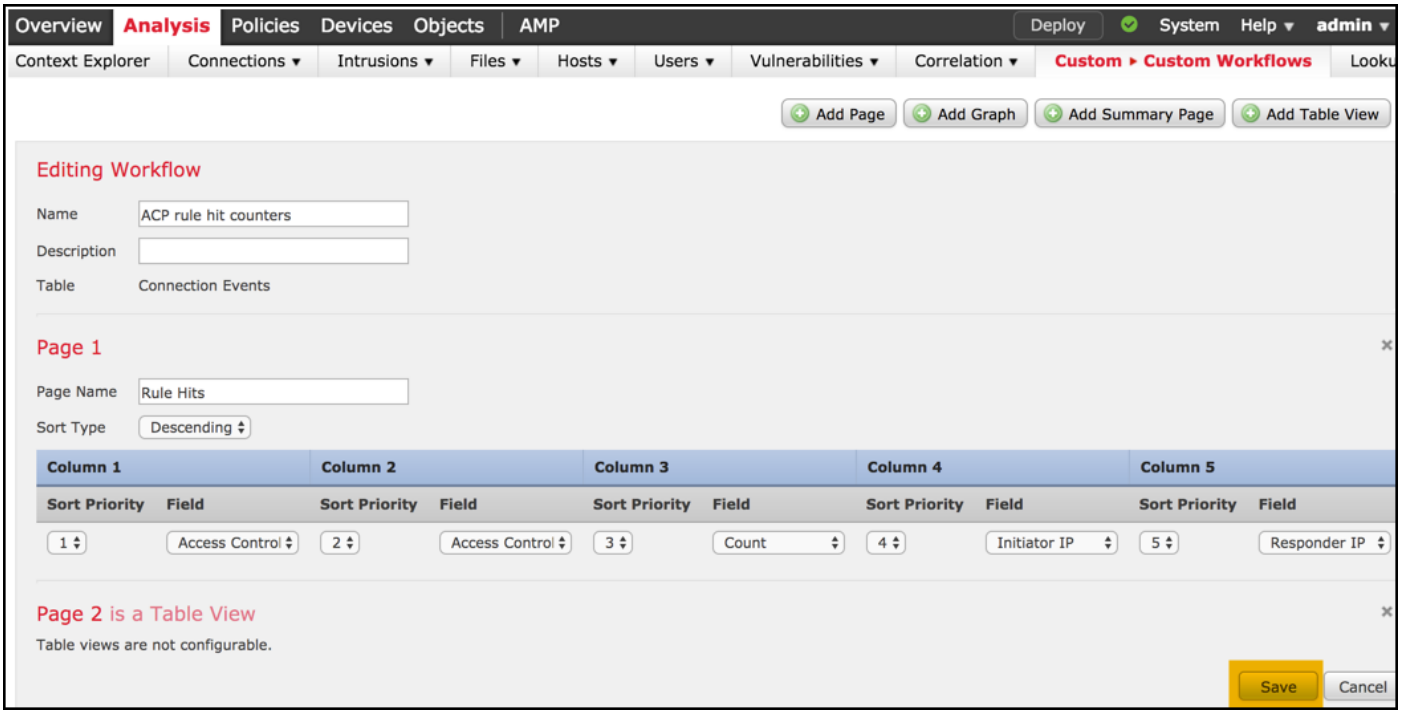
手順 5

[Add Table View] **2**



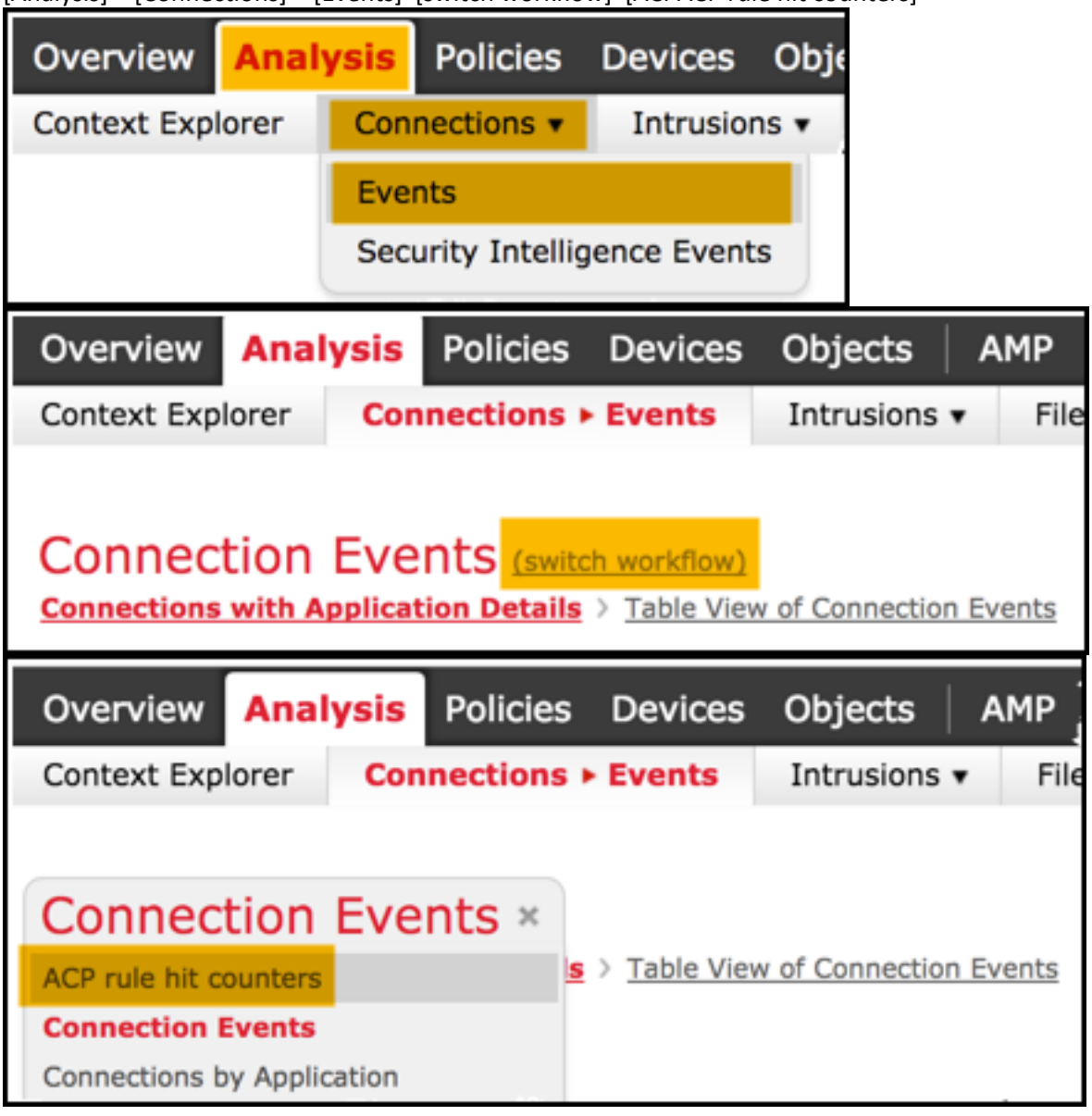
6

[Table View] **[Save]**

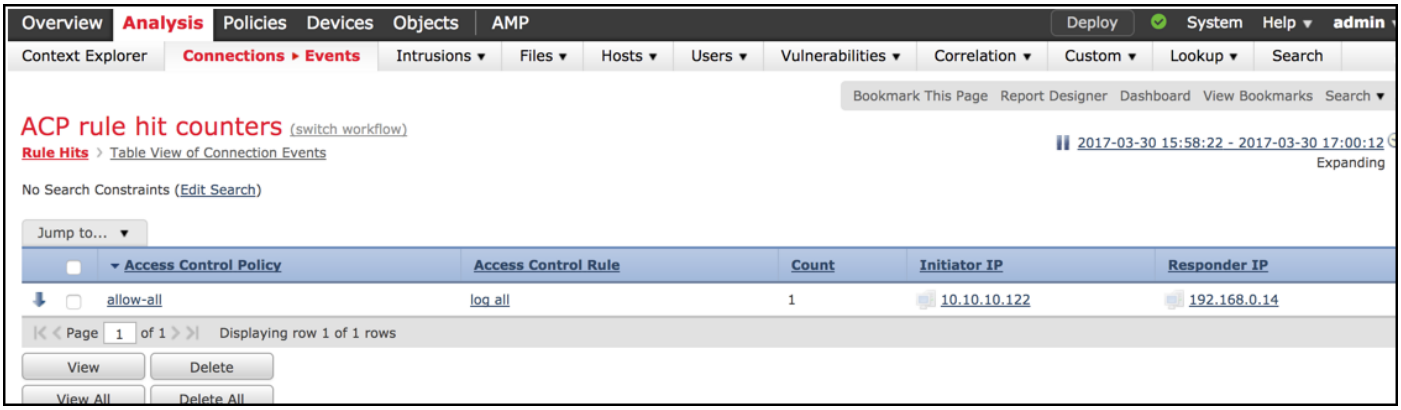


7

[Analysis] > [Connections] > [Events] [switch workflow] [ACPACP rule hit counters]



ACP AC



確認

全トラフィックのアクセス コントロール ルール ヒット カウンタをルール ベースで（グローバルに）確認するには、FTD CLISH（CLI SHELL）の **show access-control-config コマンドを使用します。その例を以下に示します。**

```
> 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)
```

トラブルシュート

firewall-engine-debug コマンドを使用すると、トラフィック フローが適切なアクセス コントロール ルールに照らし合わせて評価されているかどうかを確認することができます。

```
> 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

関連情報

- カスタム ワークフロー
- アクセス コントロール ポリシー入門
- テクニカル サポートとドキュメント – Cisco Systems