Document ID: 118481

Updated: Sep 17, 2015

Contributed by Nazmul Rajib, Cisco TAC Engineer.

Download PDF
Print
Feedback

Related Products

- Cisco FirePOWER 7000 Series Appliances
- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center Virtual Appliance

Contents

Introduction
1-Second Performance Monitor
Enable On Version 5.4 or Later
Enable On Versions Prior to 5.4
Related Documents
Related Cisco Support Community Discussions

Introduction

On an appliance running Sourcefire software, you can configure the basic parameters that monitor and report on its own performance. The performance statistic is critical to troubleshoot performance related issues on an appliance running Snort. This document provides the steps to enable this feature using a FireSIGHT Management Center.

> **Warning**: If your network is live and you enable 1-Second Performance on a production system, it can impact network performance. You should enable this only if this is requested by Cisco Technical Support for troubleshooting purpose.

> **Note**: 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.

1-Second Performance Monitor

The *1-Second Performance Monitor* feature allows you to specify the intervals at which the system updates performance statistics on your devices by configuring the following:

- Number of seconds
- Number of packets analyzed

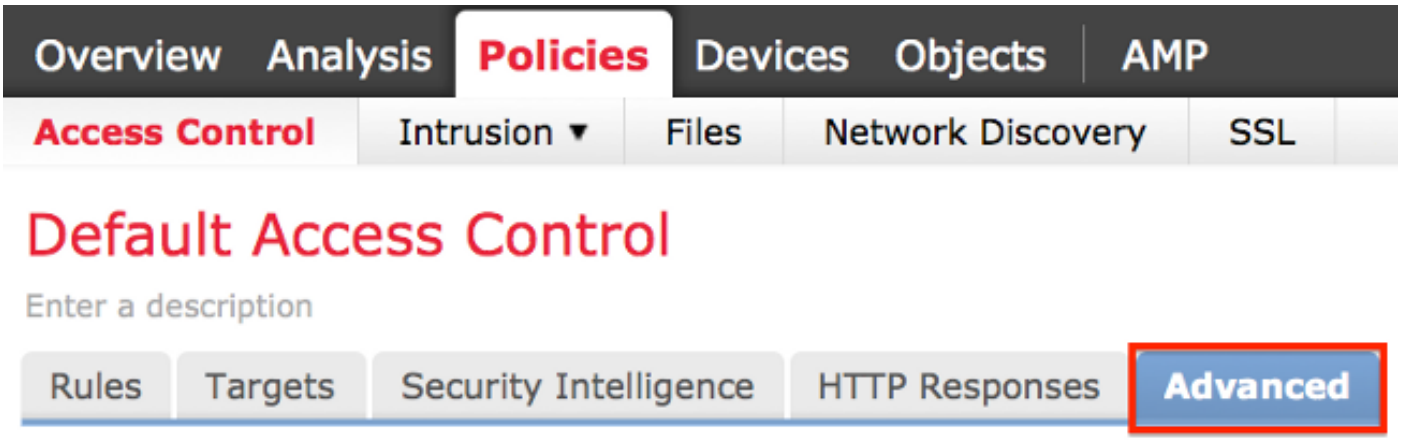
When the number of seconds specified has elapsed since the last performance statistics update, the system verifies that the specified number of packets has been analyzed. If so, the system updates performance statistics. If not, the system waits until the specified number of packets has been analyzed.

Enable On Version 5.4 or Later

Step 1: Select **Policies > Access Control**. The Access Control Policy page appears.

Step 2: Click the *pencil* icon next to the access control policy you want to edit.

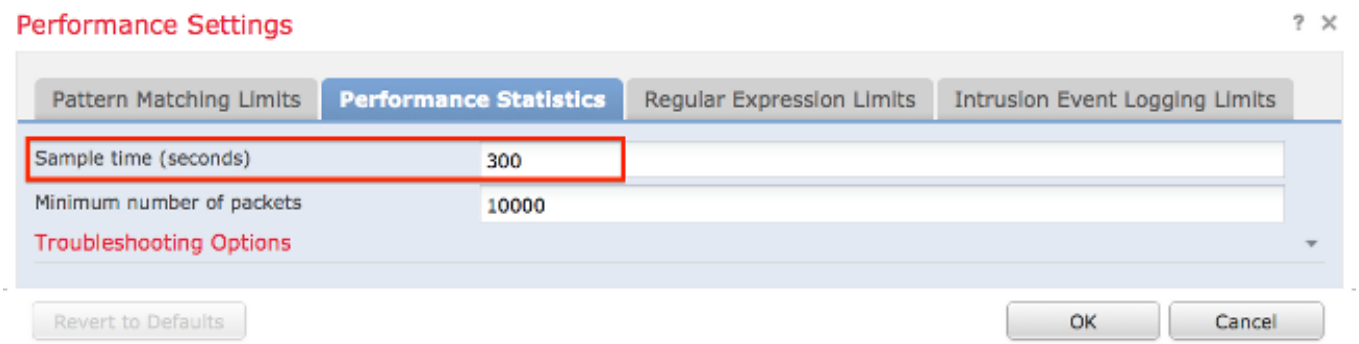
Step 3: Select the **Advanced** tab. The access control policy advanced settings page appears.



Step 4: Click the *pencil* icon next to **Performance Settings**.



Step 5: Select the **Performance Statistics** tab in the pop-up window that appears. Modify the Sample time or Minimum number of packets as described above.



Step 6: *Optionally*, expand the **Troubleshoot Options** section and modify those options only if asked to do so by Cisco TAC.

Step 7: Click OK.

Step 8: You must save and apply the access control policy for your changes to take effect.

Enable On Versions Prior to 5.4

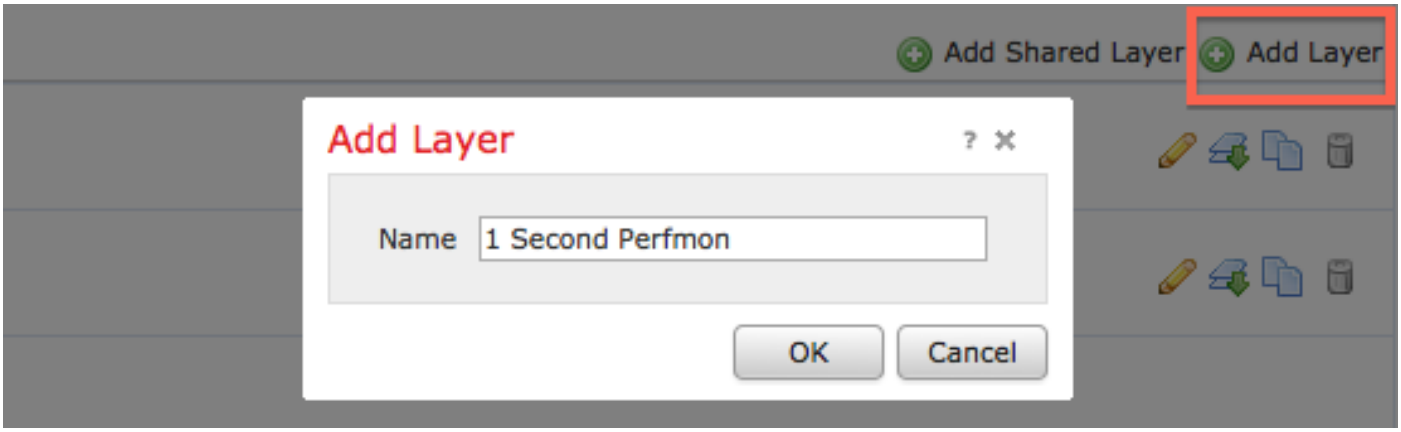
Step 1: Navigate to the Intrusion Policy page. Login to your FireSIGHT Management Center. Navigate to **Policies > Intrusion > Intrusion Policy.**

Step 2: Edit the intrusion policy that you want to apply. Click the *pencil* icon to edit the policy.

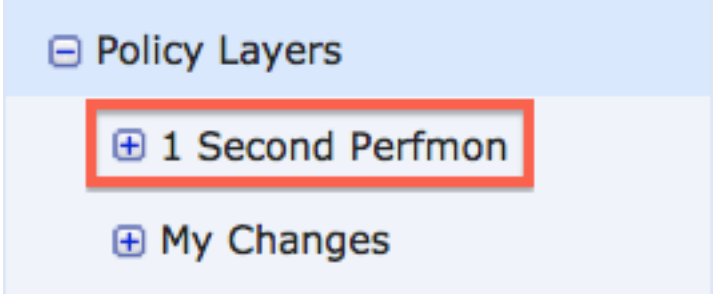


> **Note**: Due to the design of this advanced setting, you must only modify this configuration within an Intrusion Policy that is being used as the Default Action of your Access Control Policy.

Step 3: Add a policy layer. Click **Policy Layers** and then **Add Layer**. Name the layer "*1 Second Perfmon*".

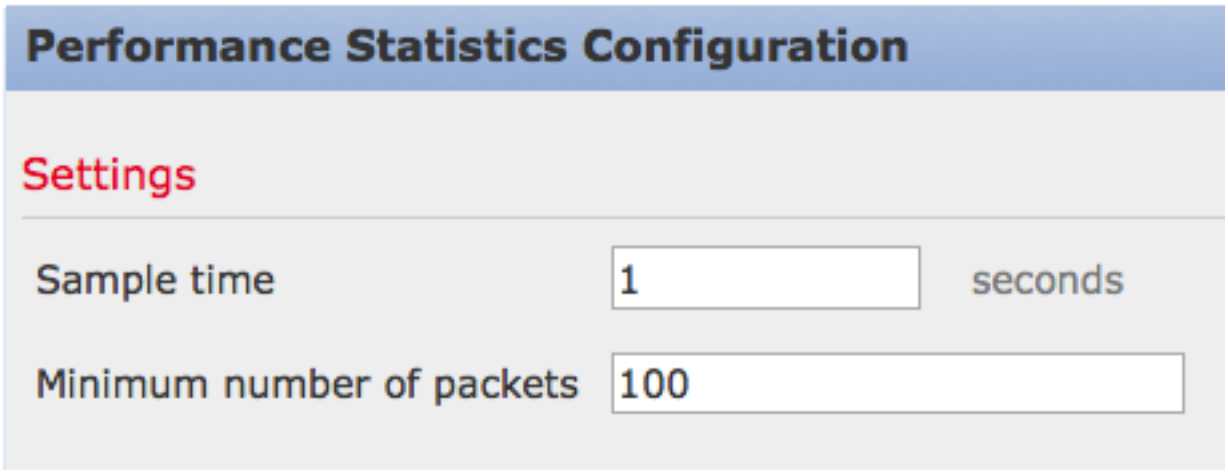


Check the **Policy Layers** in the left panel, and make sure that the new layer "*1 Second Perfmon*" is above all other layers.

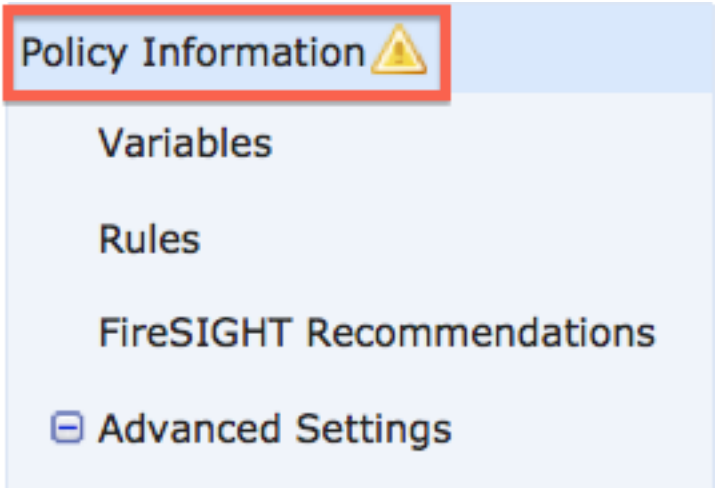


Step 4: Enable the performance statistics configuration. Under **Performance Settings**, select the radio button **Enabled** next to the **Performance Statistics Configuration**, and click **Edit**.

Step 5: Modify the default sample time to 1 second, and the minimum number of packets to 100 packets.



Step 6: Click on **Policy Information** in the left panel, commit the changes, and apply the updated policy to the devices you would like to profile.



Step 7: Revert the settings after collecting the data. In order to revert, simply delete the "*1 Second Perfmon*" policy layer.

> **Caution**: Do not forget to revert the configuration. Otherwise, it may cause performance issue.

Related Documents

- Viewing Intrusion Event Performance
- Generating Intrusion Event Performance Statistics Graphs

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.