Centre de gestion FirePower : Afficher la politique du compteur de visiteurs du contrôle d'accès

Contenu

Introduction

Conditions préalables

Ce document décrit les instructions visant à créer des **flux de travail personnalisés sur un centre de gestion Firepower (FMC) qui permet au système d'afficher les compteurs d'accès de la politique de contrôle d'accès (ACP) à l'échelle mondiale et selon des règles.** Cette fonctionnalité est utile pour effectuer un dépannage et déterminer si la circulation de trafic correspond à la règle appropriée. Il est également utile d'obtenir des informations sur l'utilisation générale des règles de contrôle d'accès, par exemple, les règles de contrôle d'accès sans accès pendant une longue période peuvent être un indique que la règle n'est plus nécessaire et qu'elle pourrait être supprimée en toute sécurité du système.

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

- Centre de gestion virtuel Firepower (FMC) – version de logiciel 6.1.0.1 (mouture 53)
- Défense contre les menaces Firepower (FTD) 4150 – version de logiciel 6.1.0.1 (mouture 53)

> **Note**: L'information décrite dans ce document n'est pas applicable au gestionnaire d'appareil Firepower (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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

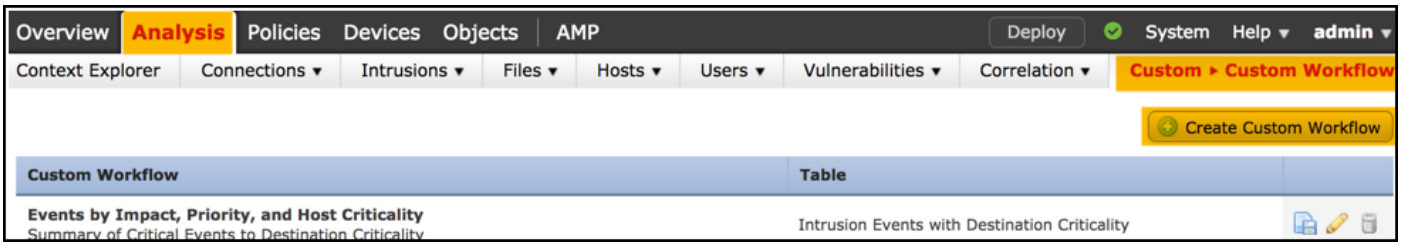
Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Centre de gestion Firepower (FMC) – version de logiciel 6.0.x et plus élevée
- Appareils gérés par Firepower – version de logiciel 6.1.x et plus élevée

Configuration

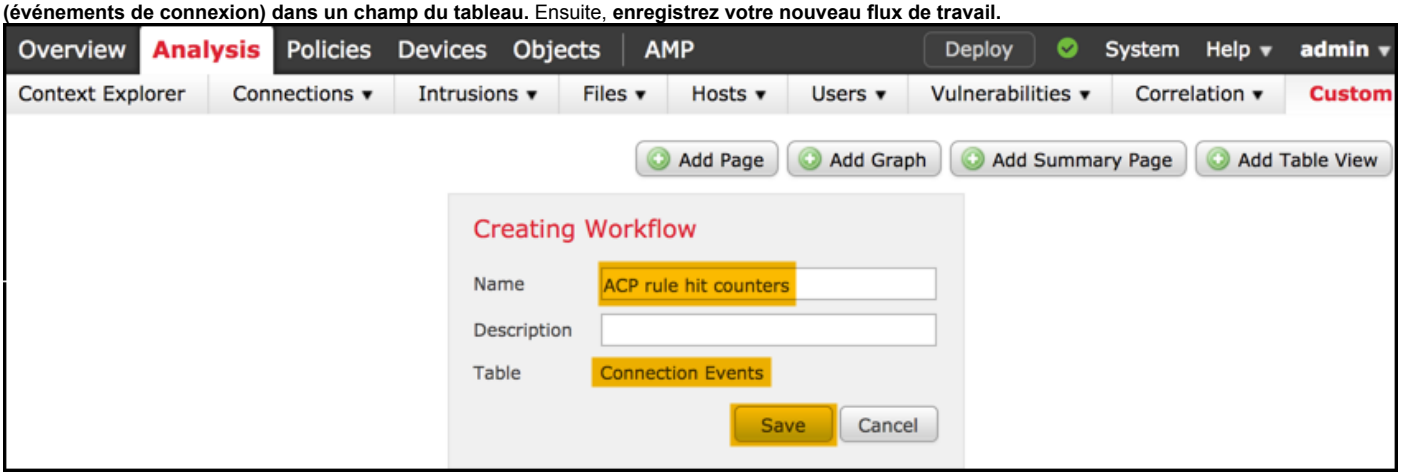
Étape 1

Afin de créer un flux de travail personnalisé, naviguez vers **Analysis > Custom > Custom Workflows > Create Custom Workflow: (analyse > personnalisée > flux de travail personnalisés > créer un flux de travail personnalisé :)**



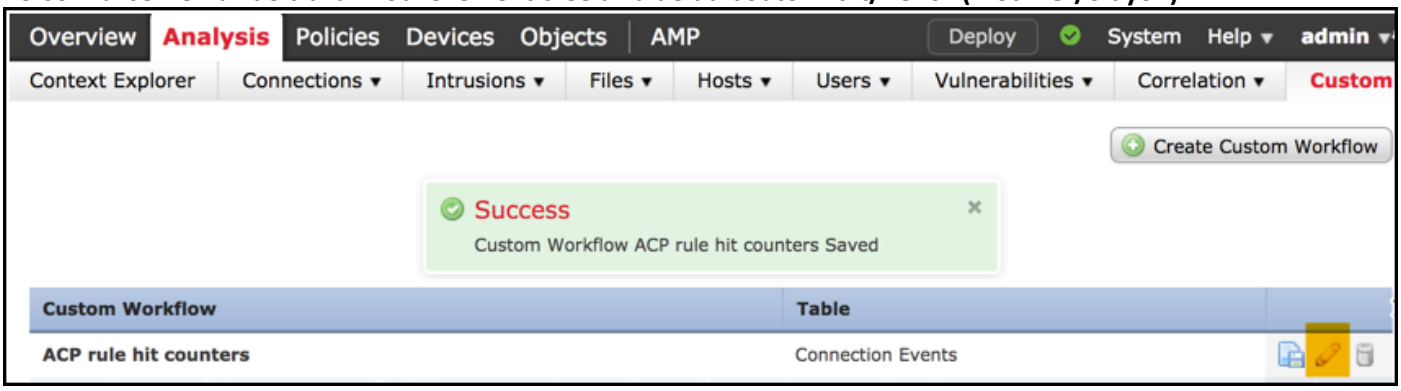
Étape 2

Définissez le nom du **flux de travail personnalisé, par exemple Compteurs de visites de la règle ACP, puis sélectionnez Connection Events (événements de connexion) dans un champ du tableau.** Ensuite, **enregistrez votre nouveau flux de travail.**



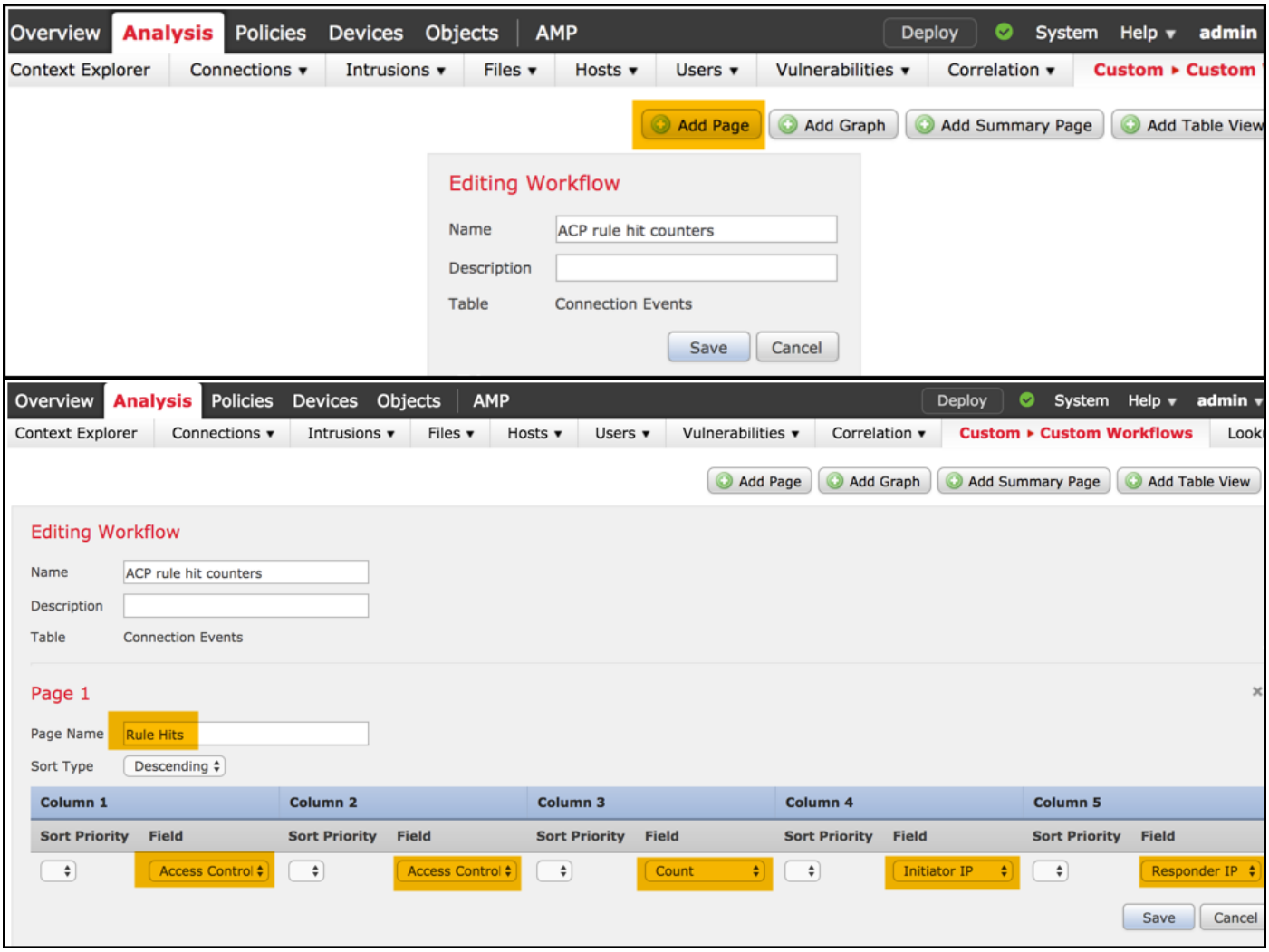
Étape 3

Personnalisez le flux de travail nouvellement créé à l'aide du bouton **Edit/Pencil (modifier/crayon).**



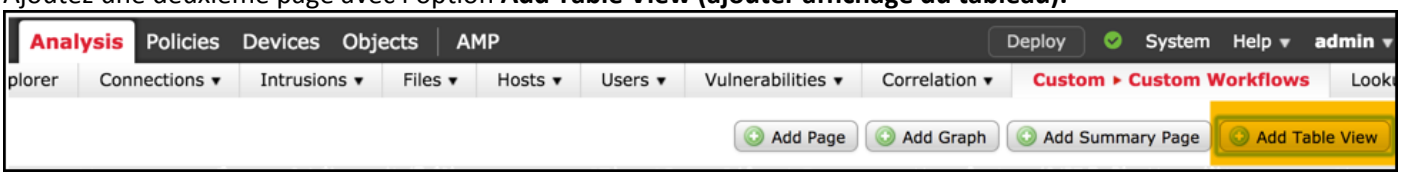
Étape 4

Ajoutez une nouvelle page pour un flux de travail avec l'option **Add Page (ajouter page), définissez son nom et triez les champs de colonne par politique de contrôle d'accès**, **règle de contrôle d'accès et par les champs Count** (compteur), **Initiator IP (IP initiateur) et Responder IP (IP répondant).**



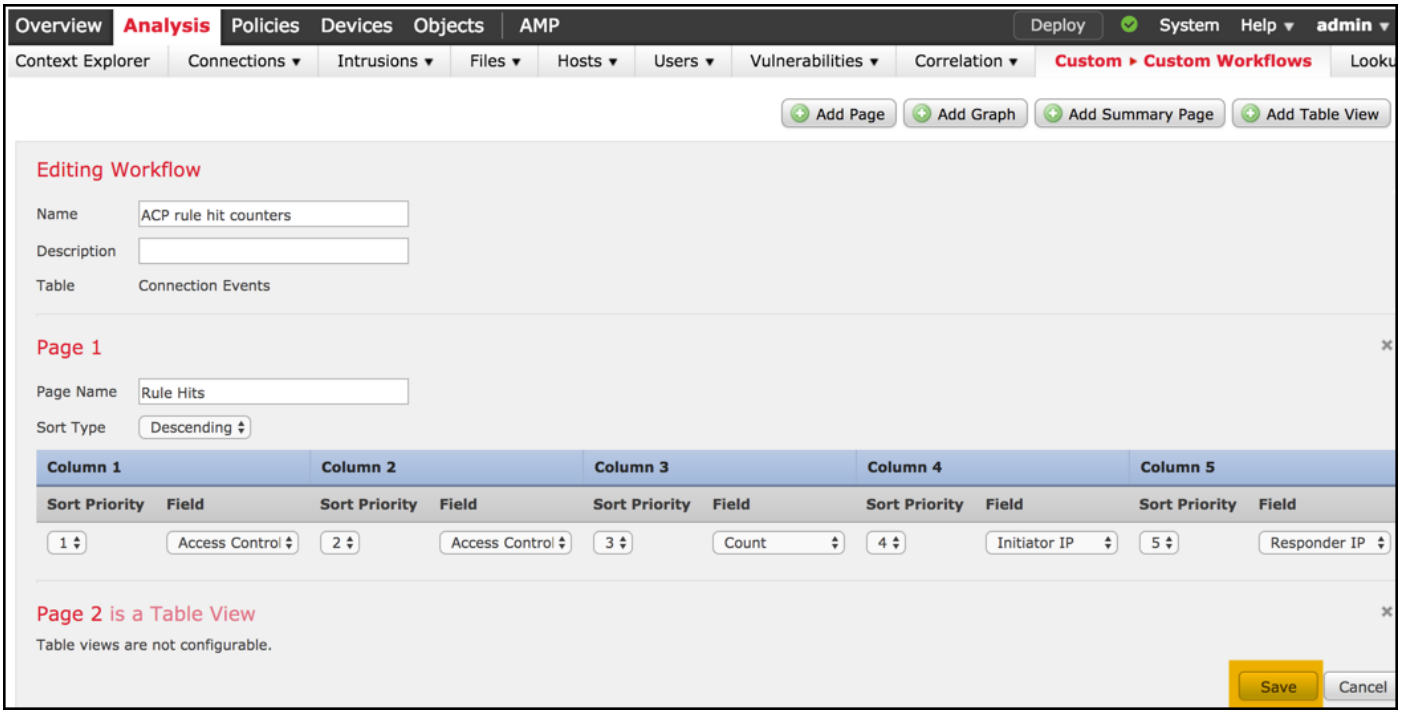
Étape 5

Ajoutez une deuxième page avec l'option **Add Table View (ajouter affichage du tableau).**



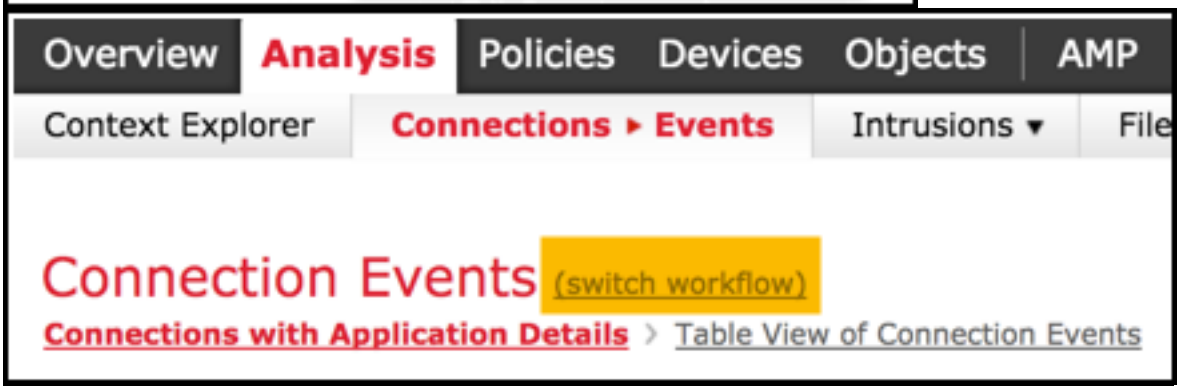
Étape 6

L'**affichage du tableau n'est pas configurable, par conséquent, continuez tout simplement et enregistrez votre flux de travail.**

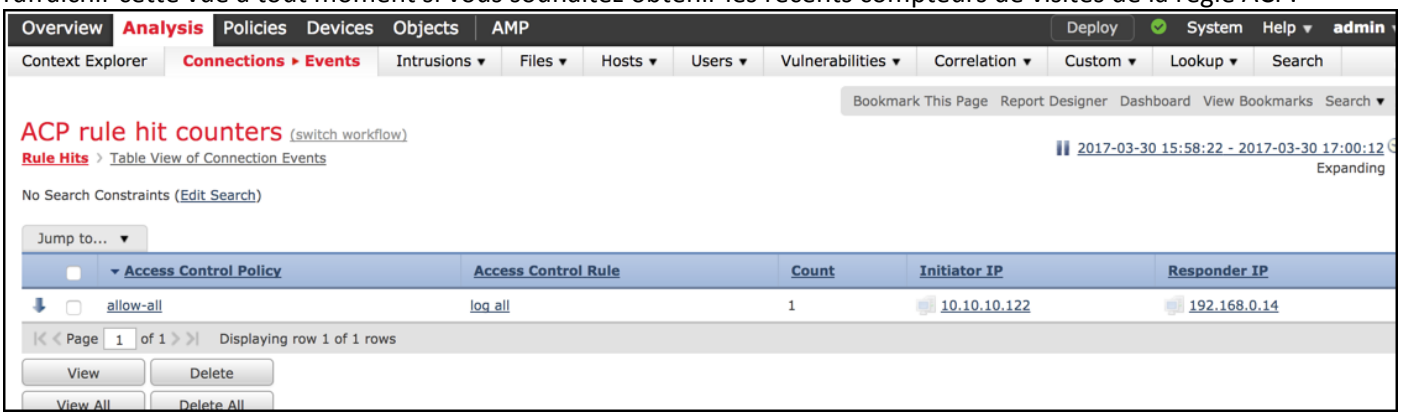


Étape 7

Naviguez vers **Analysis > Connections Events** (analyse > événements de connexions), puis sélectionnez **switch workflow** (changer de flux de travail), puis choisissez le flux de travail nouvellement créé nommé **Compteurs de visites de la règle ACP et attendez jusqu'à ce que la page se recharge.**



Une fois que la page est chargée, les compteurs de visites de la règle par chaque règle ACP sont affichés, il suffit de rafraîchir cette vue à tout moment si vous souhaitez obtenir les récents compteurs de visites de la règle ACP.



Vérification

Il est possible de confirmer que les compteurs de visites de la règle de contrôle d'accès sont fondés sur des règles pour tout le trafic (dans le monde) à partir de la commande FTD CLISH (CLI SHELL) **show access-control-config , qui est illustrée ci-dessous :**

```
> 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)
```

Dépannage

Avec la commande **firewall-engine-debug, vous pouvez confirmer si la circulation de trafic est évaluée par rapport à la règle appropriée de contrôle d'accès :**

```
> 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
```

Lorsque vous comparez les compteurs de visites pour la règle ACP nommée **log all, vous remarquez que la ligne de commande (CLI) et les sorties de l'interface graphique utilisateur (GUI) ne correspondent pas.** La raison en est que les compteurs de visites CLI sont effacés après chaque déploiement de la politique de contrôle d'accès et qu'ils s'appliquent à tout le trafic dans le monde et non à des adresses IP en particulier. D'un autre côté, l'interface graphique utilisateur (GUI) de FMC conserve les compteurs dans la base de données, et peut donc afficher les données historiques basées sur une période sélectionnée.

Informations connexes

- Flux de travail personnalisés
- Démarrage avec les politiques de contrôle d'accès
- Support et documentation techniques - Cisco Systems