FirePOWER Management Center: Anzeigen von Zugriffskontrollrichtlinien auf Zähler

Inhalt

Einführung

Voraussetzungen

In diesem Dokument werden die Anweisungen zum Erstellen **benutzerdefinierter Workflows** auf einem FirePOWER Management Center (FMC) beschrieben, mit dem das System Zugriffskontrollrichtlinien (ACS)-Trefferzähler global und für jede Regel anzeigen kann. Dies ist hilfreich, um die Übereinstimmung des Datenverkehrsflusses mit der richtigen Regel zu beheben. Es ist auch hilfreich, Informationen über die allgemeine Verwendung der Zugriffskontrollregeln zu erhalten, z. B. Zugriffskontrollregeln, die für einen längeren Zeitraum keine Treffer enthalten können. Hinweis, dass die Regel nicht mehr benötigt wird und möglicherweise sicher aus dem System entfernt werden kann.

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

- Virtual FirePOWER Management Center (FMC) - Softwareversion 6.1.0.1 (Build 53)
- Firepower Threat Defense (FTD) 4150 - Softwareversion 6.1.0.1 (Build 53)

> **Hinweis**: Die in diesem Dokument beschriebenen Informationen gelten nicht für den FirePOWER Device Manager (FDM).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

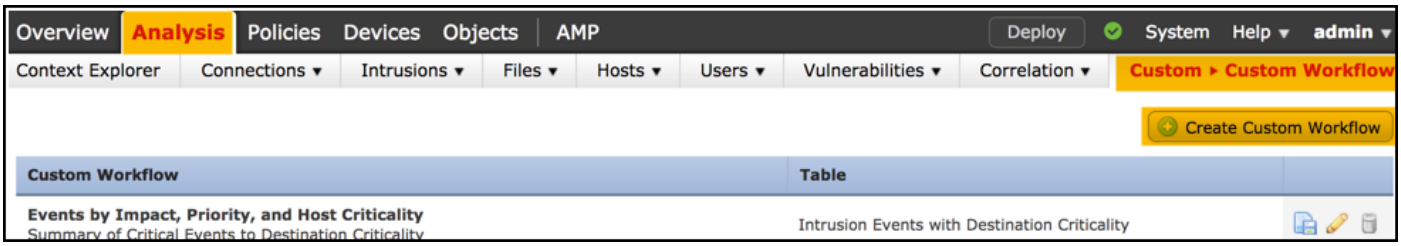
Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- FirePOWER Management Center (FMC) - Softwareversion 6.0.x und höher
- FirePOWER Managed Appliances - Software 6.1.x und höher

Konfigurieren

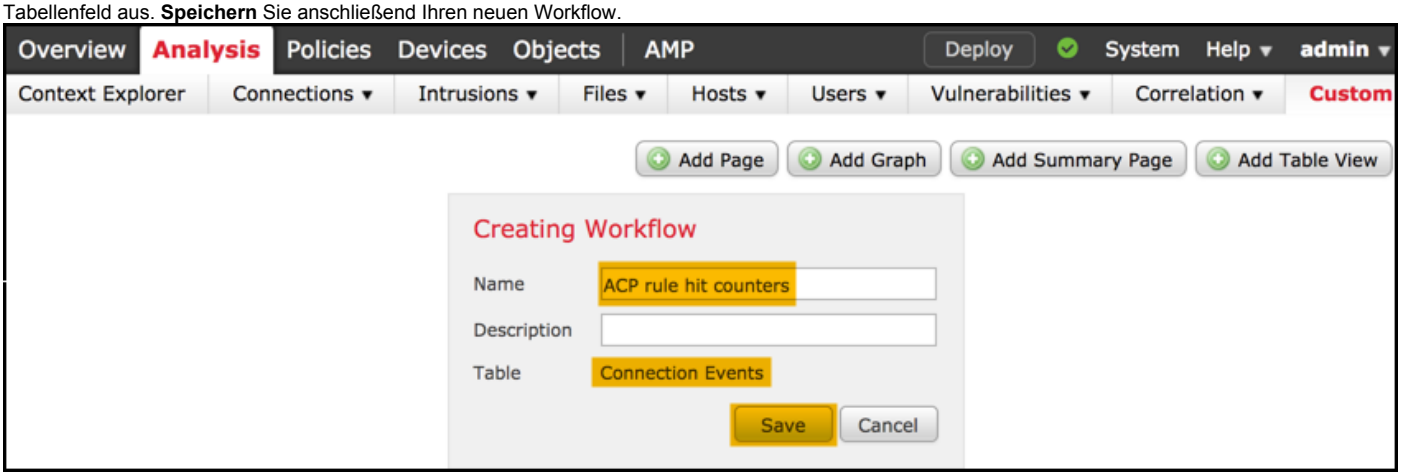
Schritt 1

Um einen benutzerdefinierten Workflow zu erstellen, navigieren Sie zu **Analysis > Custom Workflows > Create Custom Workflow:**



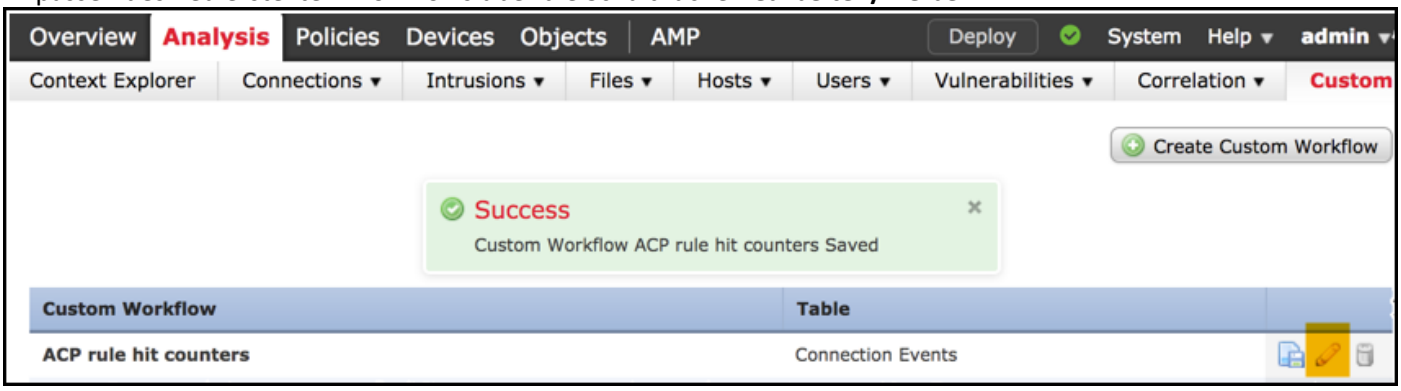
Schritt 2

Definieren Sie den Namen des **benutzerdefinierten Workflows**, z. B. **trifft die ACP-Regel Zähler,** und wählen Sie **Connection Events** in einem Tabellenfeld aus. **Speichern** Sie anschließend Ihren neuen Workflow.



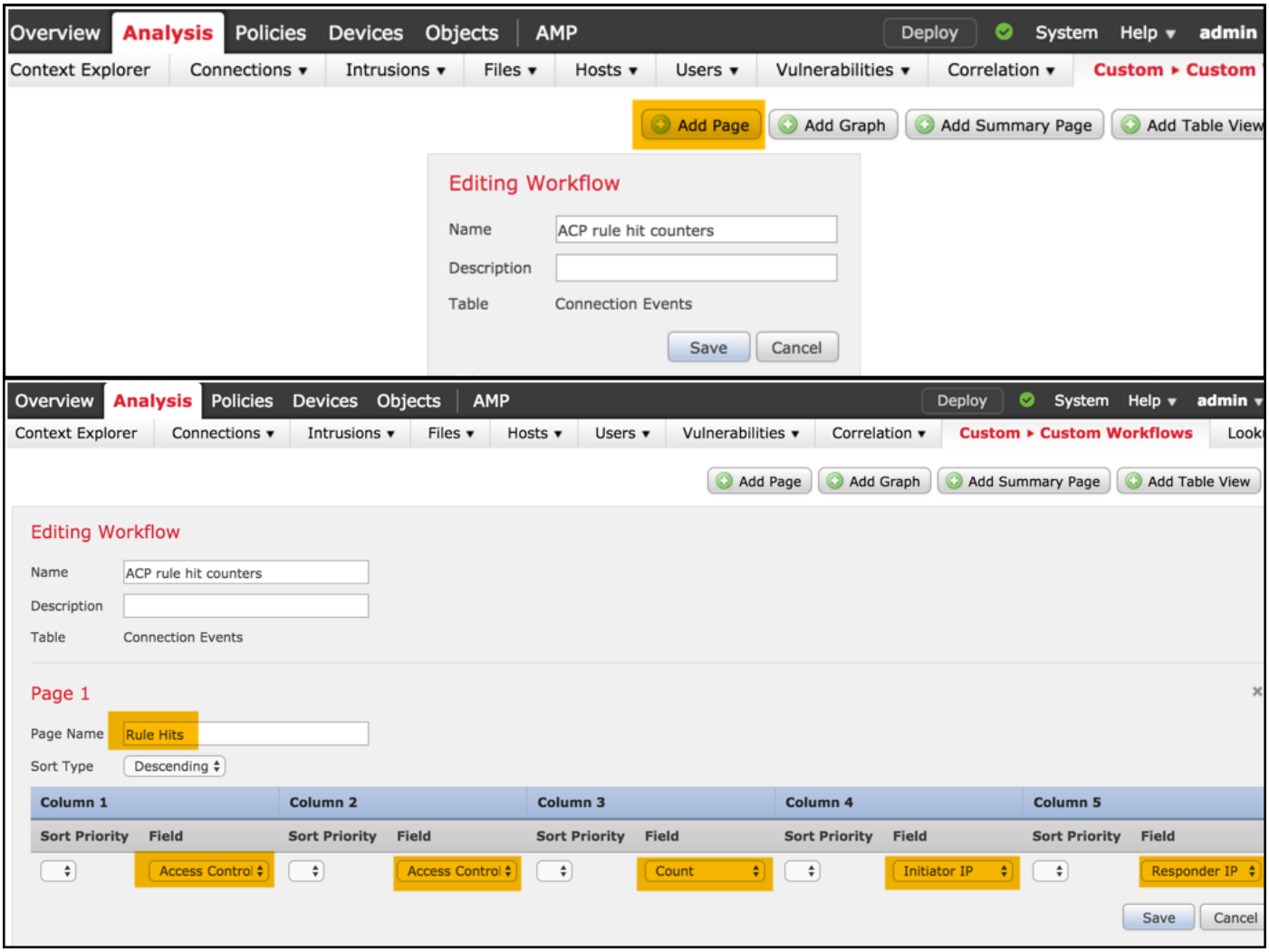
Schritt 3

Anpassen des neu erstellten Workflows über die Schaltfläche **Bearbeiten/Bleiben**.



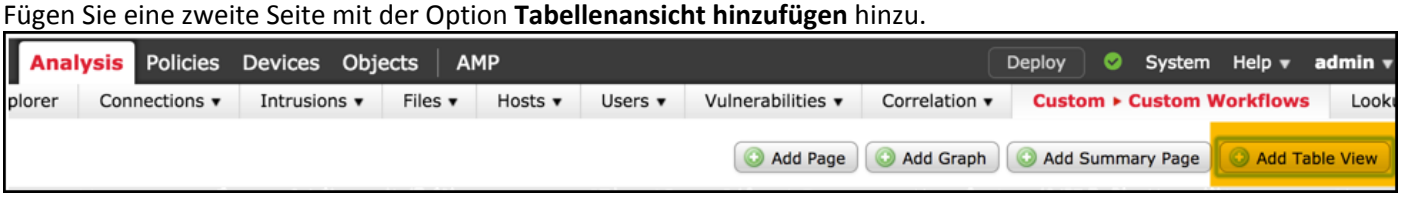
Schritt 4

Fügen Sie eine neue Seite für einen Workflow mit der Option **Seite hinzufügen** hinzu, definieren Sie den Namen und sortieren Sie die Spaltenfelder nach **Zugriffskontrollrichtlinie**, **Zugriffskontrollregel** und **Zähler**, **Initiator-IP- und Responder-IP-Feldern.**



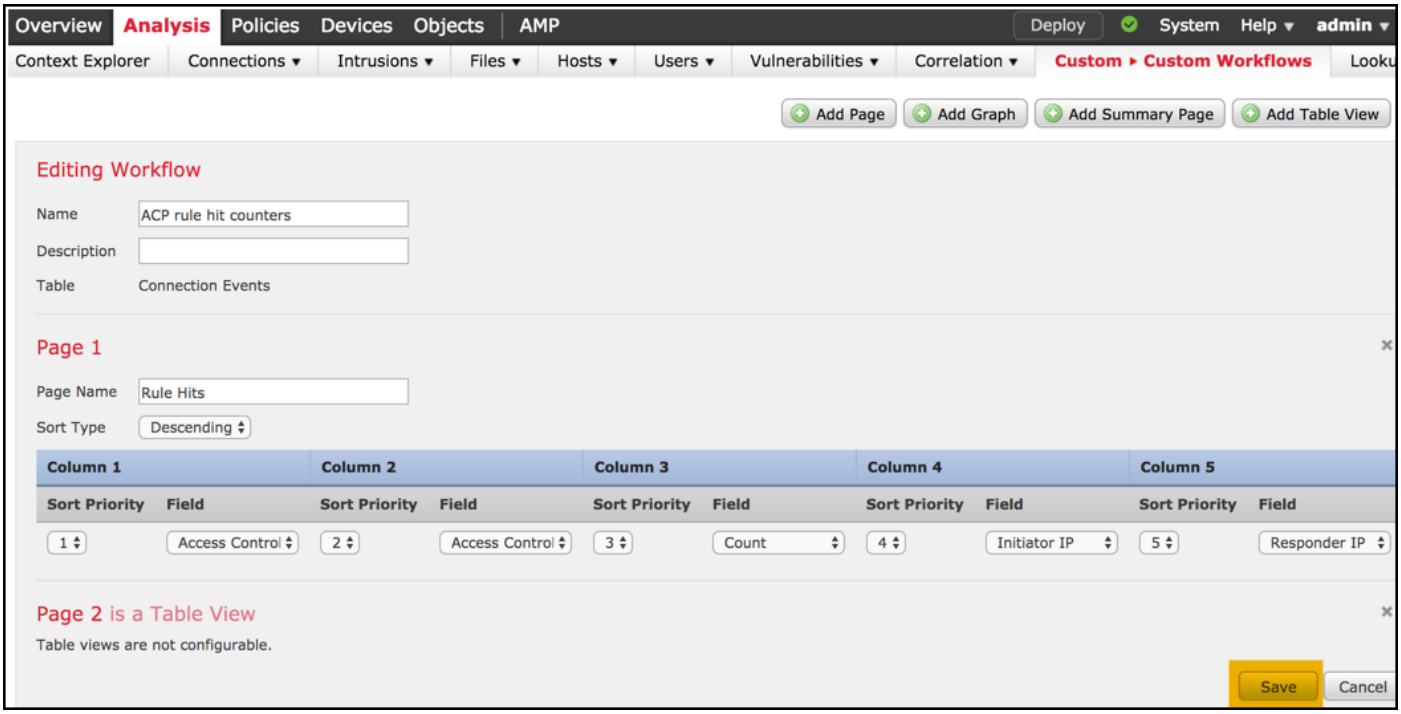
Schritt 5

Fügen Sie eine zweite Seite mit der Option **Tabellenansicht hinzufügen** hinzu.



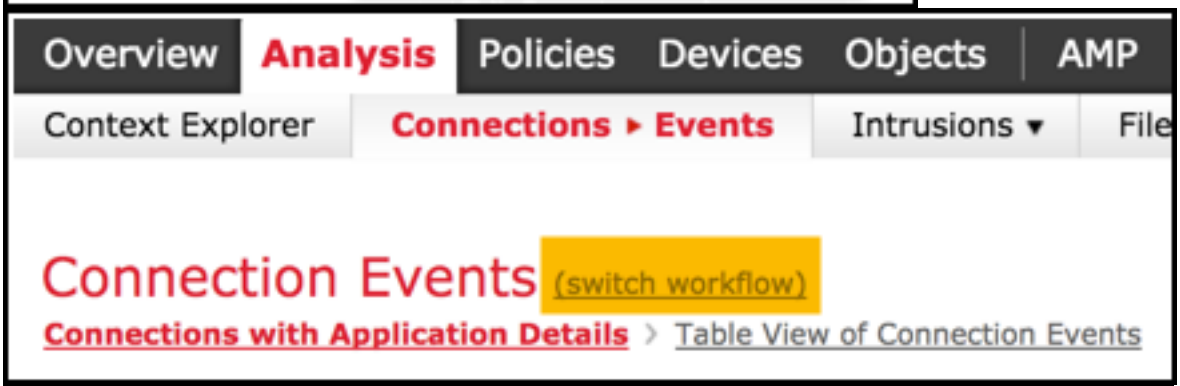
Schritt 6

Die **Tabellenansicht** ist nicht konfigurierbar. Fahren Sie daher einfach mit **Speichern** des Workflows fort.

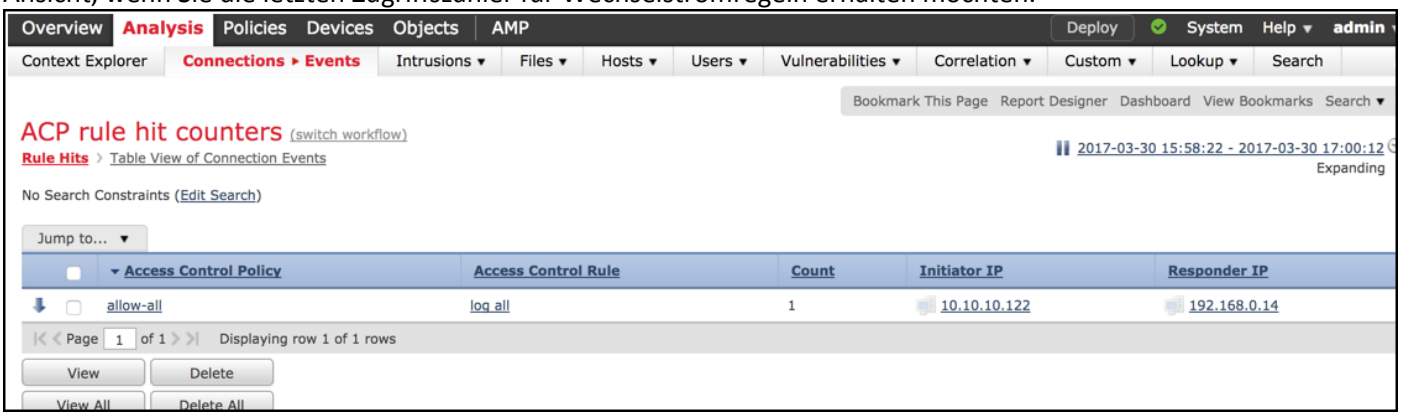


Schritt 7

Navigieren Sie zu **Analysis > Connections Events (Analyse > Verbindungsereignisse),** und wählen Sie den **Switch-Workflow aus**, wählen Sie den neu erstellten Workflow mit dem Namen **ACP-Regel für Zähler aus**, und warten Sie, bis die Seite neu geladen wird.



Nach dem Laden der Seite werden die Regelschlagzähler für jede AKP-Regel angezeigt. Aktualisieren Sie diese Ansicht, wenn Sie die letzten Zugriffszähler für Wechselstromregeln erhalten möchten.



Überprüfen

Eine Möglichkeit zur Bestätigung von Trefferzählern für Zugriffskontrollregeln auf Regelbasis für den gesamten Datenverkehr (global) kann über den Befehl **show access-control-config** CLISH (CLI SHELL) erreicht werden, der im Folgenden veranschaulicht wird:

```
> 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)
```

Fehlerbehebung

Mit dem Befehl **firewall-engine-debug** können Sie bestätigen, ob der Datenverkehrsfluss anhand der richtigen Zugriffskontrollregel bewertet wird:

```
> 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
```

Wenn Sie die Trefferzähler für die ACP-Regel **log** vergleichen**,** stellen Sie fest, dass die Ausgaben für Befehlszeile (CLI) und GUI nicht übereinstimmen. Der Grund hierfür ist, dass die CLI-Trefferzähler nach jeder Bereitstellung der Zugriffskontrollrichtlinie gelöscht werden und für den gesamten globalen Datenverkehr und nicht für bestimmte IP-Adressen gelten. Andererseits behält die FMC GUI die Zähler in der Datenbank, sodass sie die Verlaufsdaten basierend auf einem ausgewählten Zeitrahmen anzeigen können.

Zugehörige Informationen

- Benutzerdefinierte Workflows
- Erste Schritte mit Zugriffskontrollrichtlinien
- Technischer Support und Dokumentation - Cisco Systems