FireSIGHT Management Center: Kloktellers voor toegangsbeheer voor display

Inhoud

Inleiding

Voorwaarden

Dit document beschrijft de instructies om **aangepaste werkstromen** te maken op een FireSIGHT Management Center (FMC), zodat het systeem Access Control Policy (ACS) kan weergeven door tellers op wereldwijde basis en per regel te klikken. Dit is handig om problemen op te lossen of de verkeersstroom overeenkomt met de juiste regel. Het is ook handig om informatie te krijgen over het algemene gebruik van de toegangscontroleregels, bijvoorbeeld toegangscontroleregels zonder hits voor een langere periode, of om informatie te krijgen over het algemene gebruik van de toegangscontroleregels een indicatie dat de regel niet meer nodig is en mogelijk veilig van het systeem kan worden verwijderd .

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

- Virtual Firepower Management Center (FMC) - softwareversie 6.1.0.1 (gebouw 53)
- Firepower Threat Defense (FTD) 4150 - softwareversie 6.1.0.1 (Build 53)

> Opmerking: De in dit document beschreven informatie is niet van toepassing op FirePOWER Devices Manager (FDM).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Verwante producten

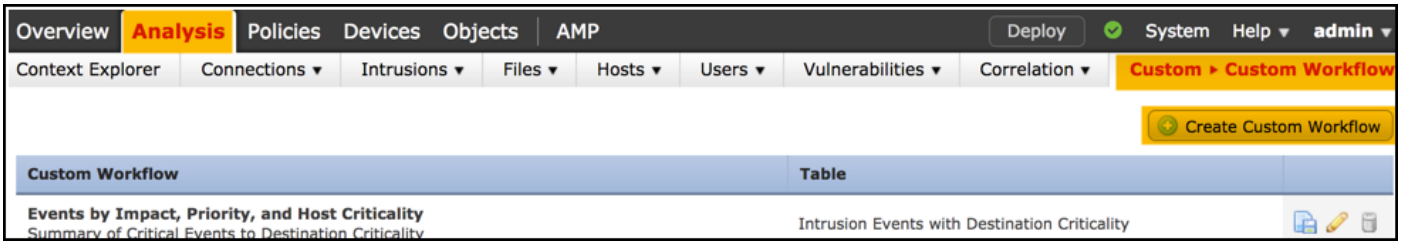
Dit document kan ook met deze hardware- en softwareversies worden gebruikt:

- Firepower Management Center (FMC) - softwareversie 6.0.x en hoger
- FireSIGHT-beheerde apparatuur - softwareversie 6.1.x en hoger

Configureren

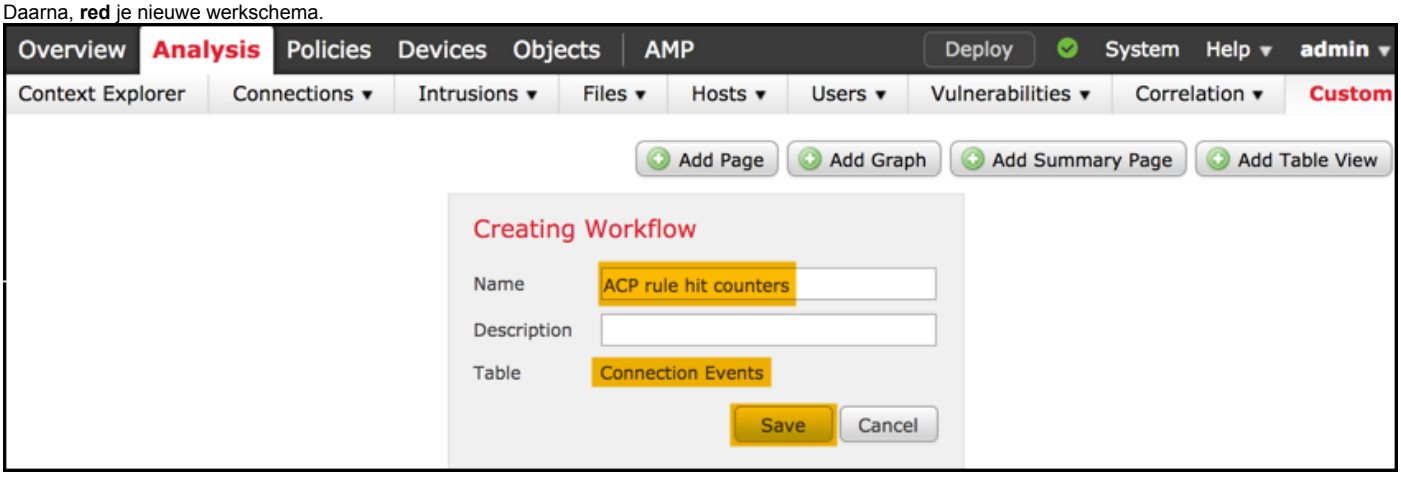
Stap 1

Om een Aangepast werkschema te maken, navigeer naar **Analyse > Aangepaste > Werkstromen > Aangepaste Werkstroom maken:**



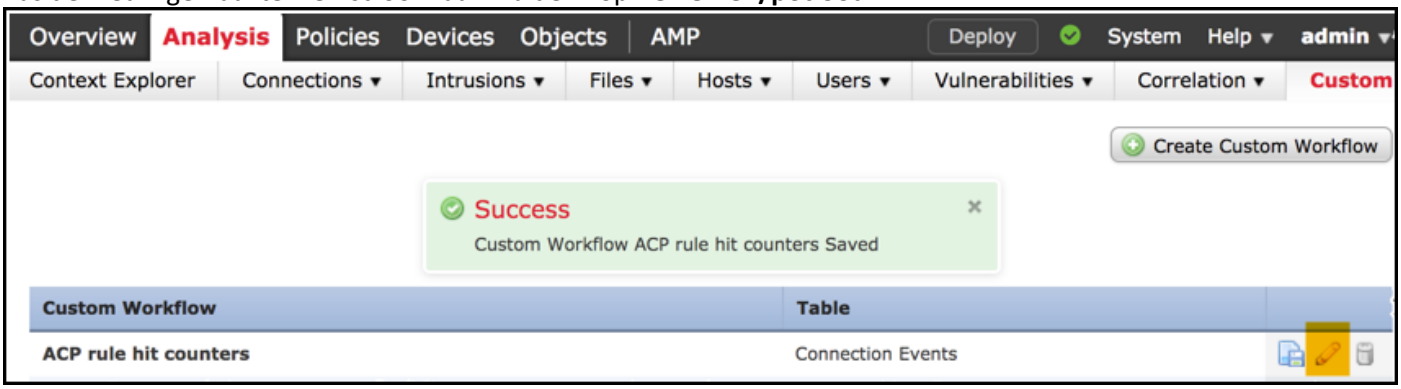
Stap 2

Defineert de naam **Aangepaste Werkstroom**, bijvoorbeeld **ACS-regel heeft tellers** ingedrukt en selecteert **verbindingsgebeurtenissen** in een tabelveld. Daarna, **red** je nieuwe werkschema.



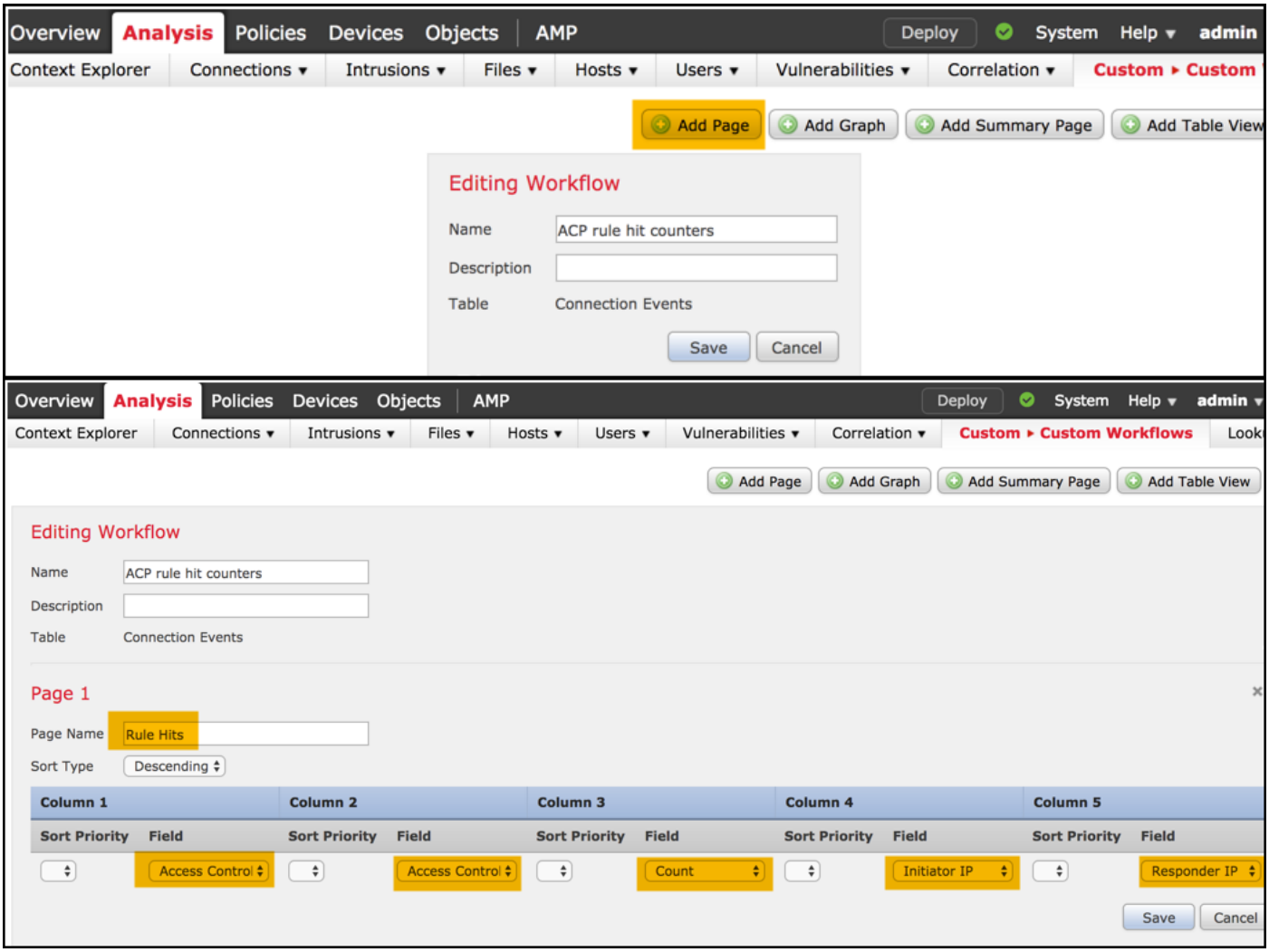
Stap 3

Pas de nieuw gemaakte werkstroom aan via de knop **Bewerken/potlood**.



Stap 4

Voeg een nieuwe pagina voor een werkschema toe met de optie **Pagina toevoegen**, definieer zijn naam en sorteren de kolom velden door **Toegangsbeheer**, **Toegangsbeheer en , IP en IP Responder**.

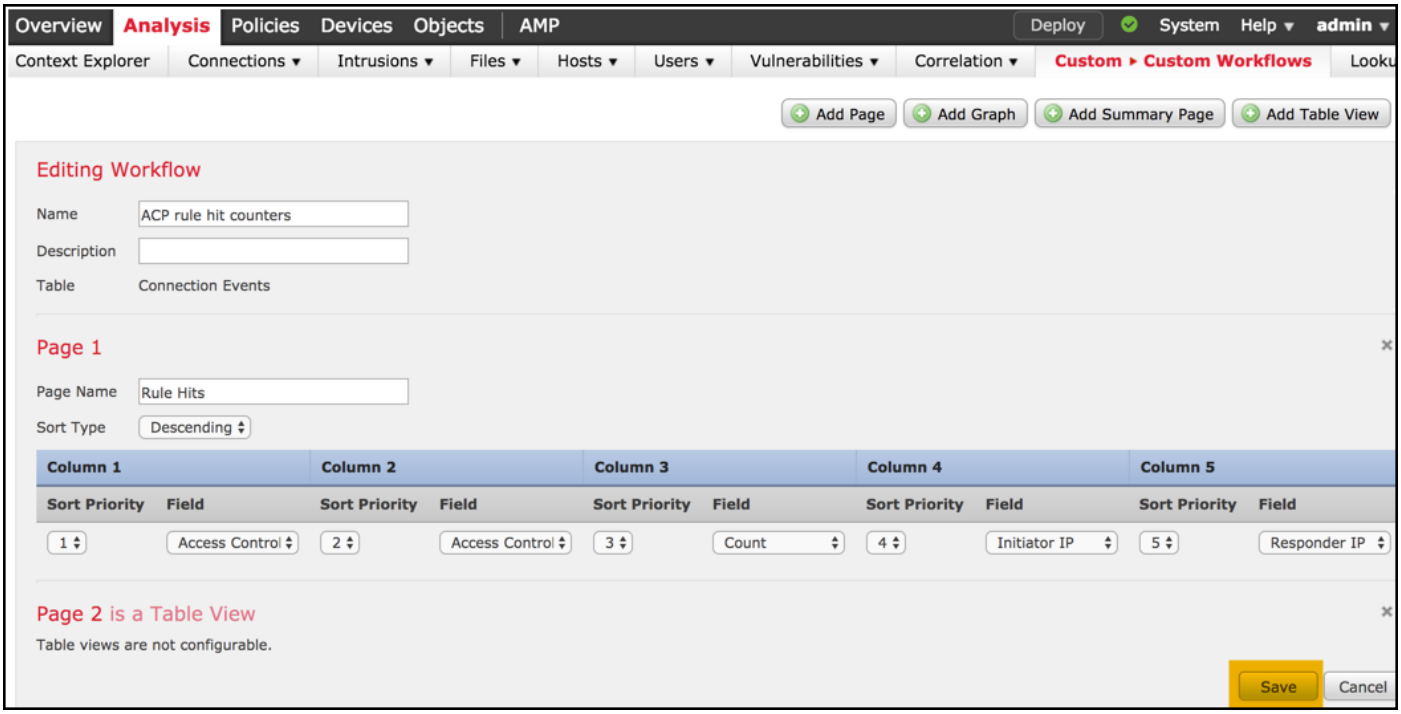


Stap 5

Voeg een tweede pagina toe met de optie **Tabelweergave toevoegen**.

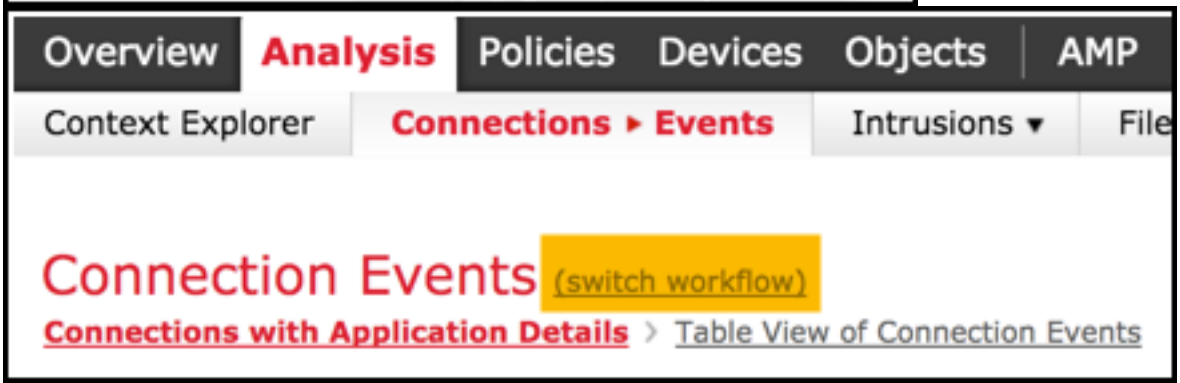
Stap 6

De **Tabelweergave** is niet configureerbaar. Ga daarom gewoon naar **Opslaan** van uw werkschema.



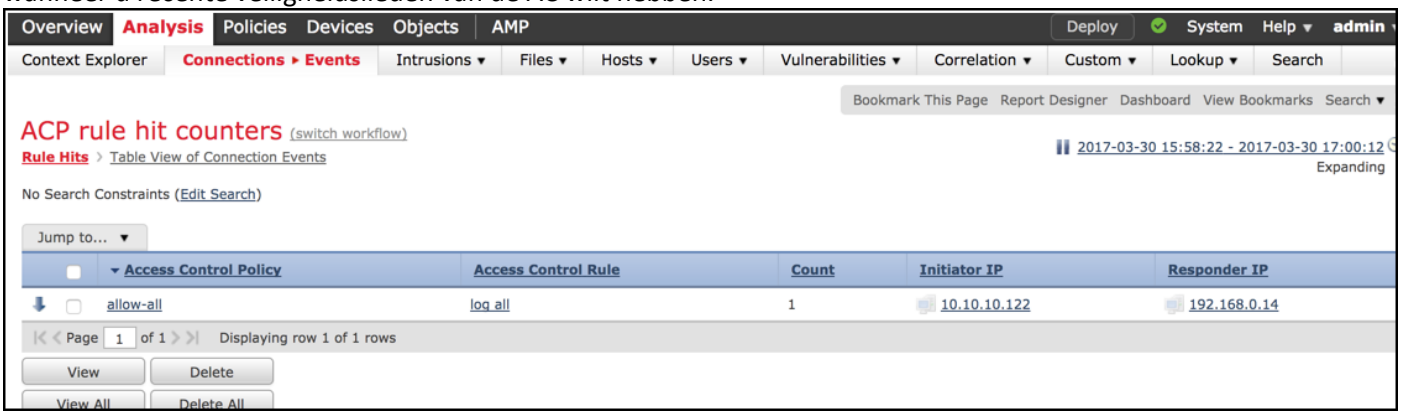
Stap 7

Navigeer naar **Analysis > Connections Events** en selecteer **switch-werkschema**, kies vervolgens de nieuw gemaakte werkschema genaamd **ACS-regel hit tellers** en wacht tot de pagina opnieuw werd geladen.



Zodra de pagina is geladen, worden de regelgetroffen tellers per elke ACS-regel weergegeven, verfrist u deze mening

wanneer u recente veiligheidslieden van de AC wilt hebben.



Verifiëren

Een manier om toegangscontrole regelteller op regelbasis voor al verkeer (globaal) te bevestigen kan van FTD CLISH (CLI SHELL) **tonen toegang-controle-klaar** bevel, dat hieronder wordt gedemonstreerd:

```
> 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)
```

Problemen oplossen

Met de opdracht **firewall-engine-debug** kunt u bevestigen of de verkeersstroom tegen de juiste regel voor toegangscontrole is geëvalueerd:

```
> 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
```

Wanneer u de slagtelers voor de ACS-regel vergelijkt met de naam **log**, merkt u **alles** op dat de uitvoer van de Opdracht Line (CLI) en GUI niet overeenkomt. De reden is dat de CLI hit tellers na elke plaatsing van het Toegangsbeheer worden ontruimd en op al verkeer wereldwijd en niet op een specifieke IP adressen van toepassing zijn. Aan de andere kant houdt FMC GUI de tellers in de database, zodat deze de historische gegevens kan weergeven op basis van een geselecteerd tijdframe.

Gerelateerde informatie

- Aangepaste werkstromen
- Om te beginnen met beleid voor toegangscontrole
- Technische ondersteuning en documentatie – Cisco Systems