Document ID: 117924

Updated: Oct 21, 2015

Contributed by Nazmul Rajib, Cisco TAC Engineer.

Download PDF
Print
Feedback

Related Products

- Cisco FireSIGHT Management Center 750
- Cisco FireSIGHT Management Center 3500
- Cisco FireSIGHT Management Center 1500
- Cisco FirePOWER 7000 Series Appliances
- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center Virtual Appliance
- + Show More

Contents

Introduction
Prerequisites
Requirements
Components Used
Working with the Custom Local Rules
Import Local Rules
View Local Rules
Enable Local Rules
View the Deleted Local Rules
Numbering of the Local Rules
Related Cisco Support Community Discussions

Introduction

A custom local rule on a FireSIGHT System is a custom standard Snort rule that you import in an ASCII text file format from a local machine. A FireSIGHT System allows you to import local rules using the web interface. The steps to import local rules are very straightforward. However, to write an optimal local rule, a user requires in-depth knowledge on Snort and networking protocols.

The purpose of this document is to provide you with some tips and assistance to write a custom local rule. The instructions on creating local rules are available in the *Snort Users Manual,* which is available at snort.org. Cisco recommends that you download and read the Users Manual before you write a custom local rule.

> **Note**: The rules provided in a Sourcefire Rule Update (SRU) package are created and tested by the Cisco Talos Security Intelligence and Research Group, and supported by the Cisco

Technical Assistance Center (TAC). The Cisco TAC does not provide assistance on writing or tuning a custom local rule, however if you experience any issues with the rule import functionality of your FireSIGHT System, please contact the Cisco TAC.

Warning: A poorly written custom local rule can impact the performance of a FireSIGHT System which can lead to performance degradation of the entire network. If you are experiencing any performance issues in your network, and there are some custom local Snort rules enabled on your FireSIGHT System, Cisco recommends you to disable those local rules.

Prerequisites

Requirements

Cisco recommends that you have knowledge on Snort rules and the FireSIGHT System.

Components Used

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

- The FireSIGHT Management Center (also known as Defense Center)
- Software Version 5.2 or later

Working with the Custom Local Rules

Import Local Rules

Before you begin, you must make sure that the rules in the file do not contain any escape characters. The rule importer requires all custom rules to be imported using ASCII or UTF-8 encoding.

The following procedure explains how to import local standard text rules from a local machine:

1. Access the **Rule Editor** page by navigating to **Policies > Intrusion > Rule Editor**.

2. Click **Import Rules**. The **Rule Updates** page appears.

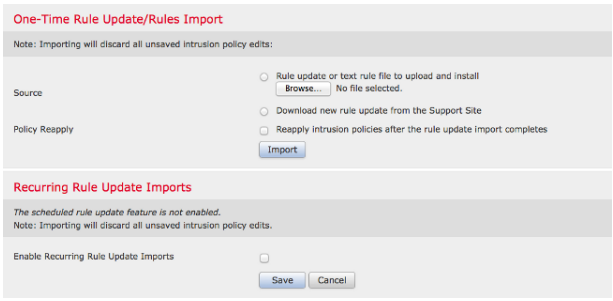


Figure: A screenshot of the Rule Updates page

3. Select **Rule update or text rule file to upload and install** and click **Browse** to select the rule file.

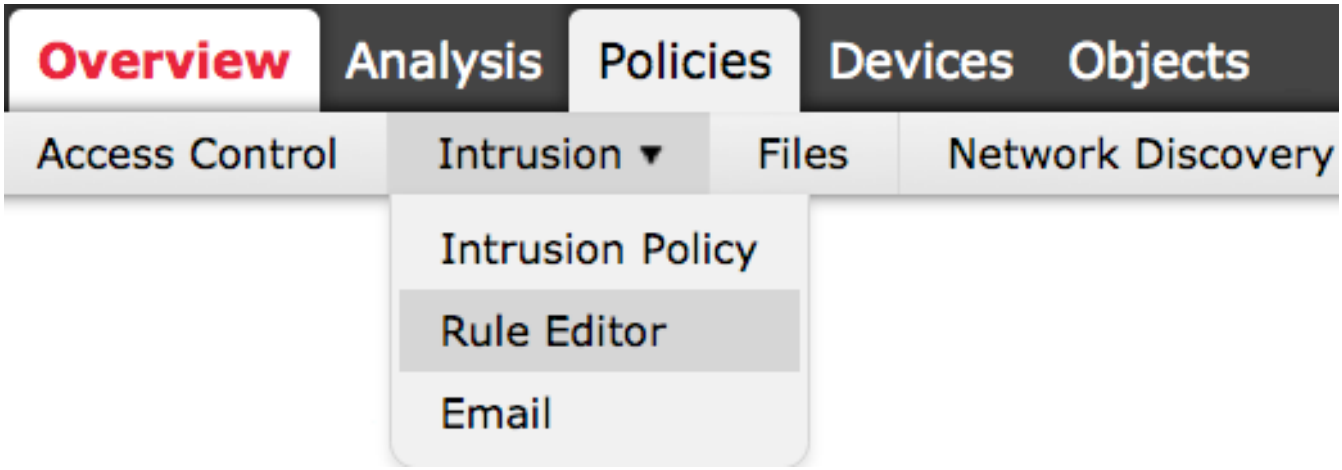
> **Note**: All uploaded rules are saved in the **local rule** category.

4. Click **Import**. The rule file is imported.

> **Caution**: The FireSIGHT Systems do not use the new rule set for inspection. To activate a local rule, you need to enable it in the Intrusion Policy, and then apply the policy.

View Local Rules

- To view the revision number for a current local rule, navigate to the **Rule Editor** page (**Policies** > **Intrusion** > **Rule Editor**).



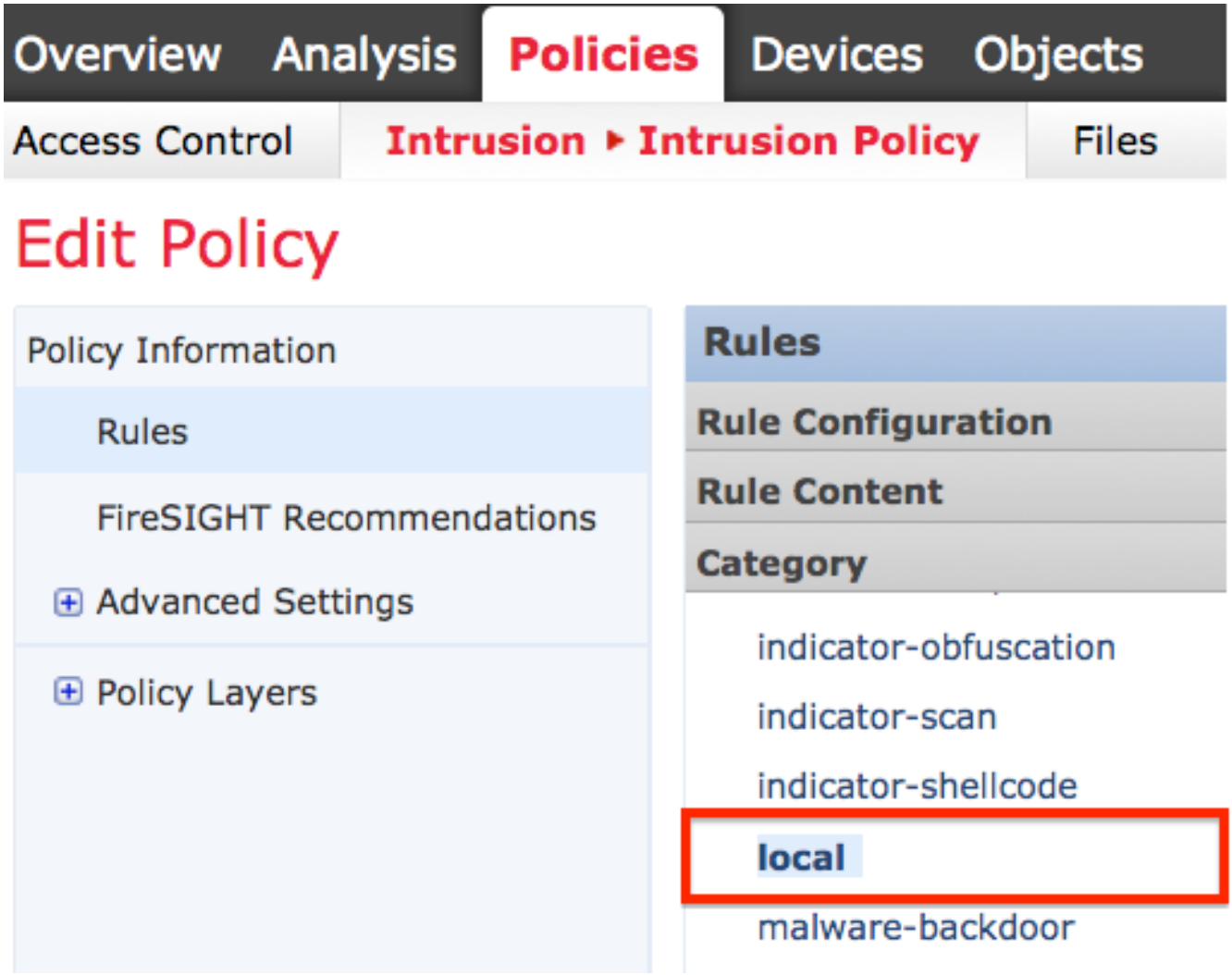
- In the Rule Editor page, click on the **Local Rule** category to expand the folder, then click **Edit** next to the rule.
- All imported local rules are automatically saved in the **local rule** category.

Enable Local Rules

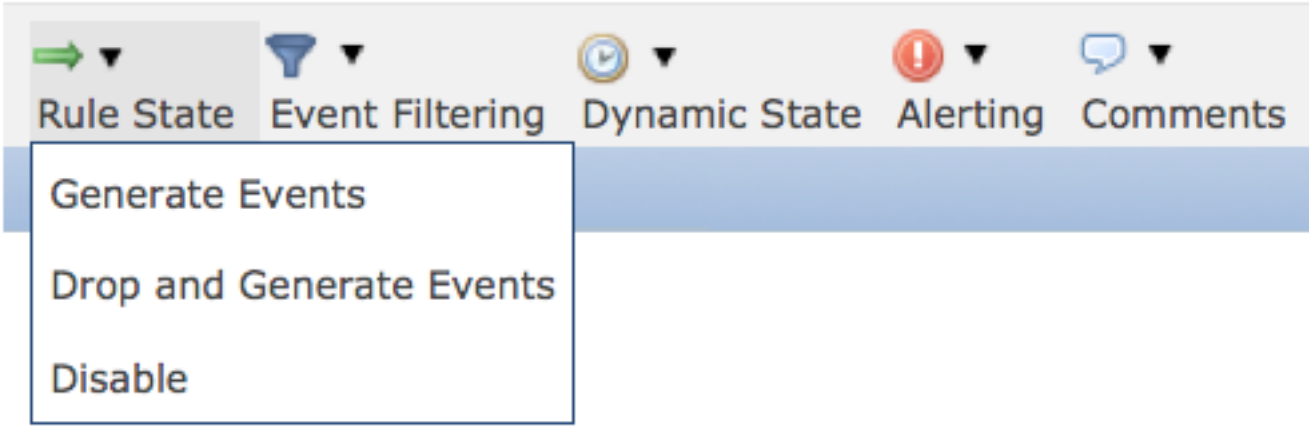
- By default, the FireSIGHT System sets the local rules in a disabled state. You must manually

set the state of local rules before you can use them in your intrusion policy.

- In order to enable a local rule, navigate to Policy Editor page (**Policies** > **Intrusion** > **Intrusion Policy**). Select **Rules** in the left panel. Under the **Category**, select **local**. All of the local rules should appear, if available.



- After selecting the desired local rules, select a state for the rules.



- Once the rule state is selected, click on the **Policy Information** option on the left panel. Select the **Commit Changes** button. The Intrusion Policy is validated.

  Note: The policy validation fails if you enable an imported local rule that uses the deprecated threshold keyword in combination with the intrusion event thresholding feature in an intrusion

policy.

View the Deleted Local Rules

- All deleted local rules are moved from the local rule category to the deleted rule category.
- To view the revision number of a deleted local rule, go to the **Rule Editor** page, click on the **deleted** category to expand the folder, then click the *pencil* icon to view the detail of the rule in the **Rule Editor** page.

Numbering of the Local Rules

- You do not have to specify a Generator (GID); if you do, you can specify only GID 1 for a standard text rule or 138 for a sensitive data rule.
- Do not specify a Snort ID (SID) or revision number when importing a rule for the first time; this avoids collisions with SIDs of other rules, including deleted rules.
- The FireSIGHT Management Center automatically assigns the next available custom rule SID of 1000000 or greater, and a revision number of 1.
- If you attempt to import an intrusion rule with a SID greater than 2147483647, a validation error will occur.
- You must include the SID assigned by IPS and a revision number greater than the current revision number when importing an updated version of a local rule that you have previously imported.
- You can reinstate a local rule that you have deleted by importing the rule using the SID assigned by IPS and a revision number greater than the current revision number. Note that the FireSIGHT Management Center automatically increments the revision number when you delete a local rule; this is a device that allows you to reinstate local rules.

Was this document helpful? Yes No

Thank you for your feedback.

Open a Support Case (Requires a Cisco Service Contract.)

Related Cisco Support Community Discussions

The Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers.

Refer to Cisco Technical Tips Conventions for information on conventions used in this document.