配置FireSIGHT系统发送警报到外部系统日志服务器

目录

简介

当FireSIGHT系统在它里面时提供事件多种视图是Web接口，您可能要配置外部事件通知实现关键系统不变监听。您能配置FireSIGHT系统生成通过电子邮件、SNMP陷阱或者Syslog通知您的警报，当之一以下生成时。此条款描述如何配置FireSIGHT管理中心发送在外部系统日志服务器的警报。

先决条件

要求

思科建议您有在Syslog和FireSIGHT管理中心的知识。并且，在您的防火墙必须允许系统日志端口(默认是514)。

使用的组件

本文档中的信息根据软件版本5.2或以上。

> **Caution**:关于本文的信息从在特定实验室环境的一个设备创建，并且开始与原始。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

发送入侵警报

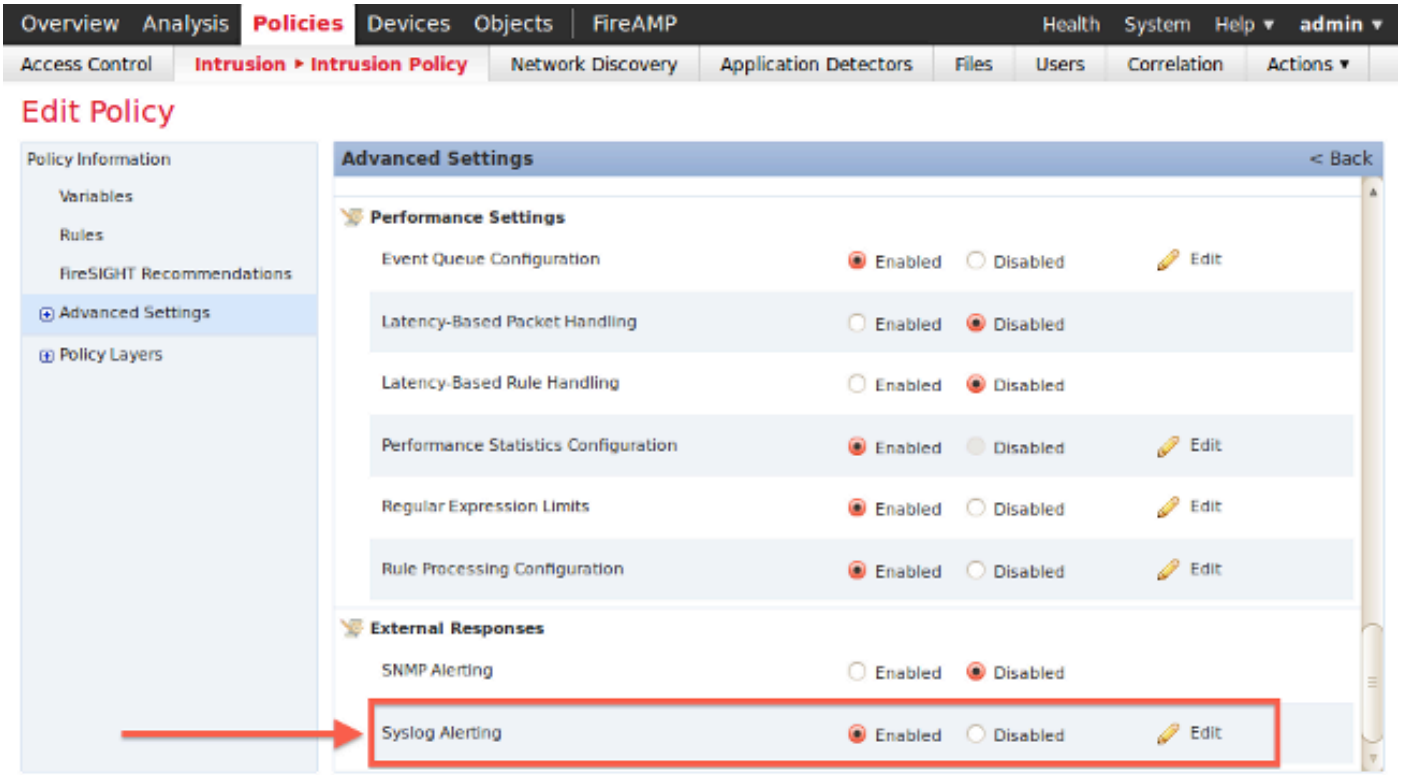
1. 登录您的FireSIGHT管理中心网页用户界面。

2. 导航对**策略>入侵>入侵策略**。

3. 单击在您要运用的策略旁边**编辑**。

4. 点击**提前的设置**。

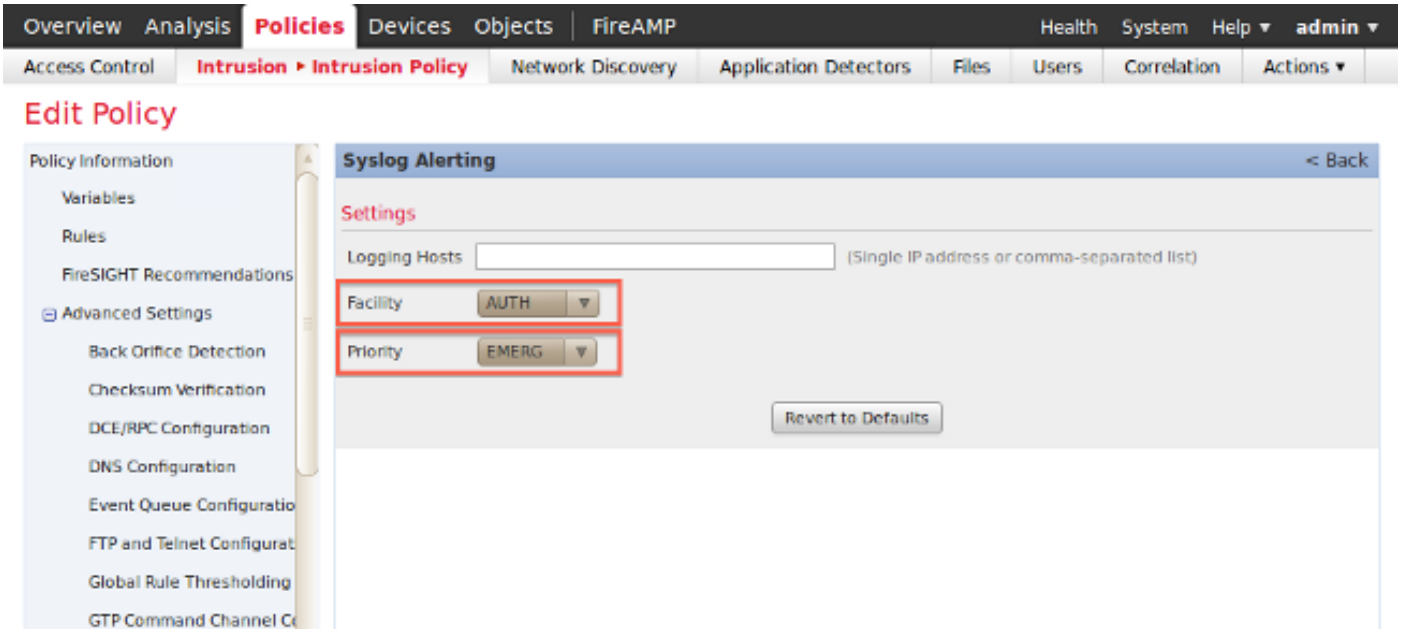
5. 找出**警告**在列表的**Syslog**并且设置它对**已启用**。



6. 单击在权利**Syslog警告旁边编辑**。

7. 键入您的在**日志主机**领域的系统日志服务器的IP地址。

8. 从下拉菜单选择一适当的**设备**和**严重性**。 除非系统日志服务器配置接受有些设备或严重性的，警报这些可以被留下在默认值。



9. 在此屏幕附近左上点击**策略信息**。

10. 点击**进行更改**按钮。

11. 重新应用您的入侵策略。

> **Note**:为了能将生成的警报，请使用此入侵策略在访问控制规则。 如果没有配置的访问控制规则，则集作为访问控制策略的默认操作将使用的此入侵策略，和重新应用访问控制策略。

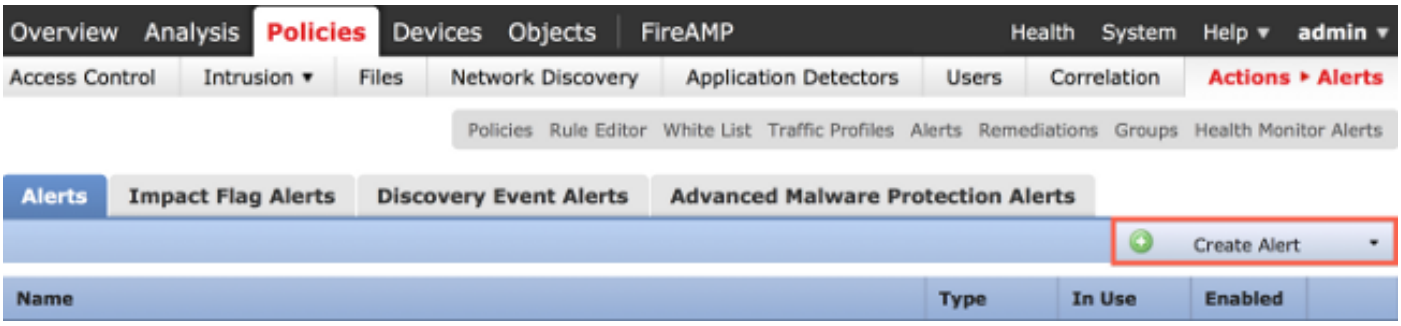
现在，如果入侵事件在该策略被触发，警报也将被发送到在入侵策略配置的系统日志服务器。

发送健康警报

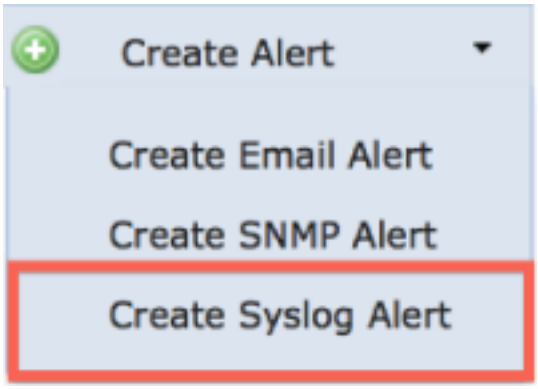
第1部分： 创建Syslog警报

1. 登录您的FireSIGHT管理中心网页用户界面。

2. 导航对**策略>操作>警报**。



3. 选择**创建警报**，在Web接口的右边。



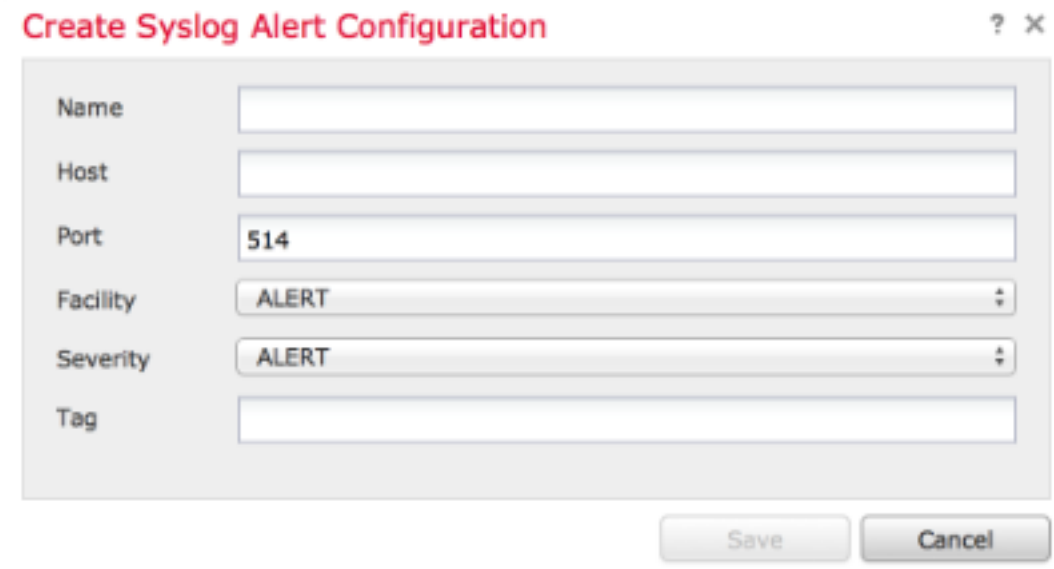
4. 单击**创建Syslog警报**。配置弹出窗口出现。

5. 为警报提供一名称。

6. 在**Host Field**填写您的系统日志服务器的IP地址。

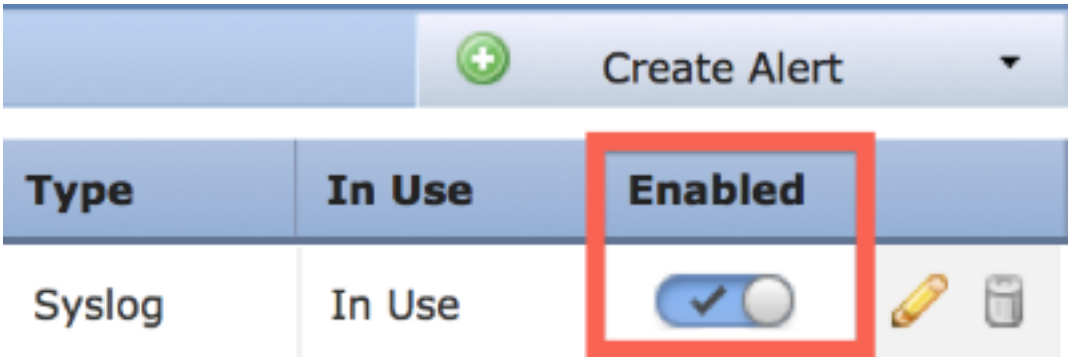
7. 由您的系统日志服务器若需要更换端口(默认端口是514)。

8. 选择一适当的**设备**和**严重性**。



9. 点击**保存按钮**。您将回到**策略>操作>警报**页。

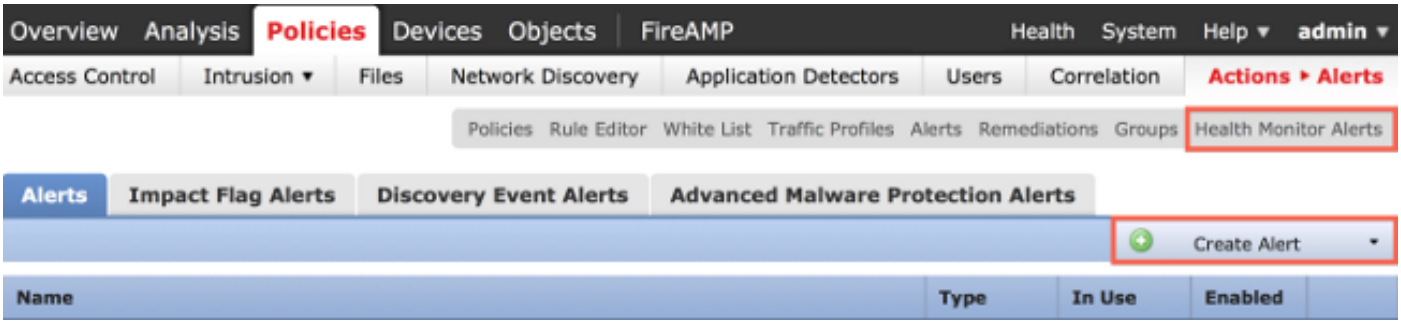
10. 启用Syslog配置。



第 2 部分： 创建健康监控警报

以下说明描述步骤配置使用Syslog警报您创建的**健康监控警报**(在前面部分) ：

1. 去**策略>操作>警报**页，并且选择**健康监控警报**，在页的顶部附近。



2. 给予健康警报名称。

3. 选择**严重性**(持续CTRL密钥，当单击可以用于选择超过一个严重性类型)时。

4. 从**模块**columnm请选择您希望发送警报到系统日志服务器的健康模块例如(磁盘使用情况)。

5. 选择以前从**警报**列的已创建Syslog警报。

6. 点击**保存按钮**。

发送影响标志，请发现事件和恶意软件警报

您能也配置FireSIGHT管理中心发送事件的Syslog警报用一特定影响标志，发现事件和恶意软件事件的特定类型。为了执行那，您必须第1部分：创建Syslog警报然后配置您希望发送到您的系统日志服务器事件的种类。您能通过导航到**策略>操作>警报**页，然后选择希望的提醒的类型的一选项卡执行那。