Firepower Management Center: Display Access Control Policy Hit Counters

Contents

Introduction

Prerequisites

This document describes the instructions to create **Custom Workflows** on a Firepower Management Center (FMC) which allows the system to display Access Control Policy (ACP) hit counters on global and per-rule basis. This is useful to troubleshoot whether the traffic flow matches the correct rule. It is also helpful to get information about the general usage of the Access Control rules, for example Access Control rules with no hits for an extended period of the time might be an indication that the rule is not needed anymore and could be potentially safely removed from the system.

Requirements

There are no specific requirements for this document.

Components Used

- Virtual Firepower Management Center (FMC) - software version 6.1.0.1 (build 53)
- Firepower Threat Defense (FTD) 4150 - software version 6.1.0.1 (Build 53)

> **Note**: The information described in this document is not applicable to Firepower Device Manager (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. If your network is live, ensure that you understand the potential impact of any command.

Related Products

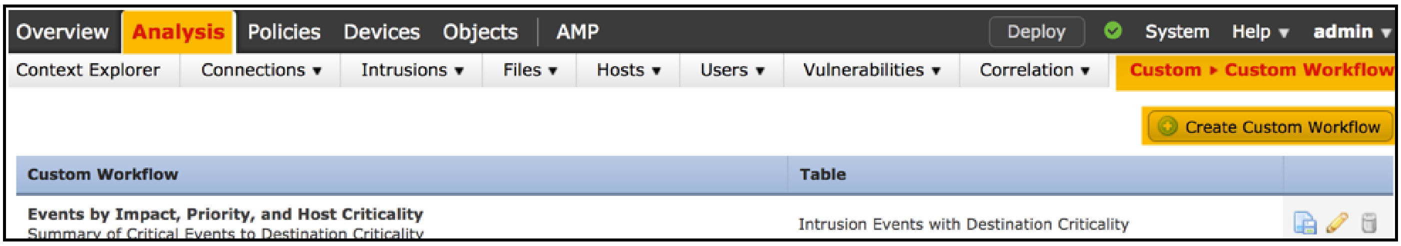
This document can also be used with these hardware and software versions:

- Firepower Management Center (FMC) - software version 6.0.x and higher
- Firepower managed appliances - software version 6.1.x and higher

Configure

Step 1

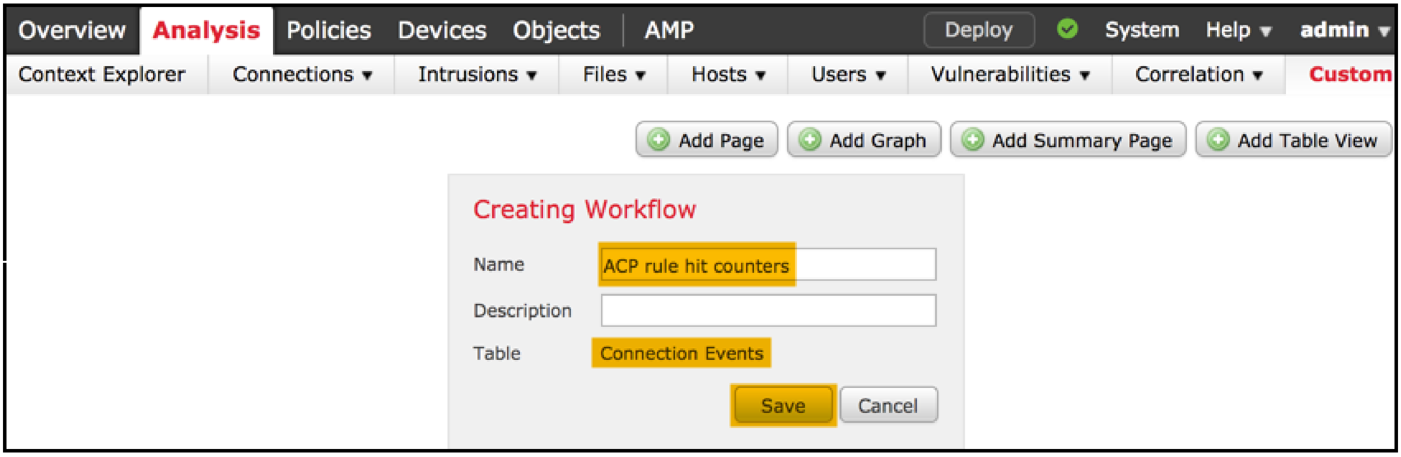
In order to create a Custom Workflow, navigate to **Analysis > Custom > Custom Workflows > Create Custom Workflow:**



Custom Workflow	Table
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality	Intrusion Events with Destination Criticality

Step 2

Define the **Custom Workflow** name, for example **ACP rule hit counters** and select **Connection Events** in a table field. Afterwards, **Save** your new workflow.



Creating Workflow

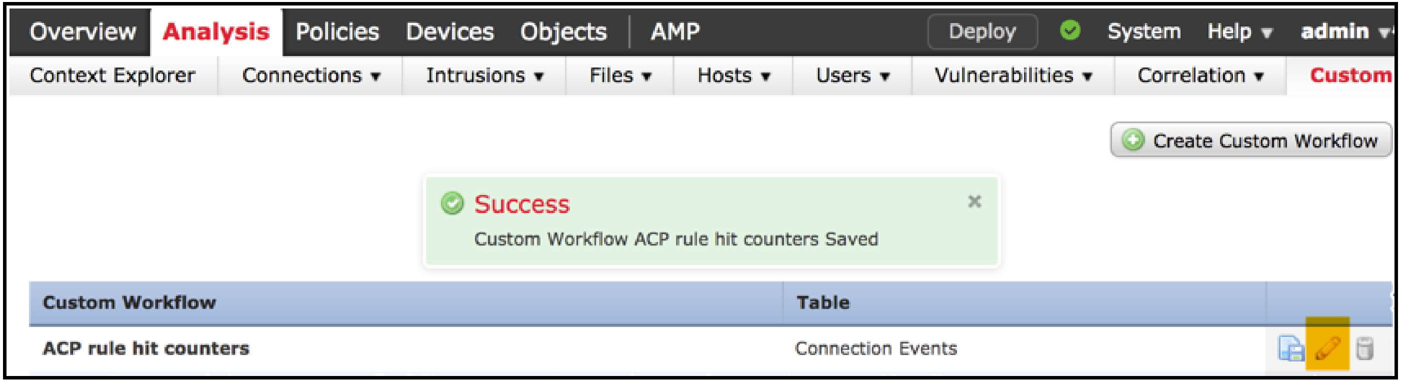
Name: ACP rule hit counters

Description:

Table: Connection Events

Step 3

Customize the newly created workflow via the **Edit/Pencil** button.



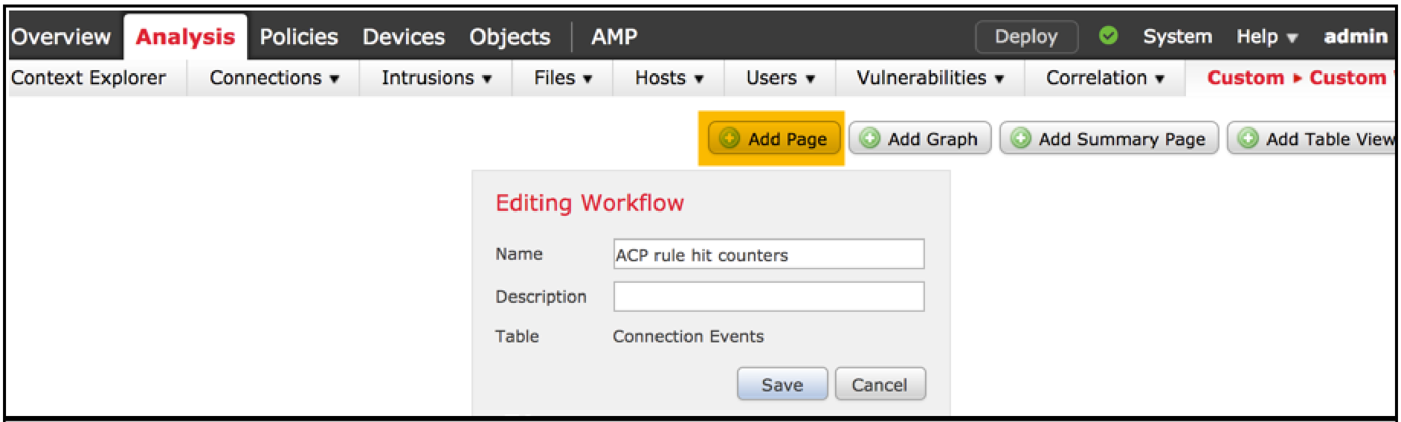
Success

Custom Workflow ACP rule hit counters Saved

Custom Workflow	Table
ACP rule hit counters	Connection Events

Step 4

Add a new page for a workflow with the **Add Page** option, define its name and sort the column fields by **Access Control Policy**, **Access Control Rule** and by **Count**, **Initiator IP** and **Responder IP** fields.

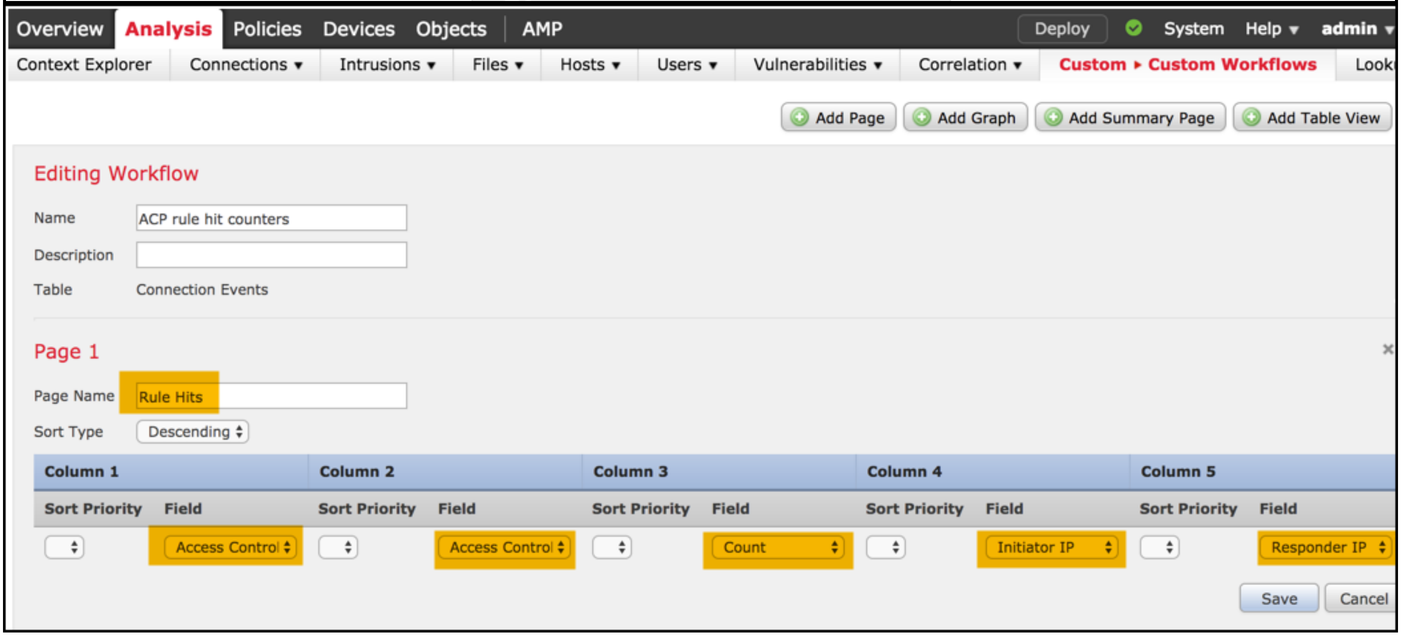


Editing Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events



Editing Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events

Page 1

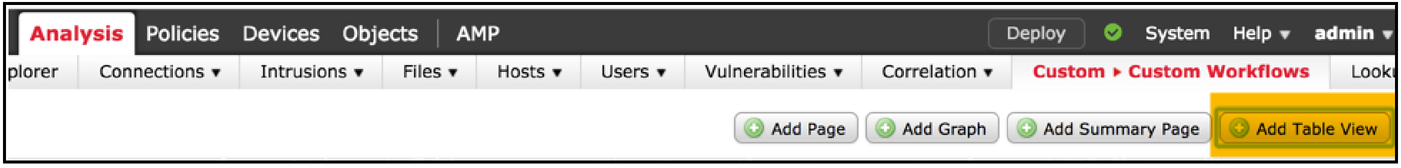
Page Name: Rule Hits

Sort Type: Descending

Column 1		Column 2		Column 3		Column 4		Column 5	
Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
	Access Control		Access Control		Count		Initiator IP		Responder IP

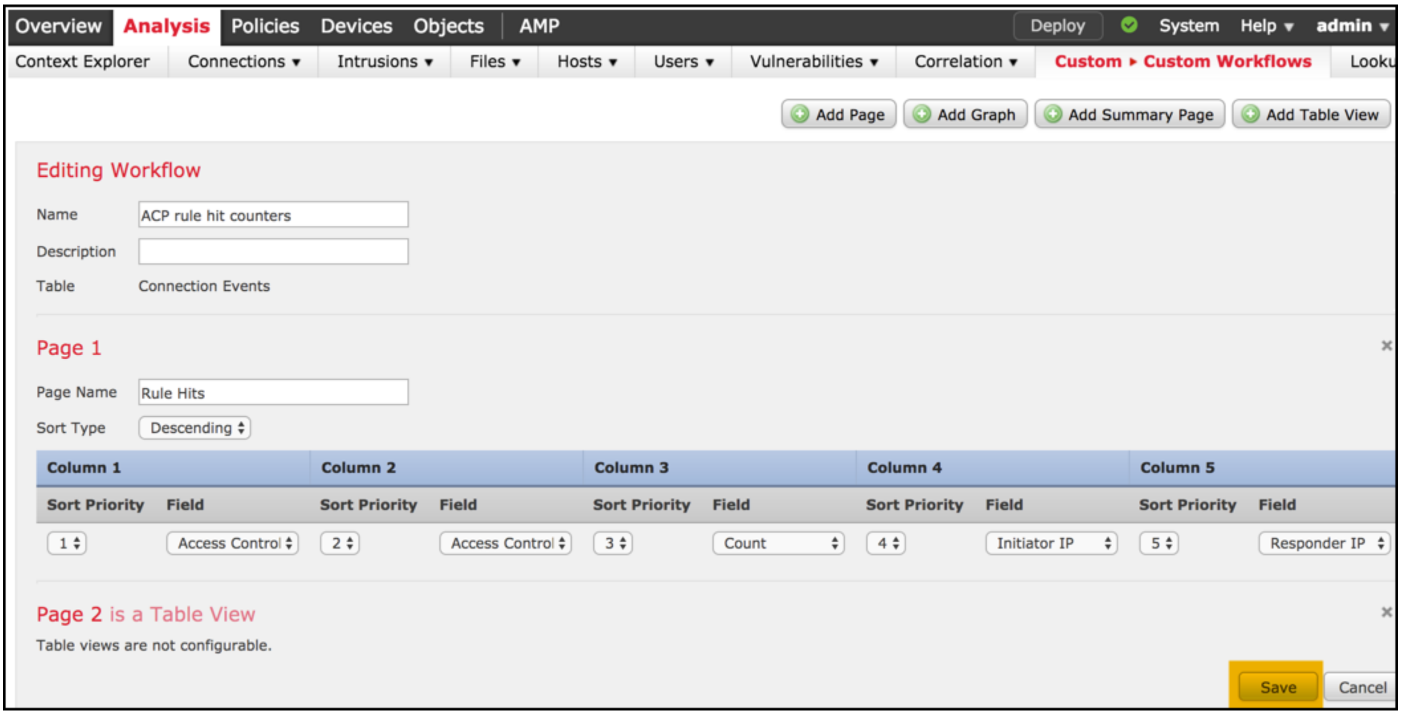
Step 5

Add a second page with the **Add Table View** option.



Step 6

The **Table View** is not configurable, hence just proceed to **Save** your workflow.



Editing Workflow

Name: ACP rule hit counters

Description:

Table: Connection Events

Page 1

Page Name: Rule Hits

Sort Type: Descending

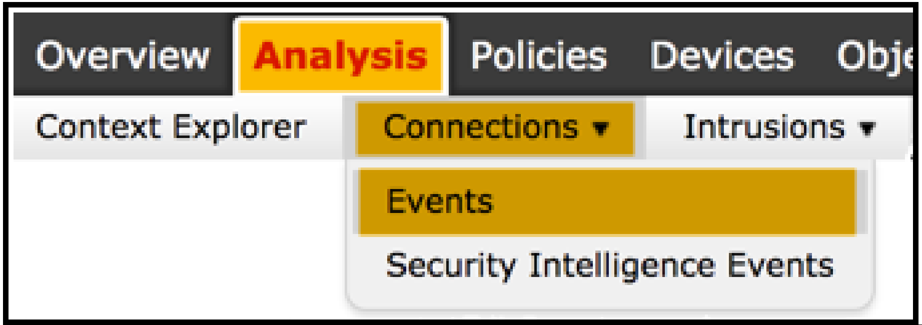
Column 1		Column 2		Column 3		Column 4		Column 5	
Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1	Access Control	2	Access Control	3	Count	4	Initiator IP	5	Responder IP

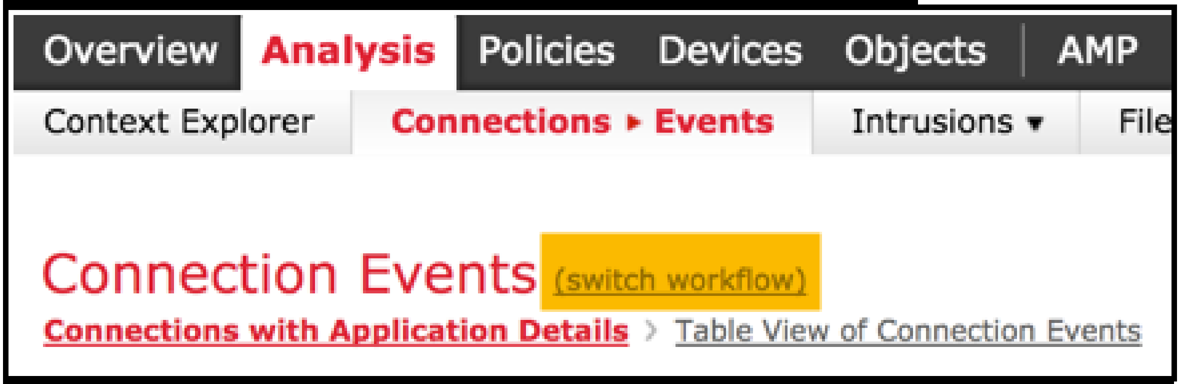
Page 2 is a Table View

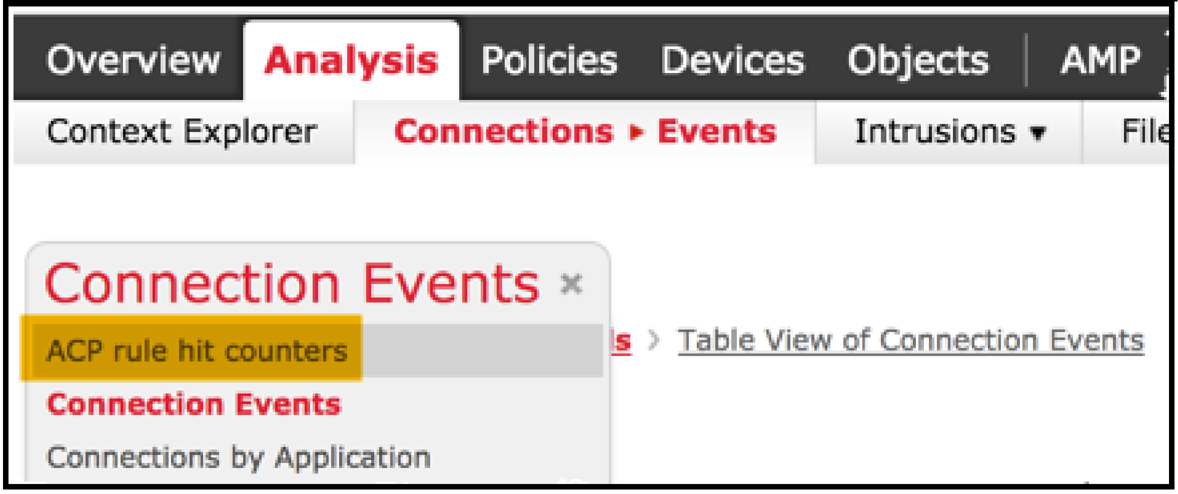
Table views are not configurable.

Step 7

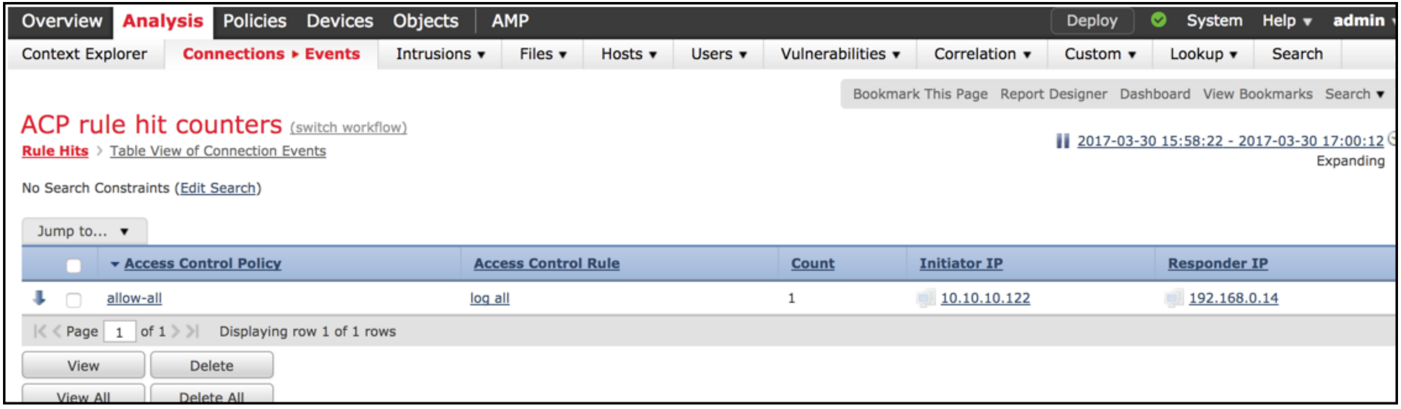
Navigate to **Analysis > Connections Events** and select **switch workflow**, then choose the newly created workflow named **ACP rule hit counters** and wait until the page reloads.







Once the page is loaded, the rule hit counters per each ACP rule are displayed, just refresh this view anytime you would like to get recent AC rule hitcounters.



ACP rule hit counters (switch workflow)

Rule Hits > Table View of Connection Events

2017-03-30 15:58:22 - 2017-03-30 17:00:12

Expanding

No Search Constraints (Edit Search)

	▾ Access Control Policy	Access Control Rule	Count	Initiator IP	Responder IP
□	allow-all	log all	1	10.10.10.122	192.168.0.14

Page 1 of 1 Displaying row 1 of 1 rows

Verify

A way to confirm Access Control rule hit counters on rule basis for all traffic (globally) can be achieved from FTD CLISH (CLI SHELL) **show access-control-config** command, which is demonstrated below:

```
> 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)
```

Troubleshoot

With the **firewall-engine-debug** command you can confirm whether traffic flow is evaluated against the proper Access Control rule:

```
> 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
```

When you compare the hit counters for the ACP rule named **log all** you notice that the Command Line (CLI) and GUI outputs do not match. The reason is that the CLI hit counters are cleared after each Access Control Policy deployment and apply to all traffic globally and not to a specific IP addresses. On other hand, FMC GUI keep the counters in the database, so it can display the historical data based on a selected time frame.

Related Information

- Custom Workflows
- Getting Started with Access Control Policies
- Technical Support & Documentation - Cisco Systems