Configure a FireSIGHT System to Send Alerts to an External Syslog Server

Document ID: 118464

Contributed by Nazmul Rajib and Keith Forbus, Cisco TAC Engineers.
Sep 17, 2014

Contents

Introduction

While a FireSIGHT System provides various views of events within it's web interface, you may want to configure external event notification to facilitate constant monitoring of critical systems. You can configure a FireSIGHT System to generate alerts that notify you via email, SNMP trap, or syslog when one of the following is generated. This article describes how to configure a FireSIGHT Management Center to send alerts on an external Syslog server.

Prerequisites

Requirements

Cisco recommends that you have knowledge on Syslog and FireSIGHT Management Center. Also, the syslog port (default is 514) must be allowed in your firewall.

Components Used

The information in this document is based on Software Version 5.2 or later.

Caution: The information on this document is created from an appliance in a specific lab environment, and started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Sending Intrusion Alerts

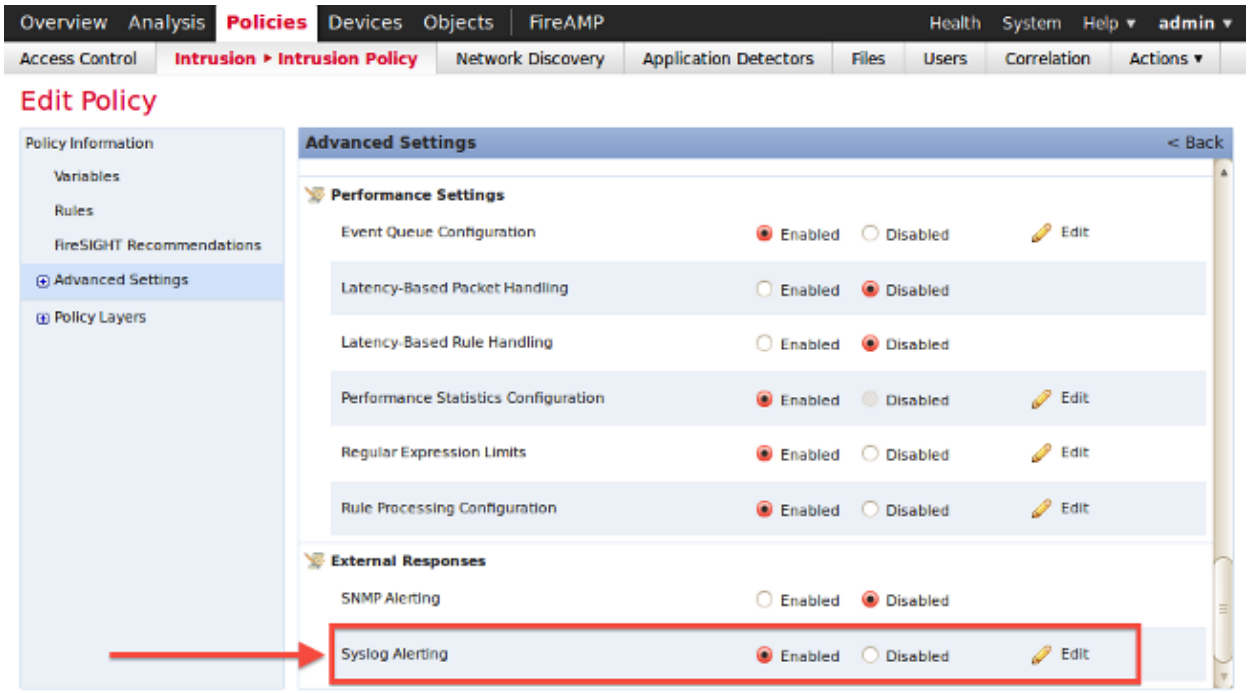
1. Log into the web user interface of your FireSIGHT Management Center.

2. Navigate to ***Policies*** > ***Intrusion*** > ***Intrusion Policy***.

3. Click ***Edit*** next to the policy you want to apply.

4. Click on ***Advanced Settings***.

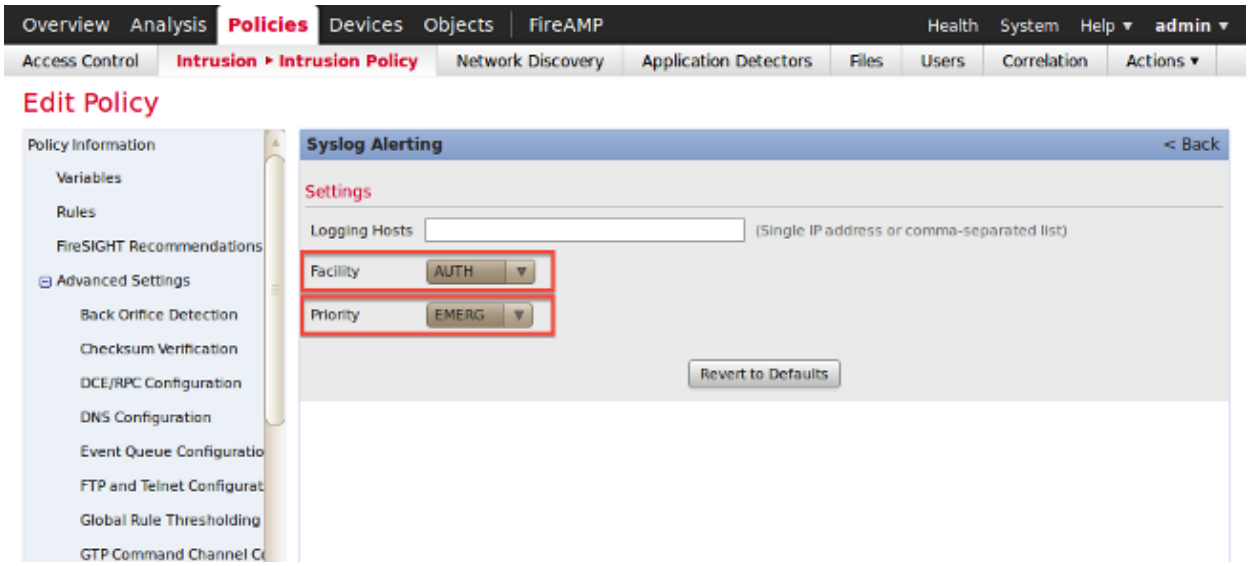
5. Locate ***Syslog Alerting*** in the list and set it to ***Enabled***.



6. Click ***Edit*** next to the right of ***Syslog Alerting***.

7. Type the IP address of your syslog server on the ***Logging Hosts*** field.

8. Choose an appropriate ***Facility*** and ***Severity*** from the drop−down menu. These can be left at the default values unless a syslog server is configured to accept alerts for a certain facility or severity.



9. Click on ***Policy Information*** near the top left of this screen.

10. Click the ***Commit Changes*** button.

11. Reapply your intrusion policy.

Note: In order for the alerts to be generated, use this intrusion policy in the Access Control rule. If there is no Access Control rule configured, then set this intrusion policy to be used as the default action of the Access Control policy, and reapply the Access Control policy.

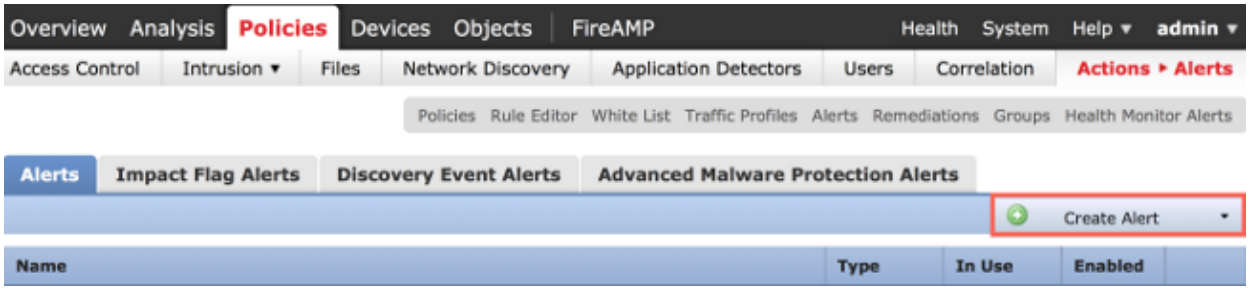
Now if an intrusion event is triggered on that policy, an alert will also be sent to the syslog server that is configured on the intrusion policy.

Sending Health Alerts

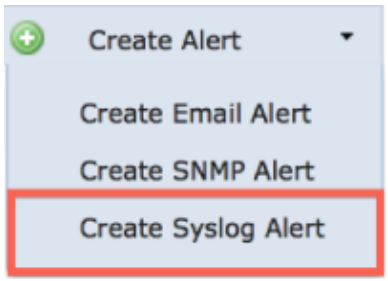
Part 1: Create a Syslog Alert

1. Log into the web user interface of your FireSIGHT Management Center.

2. Navigate to ***Policies*** > ***Actions*** > ***Alerts***.



3. Select ***Create Alert***, which is on the right−hand side of the web interface.



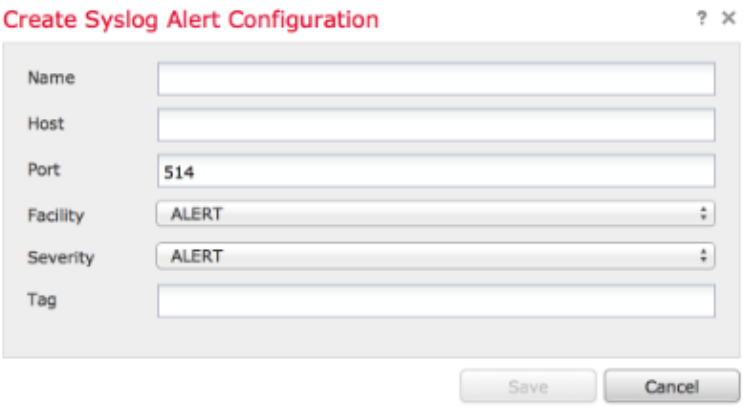
4. Click ***Create Syslog Alert***. A configuration popup window appears.

5. Provide a name for the alert.

6. Fill in the IP address of your syslog server in the ***Host*** field.

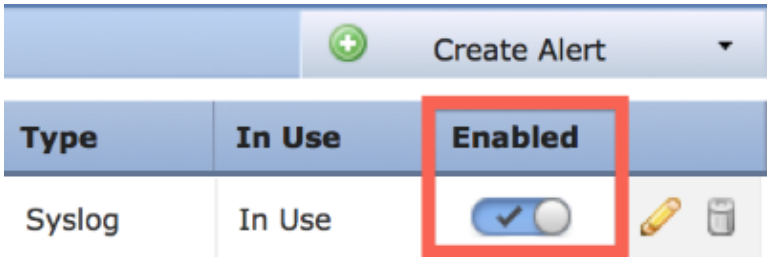
7. Change the port if needed by your syslog server (the default port is 514).

8. Select an appropriate ***Facility*** and ***Severity***.



9. Click the ***Save*** button. You will return to the ***Policies*** > ***Actions*** > ***Alerts*** page.

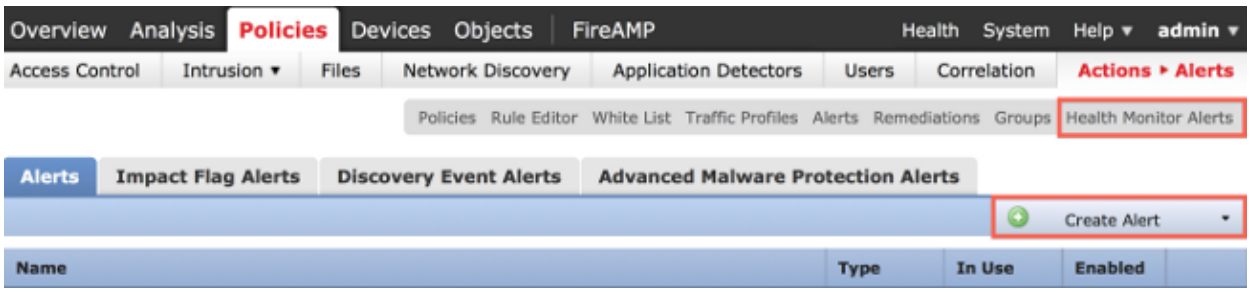
10. Enable the Syslog configuration.



Part 2: Create Health Monitor Alerts

The following instruction describes the steps to configure ***Health Monitor Alerts*** that uses the syslog alert that you have just created (in the previous section):

1. Go to ***Policies*** > ***Actions*** > ***Alerts*** page, and choose ***Health Monitor Alerts***, which is near the top of the page.



2. Give the health alert a name.

3. Choose a ***Severity*** (holding down the CTRL key while clicking can be used to select more than one severity type).

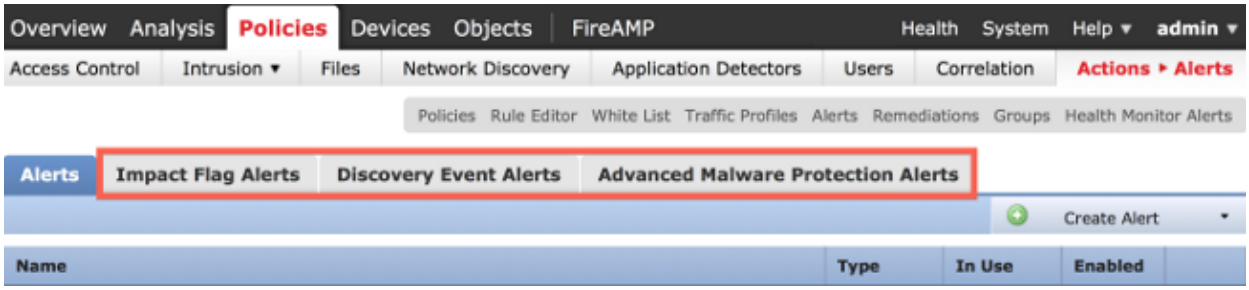
4. From the ***Module*** columnm choose the health modules for which you would like to send alerts to the syslog server (For example, Disk Usage).

5. Select previously created syslog alert from the ***Alerts*** column.

6. Click the ***Save*** button.

Sending Impact Flag, Discover Event and Malware Alerts

You can also configure a FireSIGHT Management Center to send syslog alerts for events with a specific impact flag, specific type of discovery events and malware events. In order to do that, you have to Part 1: Create a Syslog Alert and then configure the type of events that you want to send to your syslog server. You can do that by navigating to the ***Policies*** **>** ***Actions*** **>** ***Alerts*** page, and then selecting a tab for the desired alert type.



Updated: Sep 17, 2014 Document ID: 118464