Configure Firesight Management Center to Display the Hit-Counts per Access Rule

Contents

Introduction

This document describes how to configure custom workflow/event viewer page to depict the connection hit-counts per access rule name. The configuration shows a basic example of rule name field associated with hit-counts and how to add additional fields if required.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower Technology
- Knowledge of basic navigation within the Firesight Management Center

Components Used

The information in this document is based on these software and hardware versions:

- Firepower Management Center version 6.1.X and above
- Applicable to managed Threat Defense/Firepower Sensors

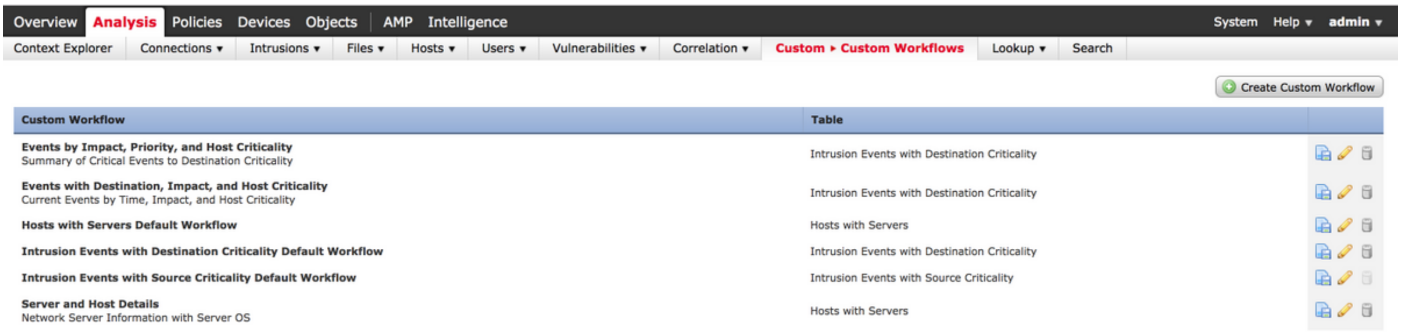
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Configurations

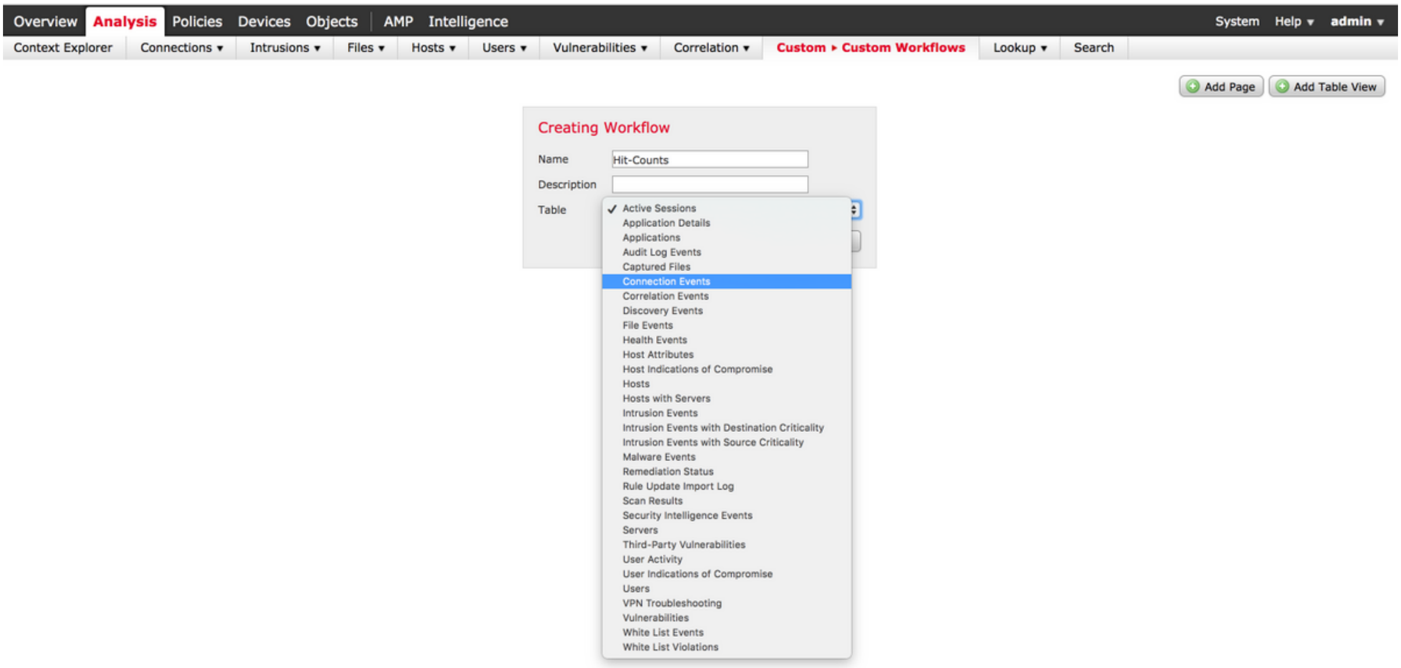
Step 1. Login to the Firesight Management Center with administrator privileges.

Once the login is successful navigate to **Analysis > Custom > Custom Workflows**, as shown in the image:



Custom Workflow	Table
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality	Intrusion Events with Destination Criticality
Events with Destination, Impact, and Host Criticality Current Events by Time, Impact, and Host Criticality	Intrusion Events with Destination Criticality
Hosts with Servers Default Workflow	Hosts with Servers
Intrusion Events with Destination Criticality Default Workflow	Intrusion Events with Destination Criticality
Intrusion Events with Source Criticality Default Workflow	Intrusion Events with Source Criticality
Server and Host Details Network Server Information with Server OS	Hosts with Servers

Step 2. Click on **Create Custom Workflow** and choose the parameters as shown in the image:



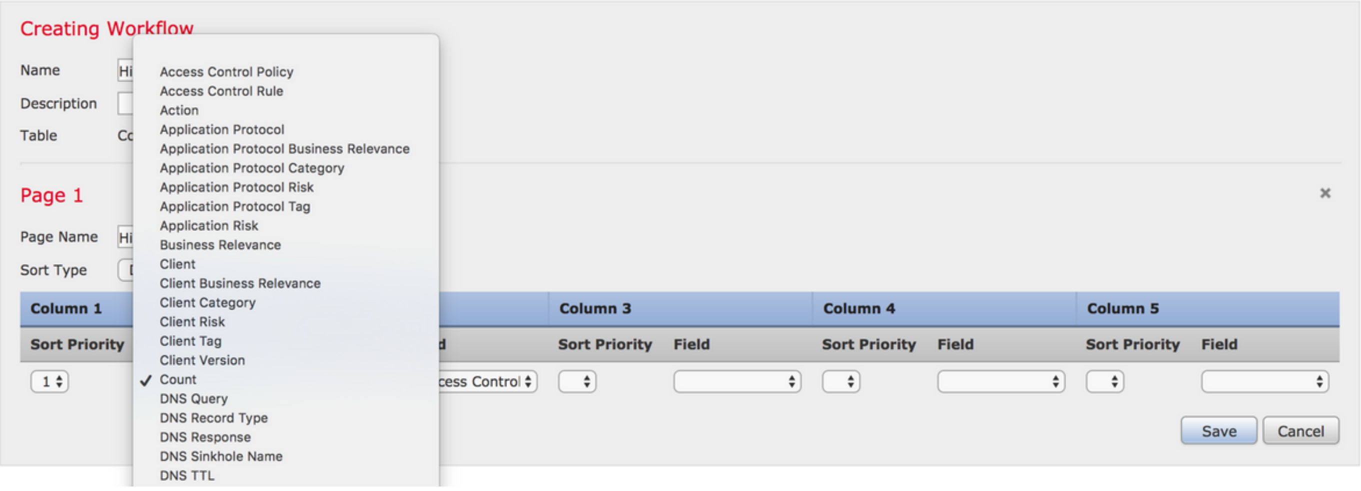
Creating Workflow

Name: Hit-Counts

Description:

Table: Connection Events

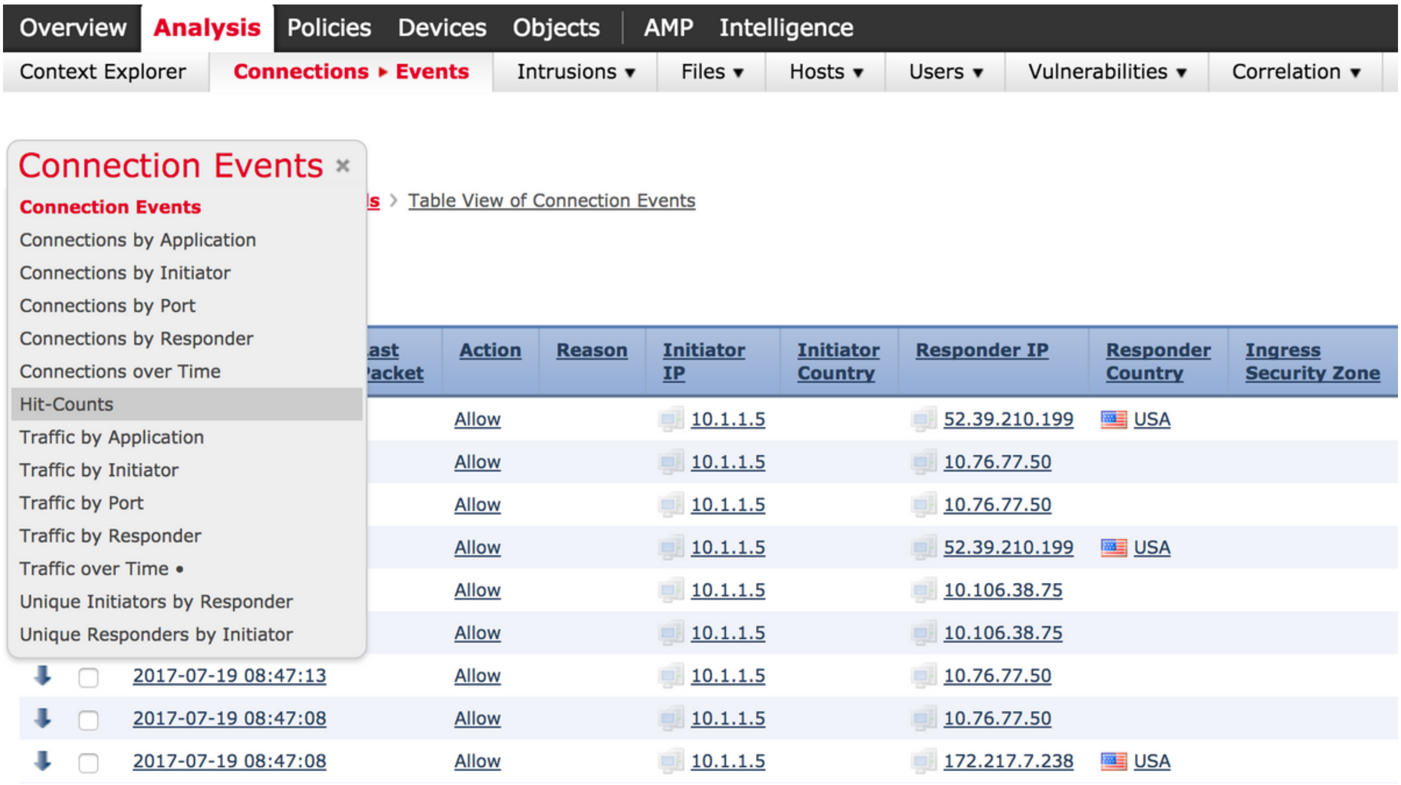
Step 3. Select the table field as **Connection Events** and enter a Workflow name, then click on **Save**. Once the workflow is saved, click on **Add Page** as shown in the image:



Note: The first column has to be Count and then in the additional Column you can choose among the available fields from the drop-down. In this case, the first column is a Count and the second column is Access Control Rule.

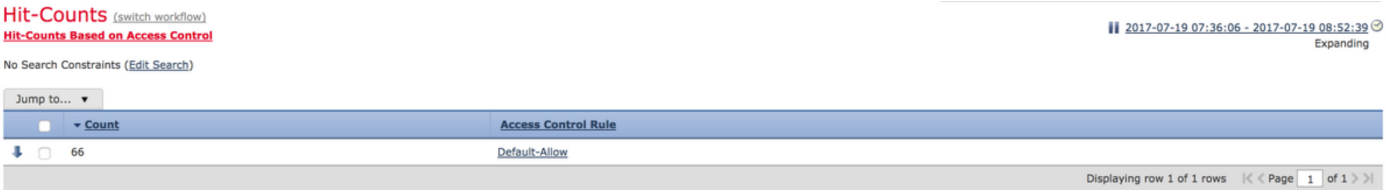
Step 4. Once the workflow page is added, click on **Save.**

In order to view the hit-counts, navigate to **Analysis > Connections > Events** and click on **Switch Workflows**, as shown in the image:



		ast Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone
			Allow		10.1.1.5		52.39.210.199	USA	
			Allow		10.1.1.5		10.76.77.50		
			Allow		10.1.1.5		10.76.77.50		
			Allow		10.1.1.5		52.39.210.199	USA	
			Allow		10.1.1.5		10.106.38.75		
			Allow		10.1.1.5		10.106.38.75		
⬇	□	2017-07-19 08:47:13	Allow		10.1.1.5		10.76.77.50		
⬇	□	2017-07-19 08:47:08	Allow		10.1.1.5		10.76.77.50		
⬇	□	2017-07-19 08:47:08	Allow		10.1.1.5		172.217.7.238	USA	

Step 5. From the drop down, choose the Custom Workflow that you have created (in this case Hit-Counts), as shown in the image:



Hit-Counts (switch workflow)
Hit-Counts Based on Access Control

2017-07-19 07:36:06 - 2017-07-19 08:52:39
Expanding

No Search Constraints (Edit Search)

□	Count	Access Control Rule
□	66	Default-Allow

Displaying row 1 of 1 rows

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.