Центр управления огневой мощи: отобразите счетчики попаданий политики контроля доступа

Содержание

Введение

Предварительные условия

Этот документ описывает инструкции для создания **Пользовательских Потоков операций** на Центре управления огневой мощи (FMC), который позволяет системе отображать счетчики попаданий Политики контроля доступа (ACP) на глобальной и основе на правило. Это полезно для устранения неполадок, совпадает ли трафик с корректным правилом. Также полезно получить информацию об общем использовании правил Управления доступом, например правила Управления доступом без соответствий для длительного периода времени времени могли бы быть индикацией, что правило больше не необходимо и могло быть потенциально безопасно удалено из системы.

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

- Действительный Центр управления огневой мощи (FMC) - версия программного обеспечения 6.1.0.1 (создают 53),
- Защита угрозы огневой мощи (FTD) 4150 - версия программного обеспечения 6.1.0.1 (Сборка 53)

> **Примечание:** Информация, описанная в этом документе, не применима к Менеджеру устройств огневой мощи (FDM).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Родственные продукты

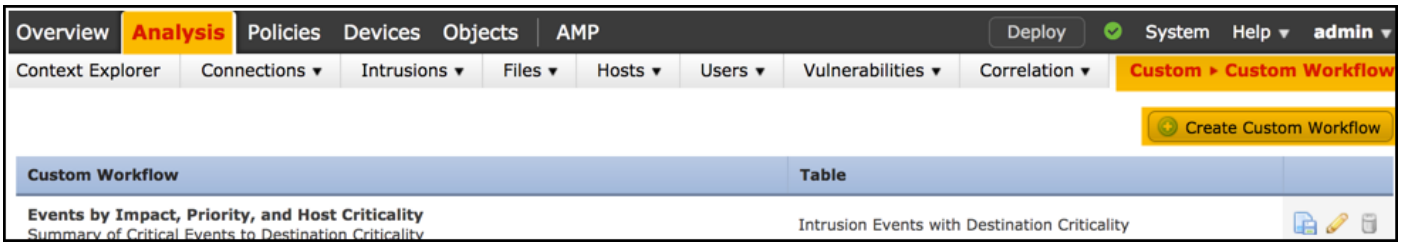
Данный документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- Центр управления огневой мощи (FMC) - версия программного обеспечения 6.0.x и выше
- Огневая мощь управляла устройствами - версия программного обеспечения 6.1.x и выше

Настройка

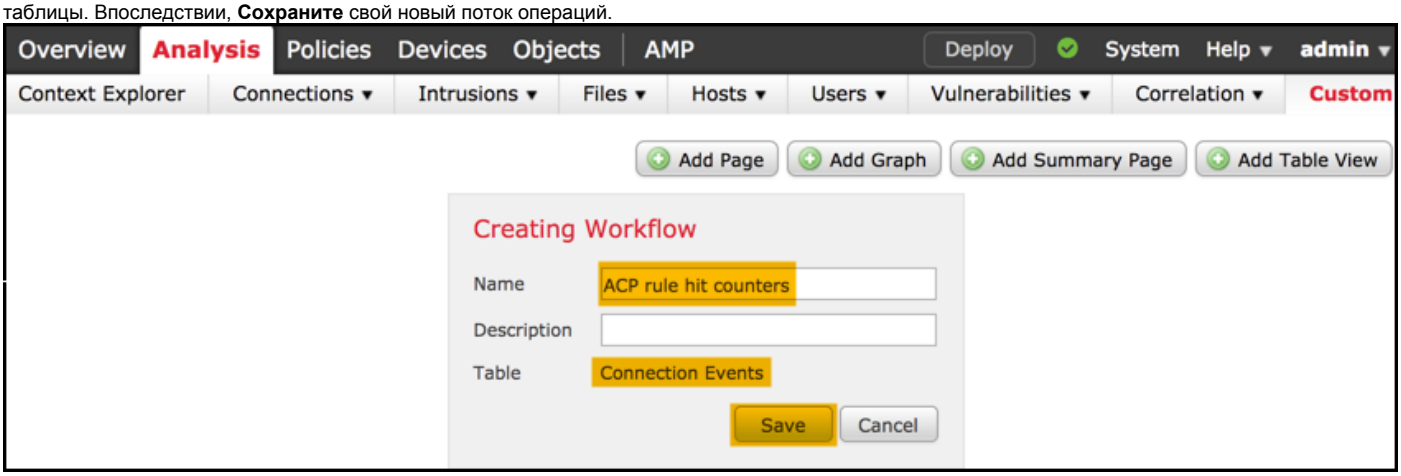
Шаг 1

Для создания Пользовательского Потока операций перейдите к **Анализу> Пользовательский>, Пользовательские Потоки операций> Создают Пользовательский Поток операций:**



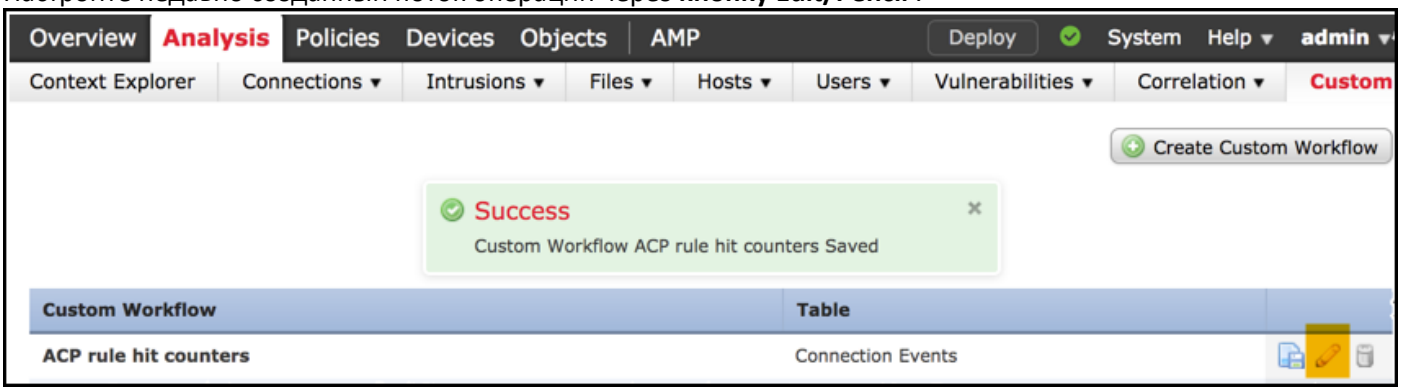
Шаг 2

Определите **Пользовательское** название **Потока операций**, например **счетчики попаданий правила ACP** и выберите **Connection Events** в поле таблицы. Впоследствии, **Сохраните** свой новый поток операций.



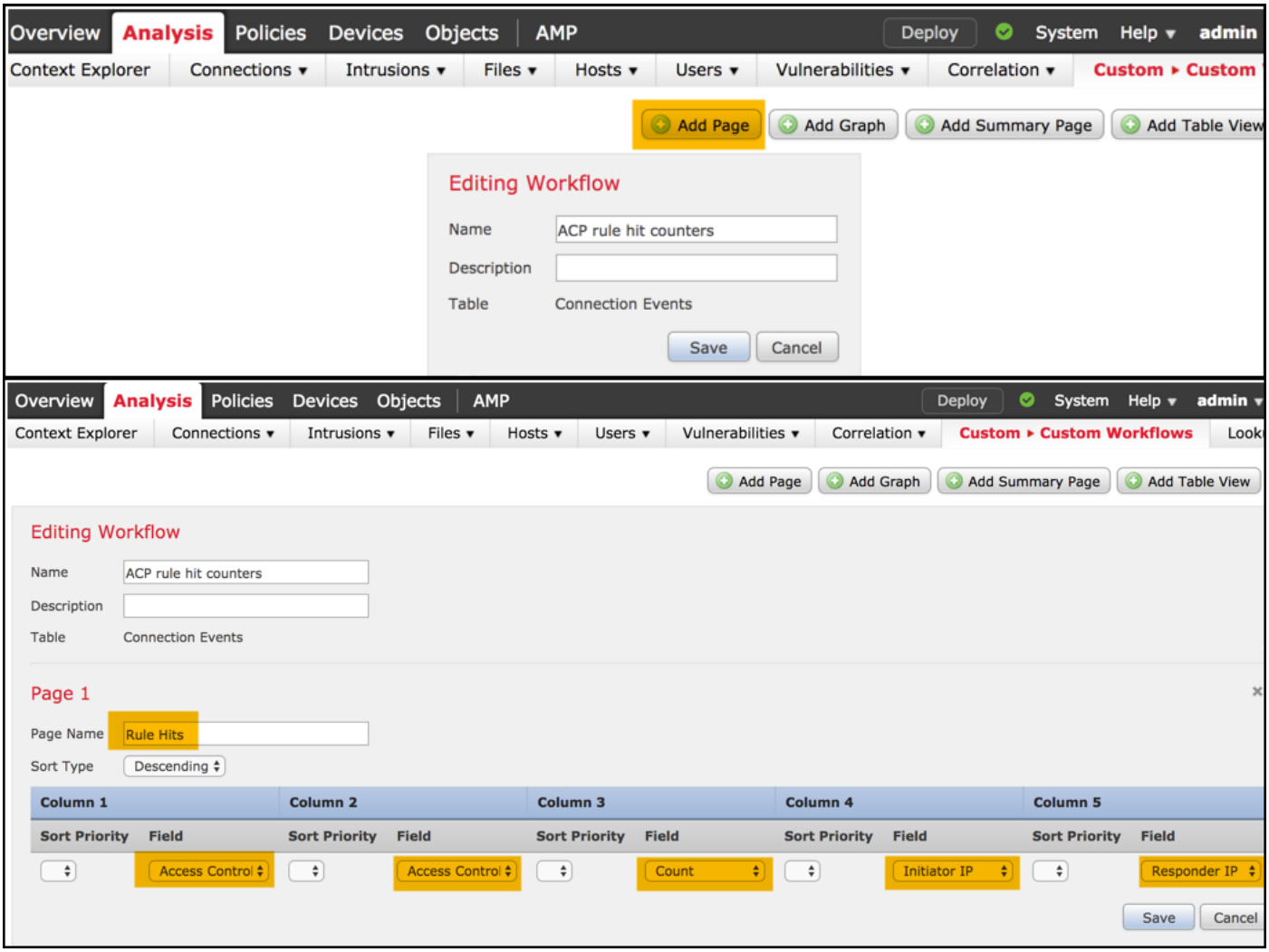
Шаг 3

Настройте недавно созданный поток операций через **кнопку Edit/Pencil** .



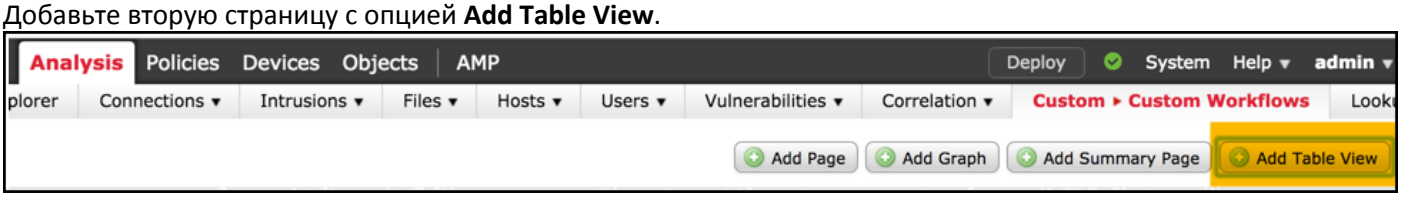
Шаг 4.

Добавьте новую страницу для потока операций с опцией **Страницы Add**, определите ее название и сортируйте поля столбца **Политикой контроля доступа**, **Правилом Управления доступом** и **количеством**, полями **Initiator IP и Responder IP**.



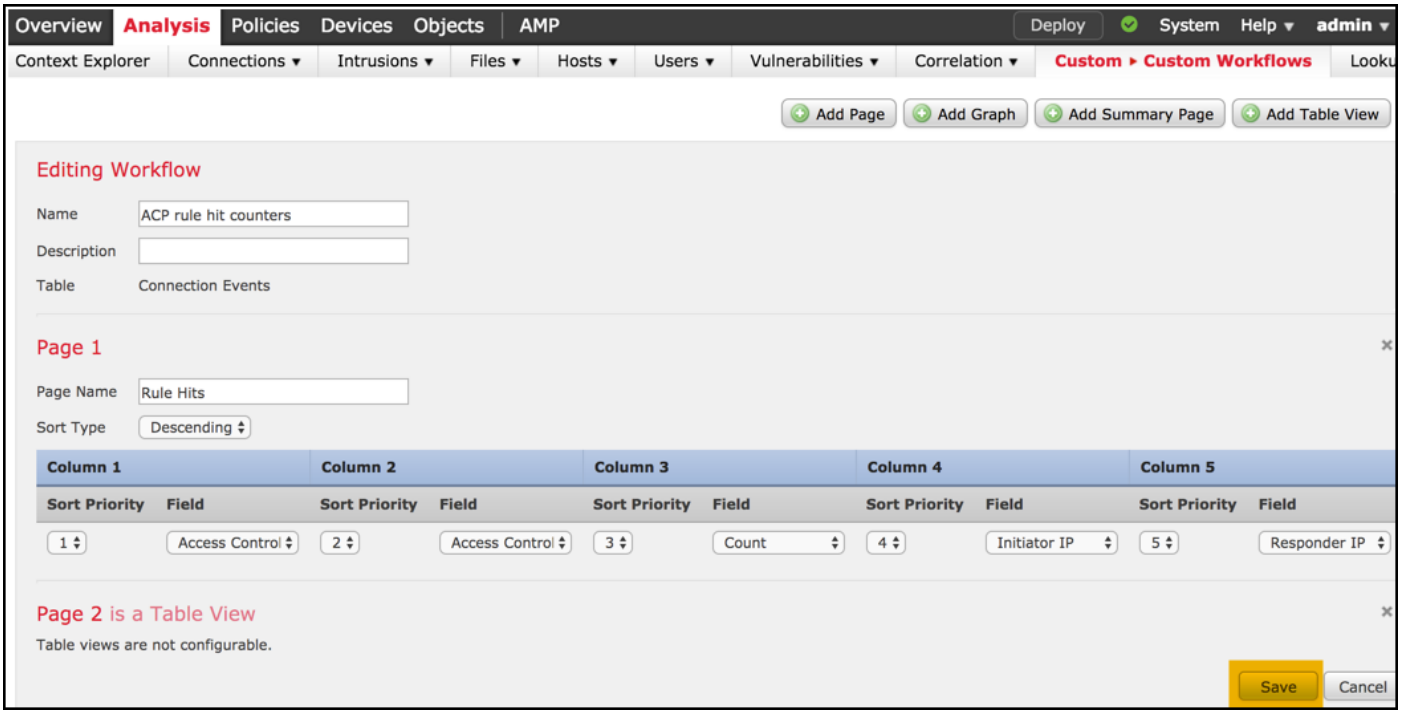
Шаг 5.

Добавьте вторую страницу с опцией **Add Table View**.



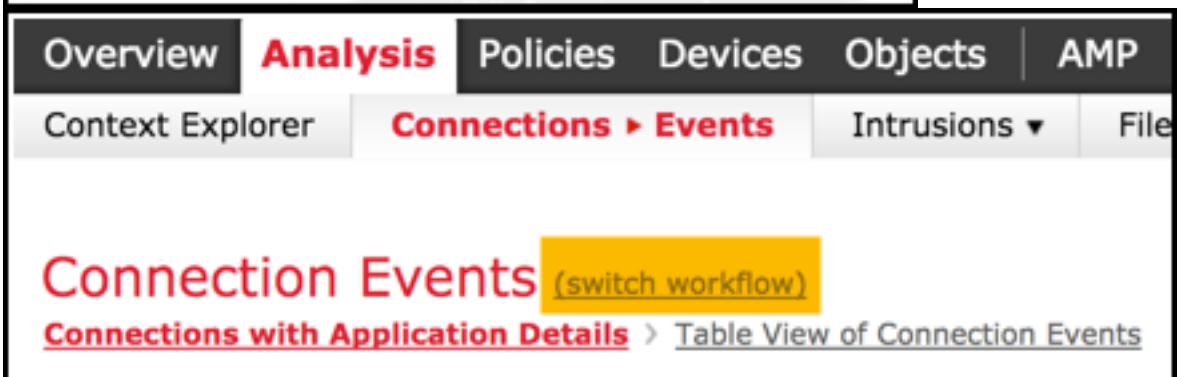
Шаг 6

Табличное представление не конфигурируемо, следовательно только продолжите **Сохранять** свой поток операций.

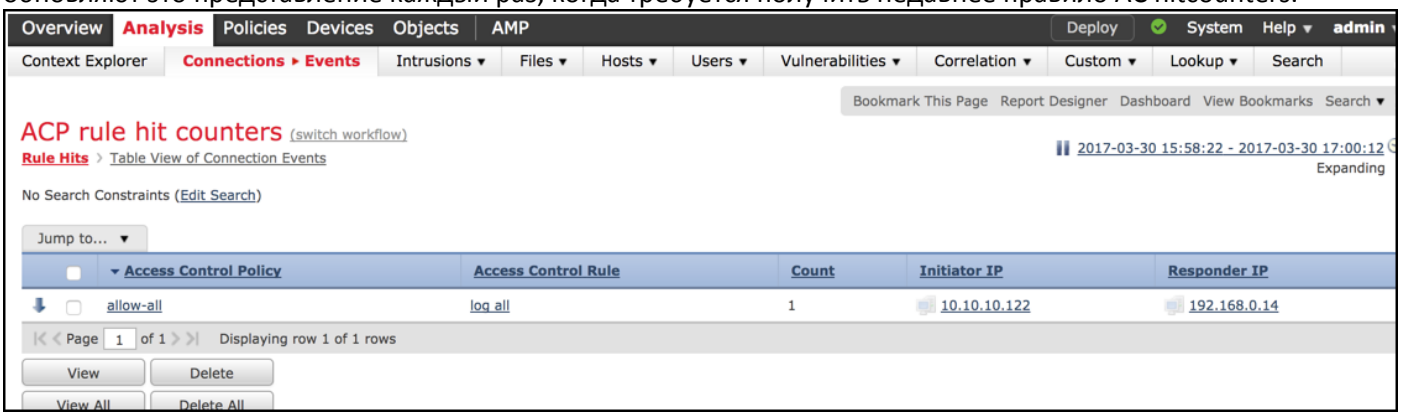


Шаг 7

Перейдите к **Анализу> События Соединений** и **поток операций Выберитя коммутатор**, затем выберите недавно созданный поток операций, названный **счетчиками попаданий правила ACP** , и ждите до повторных загрузок страницы.



Как только страница загружена, счетчики попаданий правила на каждое правило ACP отображены, просто обновляют это представление каждый раз, когда требуется получить недавнее правило AC hitcounters.



Проверка

Способ подтвердить счетчики попаданий правила Управления доступом на основе правила для всего трафика (глобально) может быть достигнут от FTD CLISH (ОБОЛОЧКА CLI) **показывают команду access-control-config** , которая продемонстрирована ниже:

```
> 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)
```

Устранение неполадок

С **командой отладки механизма межсетевого экрана** можно подтвердить, оценен ли трафик против правила Контроля за соответствующим доступом:

```
> 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
```

При сравнении счетчиков попаданий для правила ACP, названного **журналом все** , что вы замечаете, что не совпадает Командная строка (CLI) и выходные данные GUI. Причина состоит в том, что счетчики попаданий CLI очищены после каждых развертываний Политики контроля доступа и применяются ко всему трафику глобально а не к определенные IP-адреса. На другой руке GUI FMC поддерживает счетчики в базе данных, таким образом, это может отобразить исторические данные на основе выбранного выделенного интервала времени.

Дополнительные сведения

- Пользовательские потоки операций
- Начало работы с политикой контроля доступа
- Cisco Systems – техническая поддержка и документация