配置一个FireSIGHT系统发送戒备到一个外部系统日志服务器

Contents

Introduction

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恒定的监控。您能配置FireSIGHT系统生成通过电子邮件、SNMP陷阱或者Syslog通知您的戒备，当之一以下生成时。此条款描述如何配置FireSIGHT管理中心发送在一个外部系统日志服务器的戒备。

Prerequisites

Requirements

Cisco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(默认值是514)。

Components Used

本文的信息根据软件版本5.2或以上。

> **警告**：关于本文的信息从一种工具在特定实验室环境里被创建，并且从原始开始。If your network is live, make sure that you understand the potential impact of any command.

发送闯入戒备

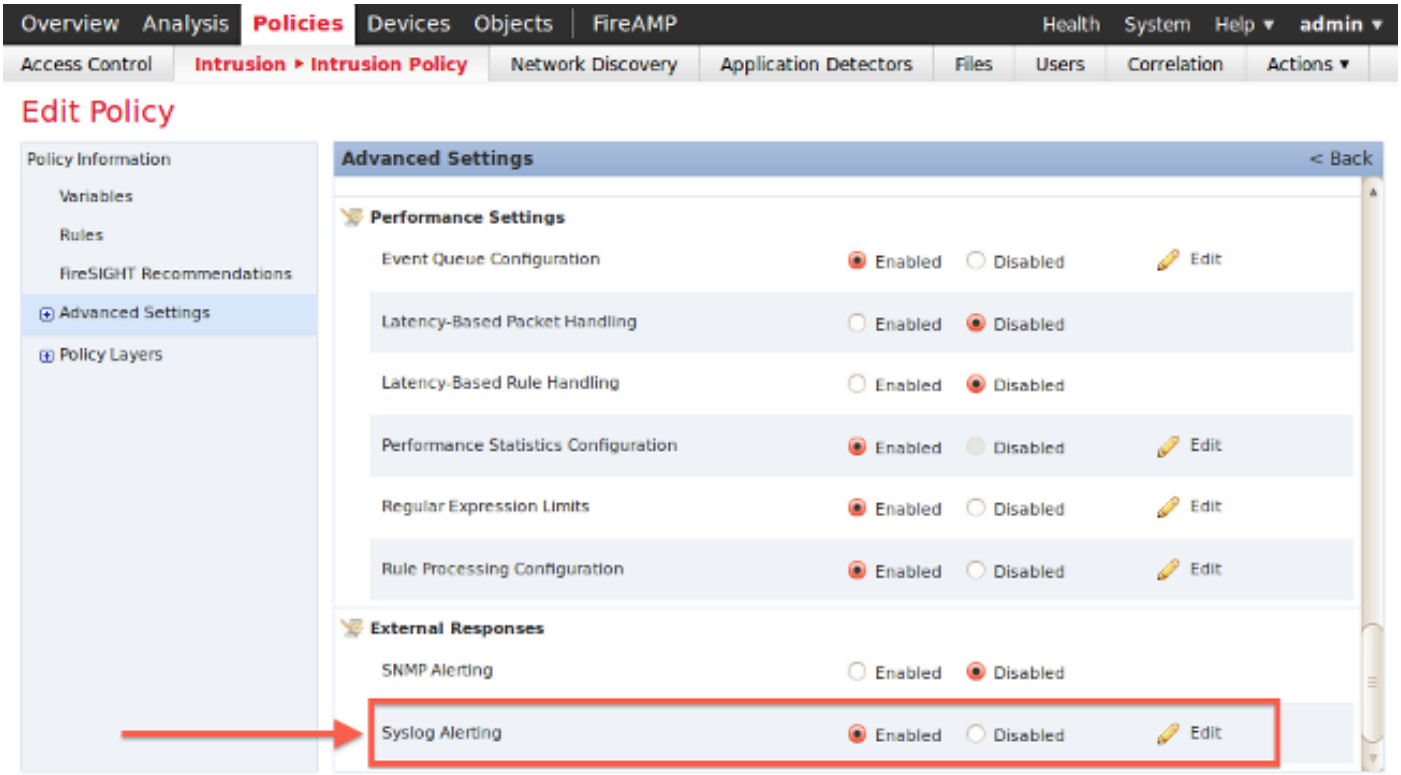
1. 日志到您的FireSIGHT管理中心里网页用户界面。

2. 连接对**策略>闯入>闯入策略**。

3. 点击在您要运用的策略旁边**编辑**。

4. 点击**提前的设置**。

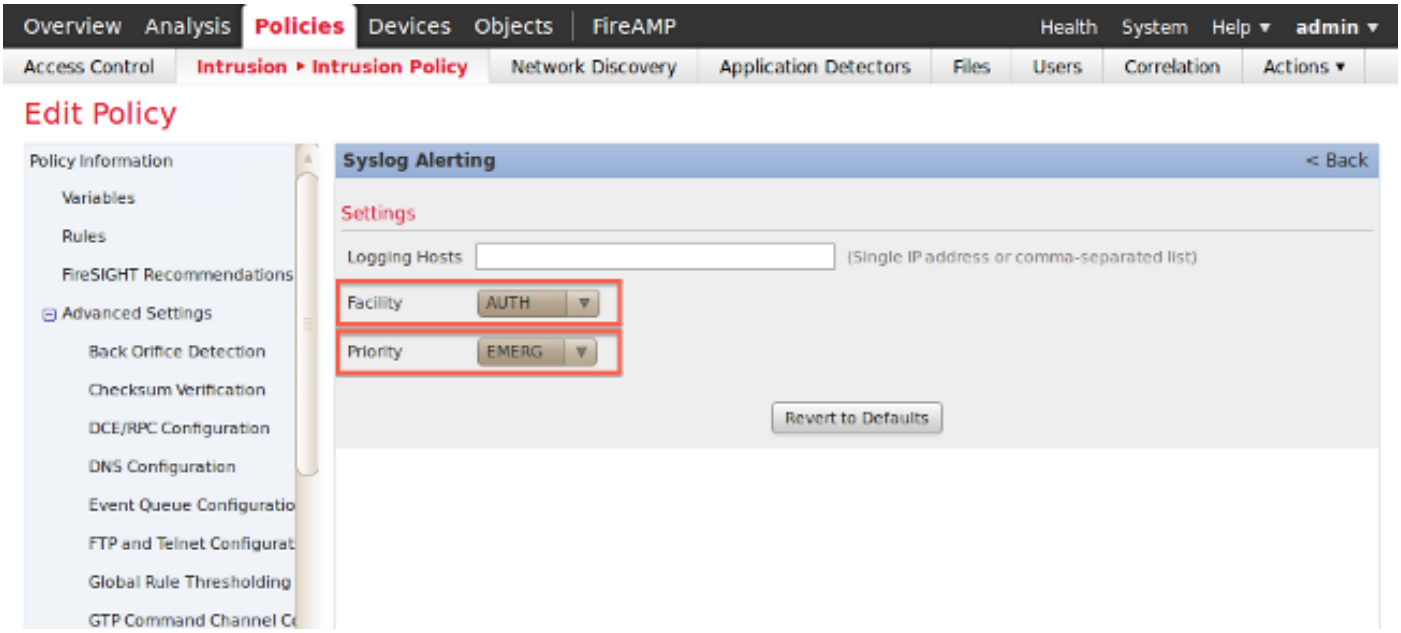
5. 找出**警告的Syslog**列表并且设置它对**启用**。



6. 点击在权利**Syslog警告旁边编辑**。

7. 键入您的在**记录主机**领域的系统日志服务器的IP地址。

8. 从下拉菜单选择适当的**设备**和**严重性**。 除非配置系统日志服务器接受有些设备或严重性的，戒备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. 重新应用您的闯入策略。

> **Note**:为了能将生成的戒备，请使用此闯入策略在访问控制规则。 如果没有被配置的访问控制规则，则请设置作为访问控制策略的默认动作将使用的此闯入策略，并且重新应用访问控制策略。

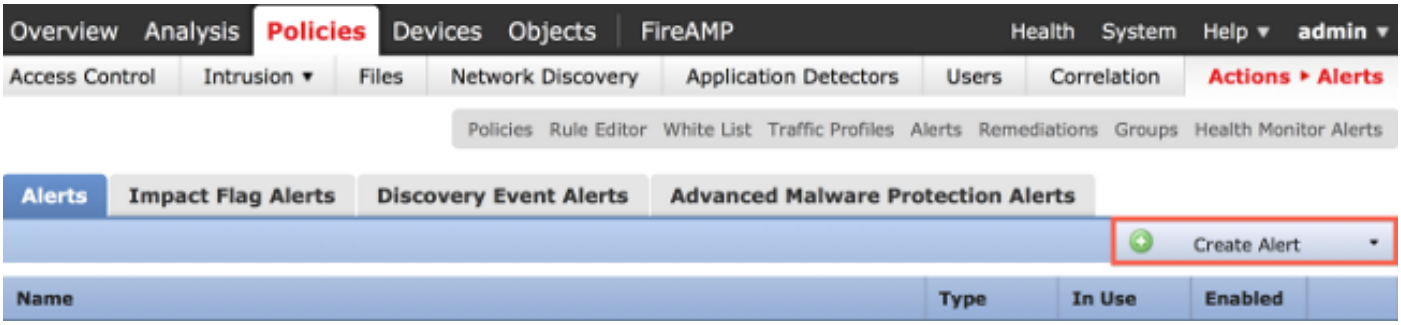
现在，如果闯入事件在该策略被触发，戒备也将被发送到在闯入策略被配置的系统日志服务器。

发送健康戒备

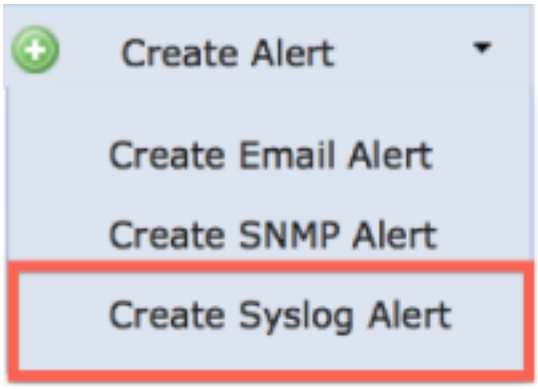
第1部分： 创建一次Syslog戒备

1. 日志到您的FireSIGHT管理中心里网页用户界面。

2. 连接对**策略>动作>戒备**。



3. 选择**创建戒备**，在Web接口的右边。



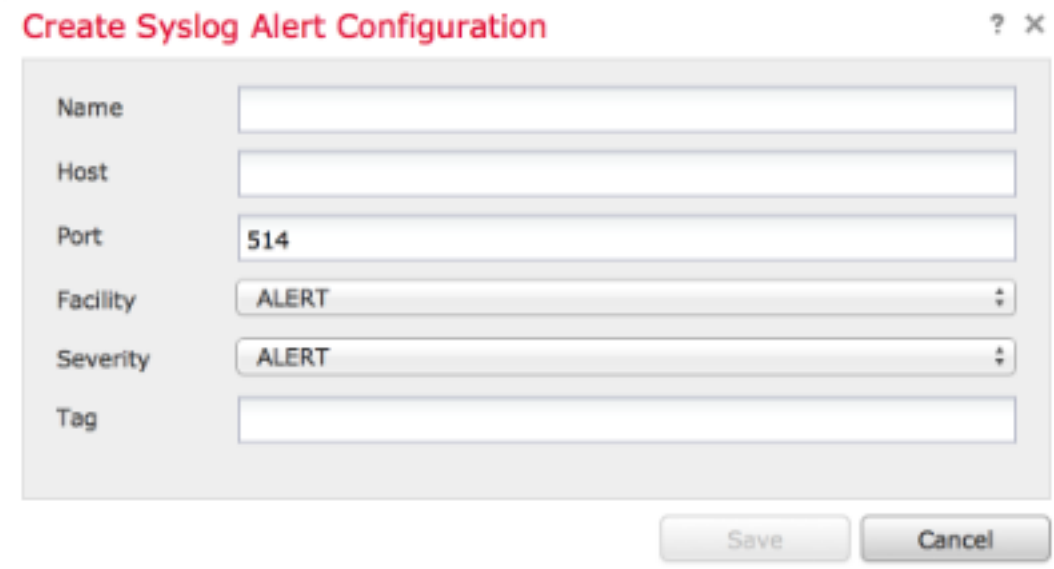
4. 点击**创建Syslog戒备**。配置弹出窗口出现。

5. 为戒备提供一个名字。

6. 填写您的在**主机**领域的系统日志服务器的IP地址。

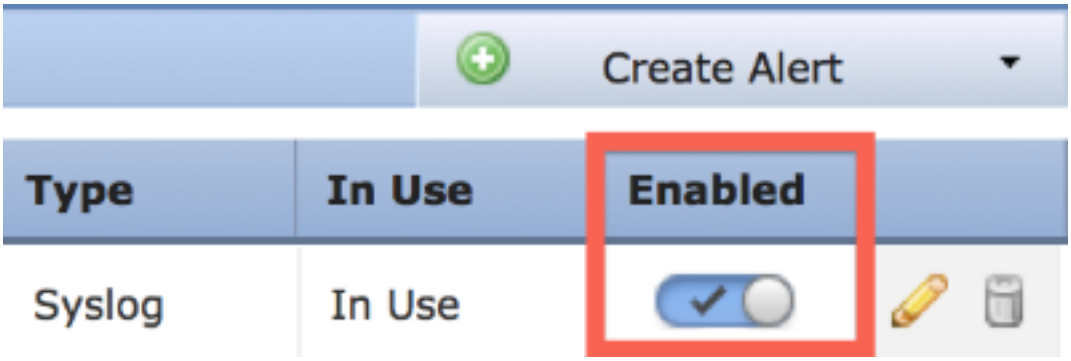
7. 由您的系统日志服务器若需要更改端口(默认端口是514)。

8. 选择适当的**设备**和**严重性**。



9. 点击**保存按钮**。您将回到**策略>动作>戒备**页。

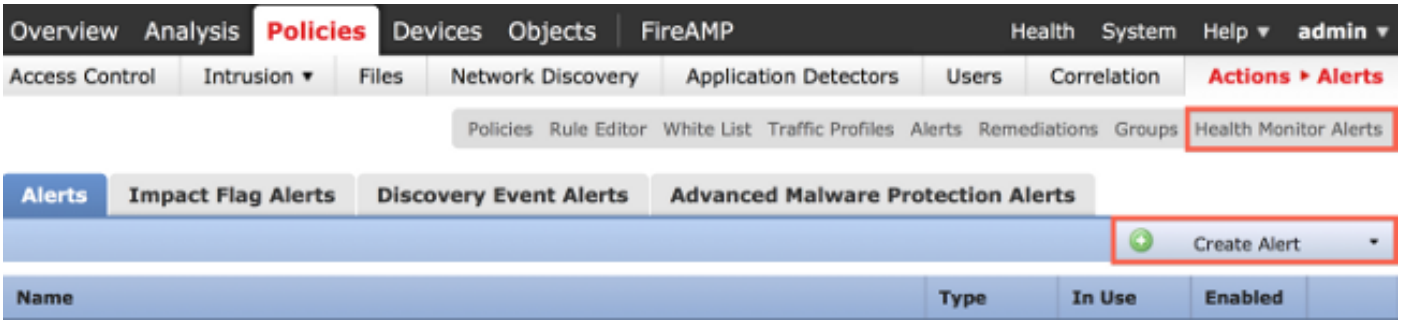
10. Enable (event) Syslog配置。



第2部分： 创建健康监控戒备

以下说明描述步骤配置使用Syslog戒备您创建了的**健康监控戒备**(在前面的部分) ：

1. 去**策略>动作>戒备**页，并且选择**健康监控戒备**，在页的顶层附近。



2. 给予健康戒备一个名字。

3. 选择**严重性**(持续CTRL键，当点击可以用于选择超过一种严重性类型)时。

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

5. 选择以前被创建的Syslog戒备从**戒备**列。

6. 点击**保存按钮**。

发送影响标志位，请发现事件和Malware戒备

您能也配置FireSIGHT管理中心发送事件的Syslog戒备与一个特定影响标志位，发现事件和malware事件的特定类型。为了执行那，您必须第1部分：创建一次Syslog戒备然后配置您要发送到您的系统日志服务器事件的种类。您能通过连接到**策略>动作>戒备**页，然后选择选项执行那期望提醒的类型的。