Configuration to View Changes in an Access Control Policy

Contents

Introduction

This document describes how to view/check the changes made to an Access Control Policy (ACP). This is also applicable to determine the changes made to interface settings.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower Technology

Components used

The information in this document is based on Firepower Management Center 6.1.0.5 and above.

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.

Configure

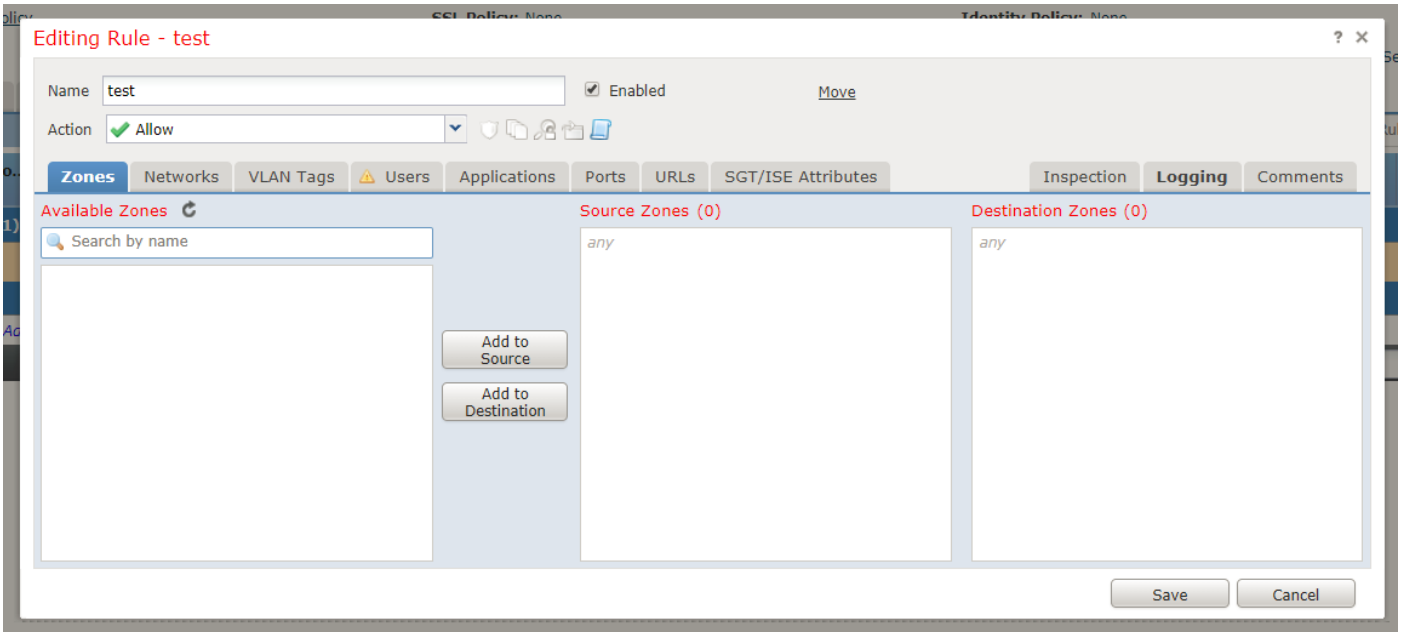
Configurations

Step 1. Login to the GUI of the Firepower Management Center using administrator privileges.

Step 2. Navigate to **Policies > Access Control** and click to edit (or even create a new) a policy.

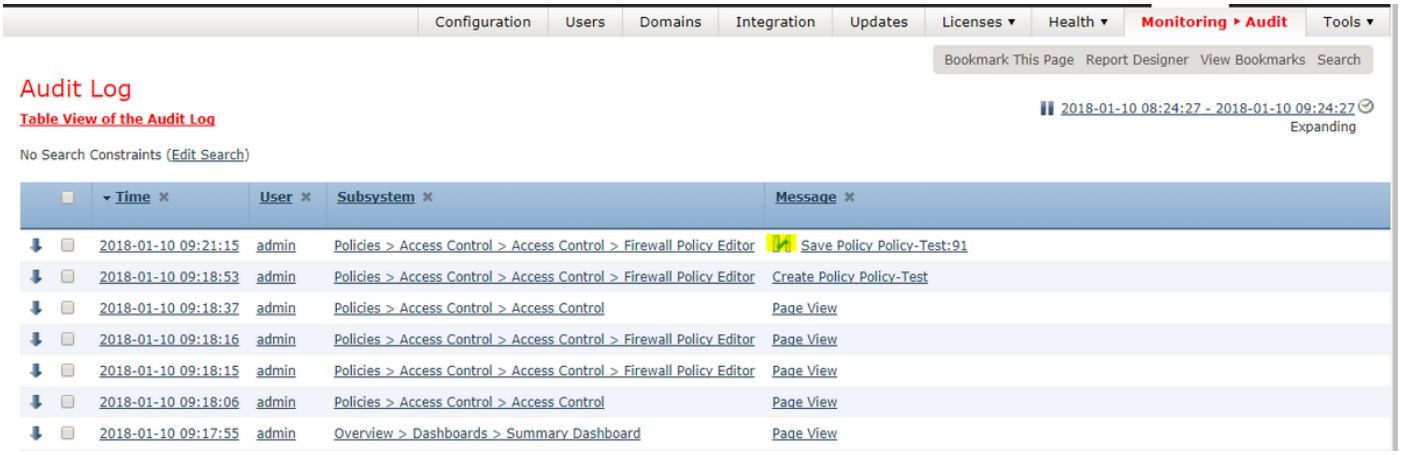
Example:

Make some changes to the policy. For instance, add a new rule, as shown in the image:



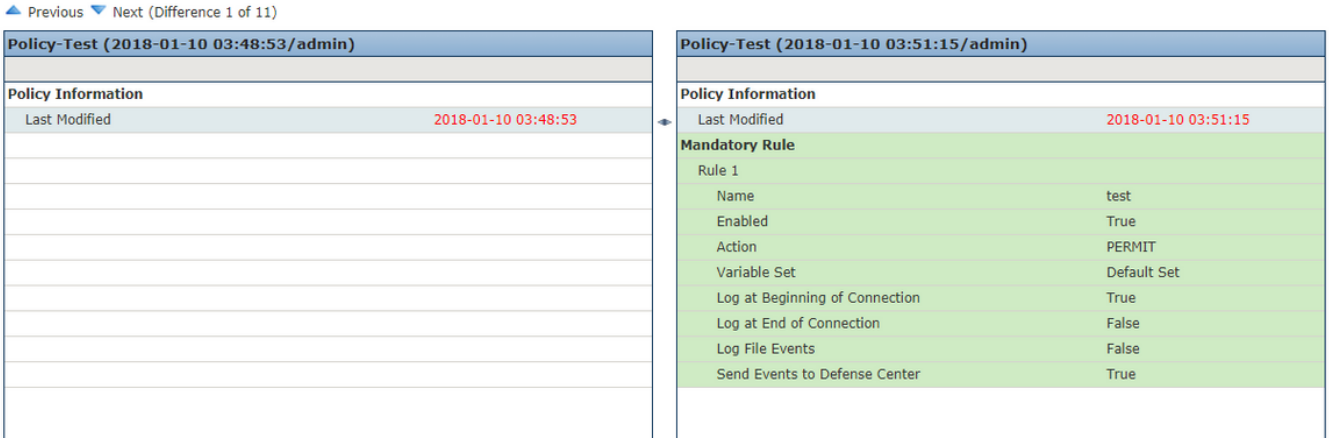
Step 3. Next, save the policy changes.

Step 4. Now, navigate to **System > Monitoring > Audit** and find the log of the change you just made. It appears as shown in this image:



Step 5. You are now able to see a log, as shown in the preceeding image, in it's first line **Save Policy <Policy_name>** along with an icon next to it (highlighted).

Step 6. Click on the icon and it would be redirected to a different page which shows the detailed changes/additions/modifications made to the policy.



Verify

These logs are available to the point audit logs are not pruned.

Troubleshoot

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