配置FireSIGHT系统以将警报发送到外部系统日志服务器

目录

简介

虽然FireSIGHT系统在其网络界面内提供各种事件视图，但您可能要配置外部事件通知以促进对关键系统的持续监控。您可以将FireSIGHT系统配置为生成警报，在生成以下内容之一时通过邮件、SNMP陷阱或系统日志通知您。本文介绍如何配置FireSIGHT管理中心以在外部系统日志服务器上发送警报。

先决条件

要求

Cisco建议您了解系统日志和FireSIGHT管理中心的相关知识。此外，防火墙中必须允许系统日志端口（默认值为514）。

使用的组件

本文档中的信息基于软件版本5.2或更高版本。

> **警告：**本文档中的信息是从特定实验环境中的设备创建的，并以清除（默认）配置开头。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

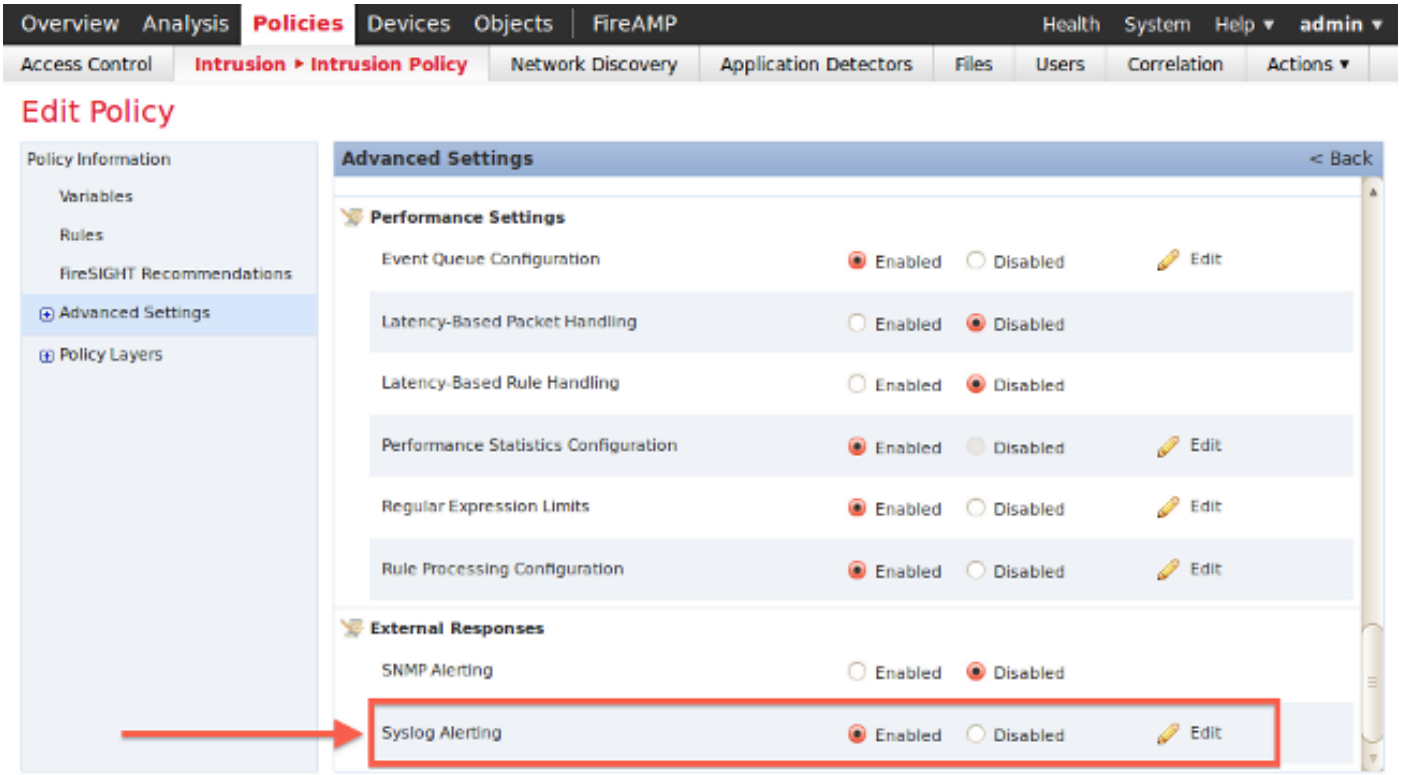
1.登录到FireSIGHT管理中心的Web用户界面。

2.导航到**Policies > Intrusion > Intrusion Policy**。

3.点击要应用的策略旁边的**Edit**。

4.单击**Advanced Settings**。

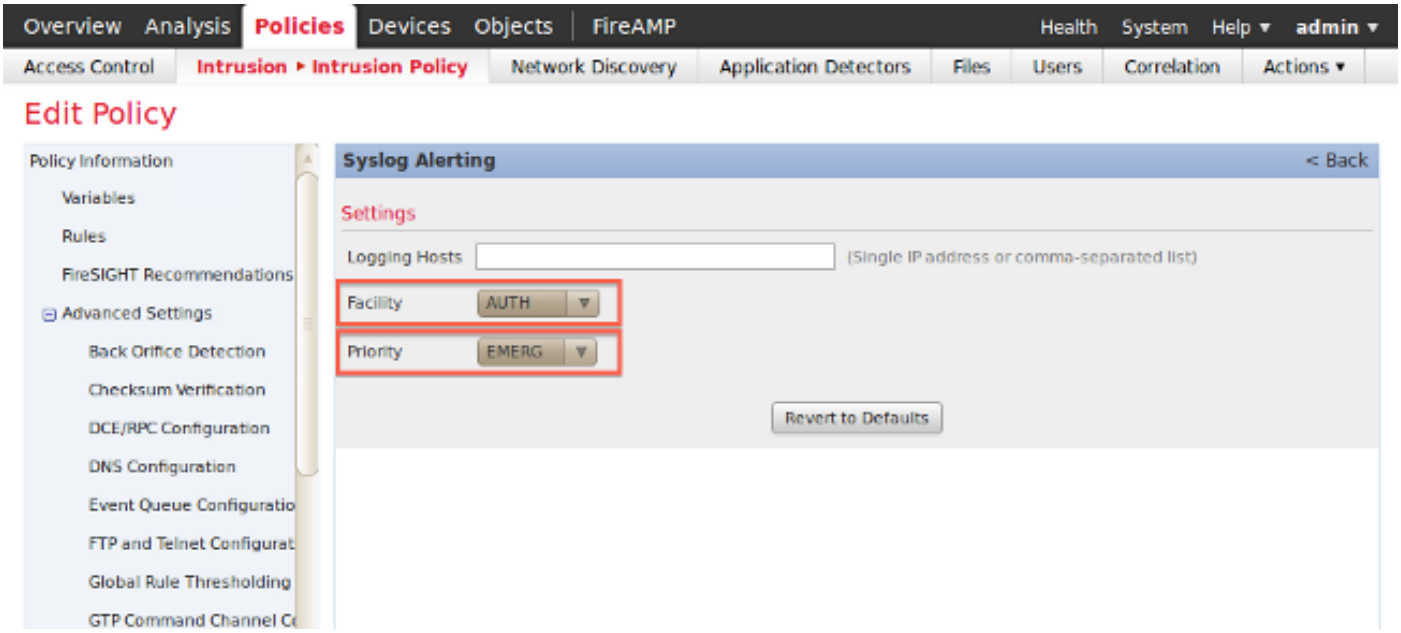
5.在列表中找到**Syslog Alerting**并将其设置为**Enabled**。



6.单击**Syslog Alerting**右侧的**Edit**。

7.在**Logging Hosts**字段中键入系统日志服务器的IP地址。

8.从下拉菜单中选择相应的**Facility**和**Severity**。 这些值可以保留为默认值，除非系统日志服务器配置为接受特定设施或严重性的警报。



9.单击此屏幕左上角附近的**Policy Information**。

10.单击**Commit Changes**按钮。

11.重新应用入侵策略。

> **注意**：为了生成警报，请在访问控制规则中使用此入侵策略。 如果未配置访问控制规则，则将此入侵策略设置为用作访问控制策略的默认操作，并重新应用访问控制策略。

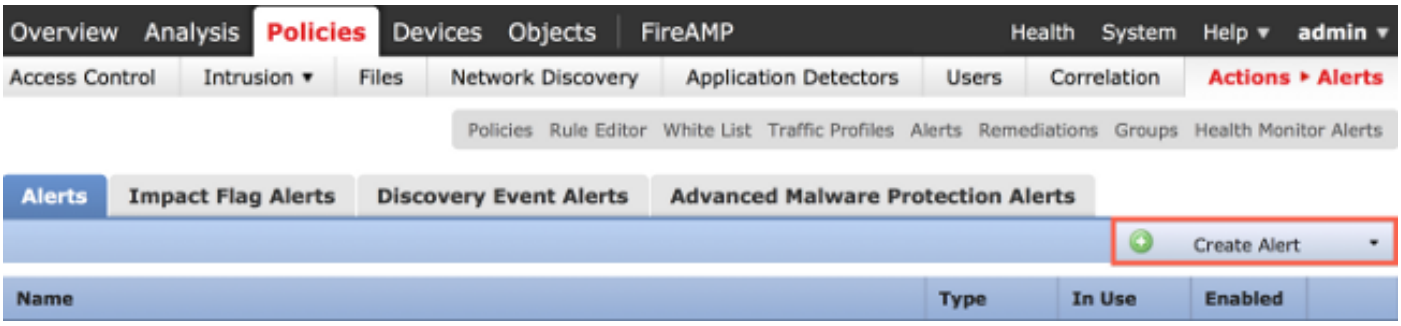
现在，如果在该策略上触发入侵事件，系统还会向在入侵策略上配置的系统日志服务器发送警报。

发送运行状况警报

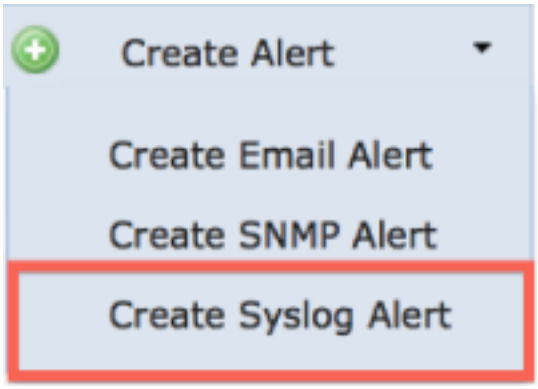
第1部分： 创建系统日志警报

1.登录到FireSIGHT管理中心的Web用户界面。

2.定位至**策略>操作>预警**。



3.选择Web界面右侧的**Create Alert**。



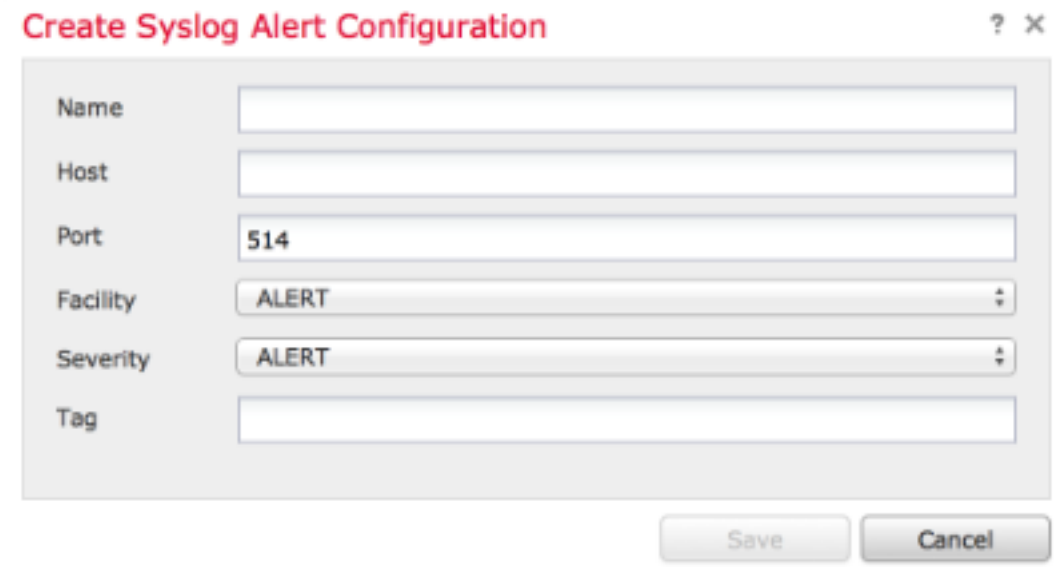
4.单击**Create Syslog Alert**。系统将显示配置弹出窗口。

5.提供预警的名称。

6.在**主机**字段中填写系统日志服务器的IP地址。

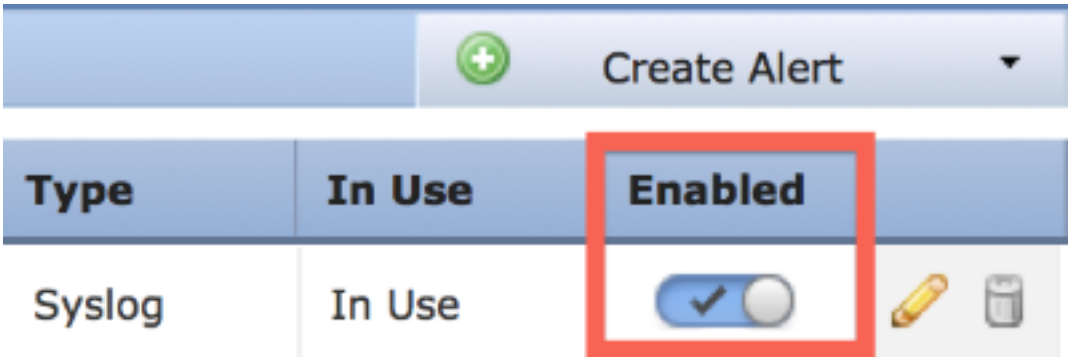
7.如果需要，请更改系统日志服务器的端口（默认端口为514）。

8.选择适当的**设施**和**严重性**。



9.单击**保存**按钮。您将返回**Policies > Actions > Alerts**页。

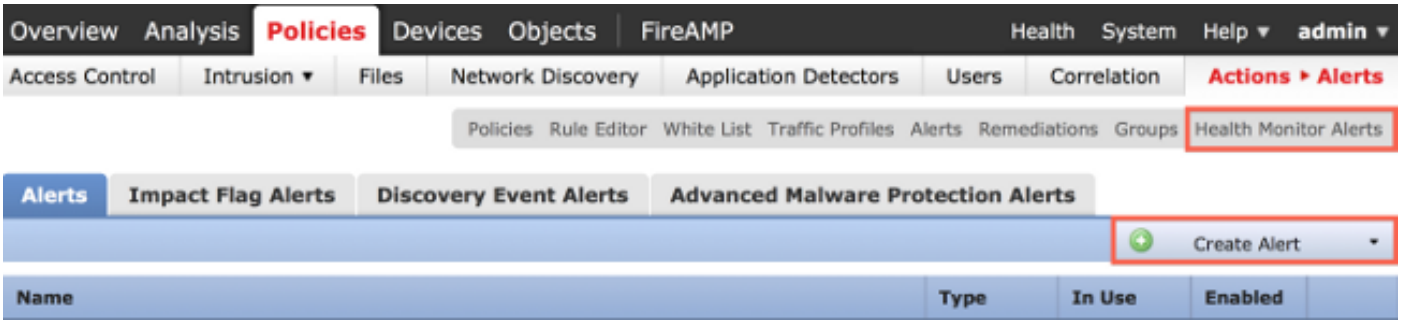
10.启用系统日志配置。



第 2 部分： 创建运行状况监视器警报

以下说明介绍了使用您刚刚创建的syslog警报（在上一节中）配置**运行状况监控警报**的步骤：

1.转到**策略>操作>警报**页，然后选择**运行状况监控器警报**，该页位于页面顶部。



2.为运行状况警报命名。

3.选择**Severity**（按住CTRL键的同时单击可用来选择多个严重性类型）。

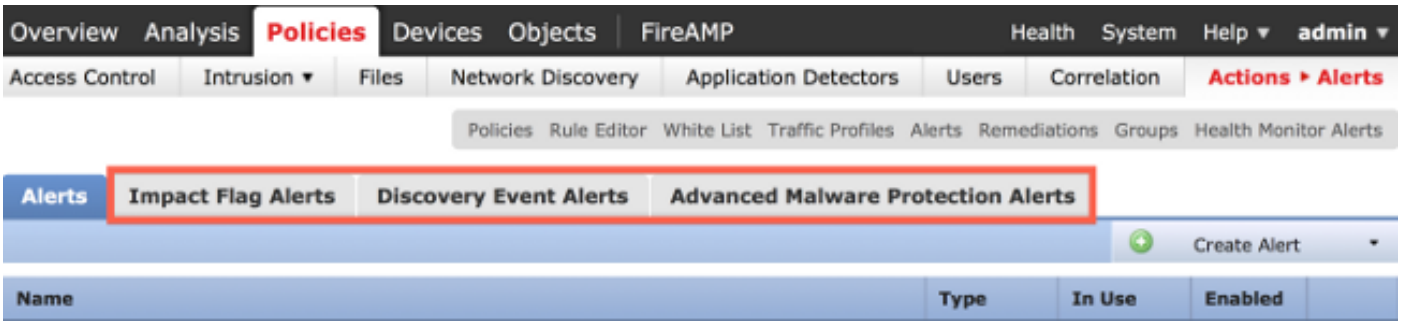
4.从**Module**列中选择要向其发送警报的系统日志服务器的运行状况模块（例如，磁盘使用情况）。

5.从**Alerts**列中选择以前创建的syslog警报。

6.单击**保存**按钮。

发送影响标志、发现事件和恶意软件警报

您还可以配置FireSIGHT管理中心，以便针对具有特定影响标志、特定类型的发现事件和恶意软件事件的事件发送系统日志警报。为此，您必须第1部分：创建系统日志警报，然后配置要发送到系统日志服务器的事件类型。为此，您可以导航到**策略>操作>警报**页面，然后选择所需警报类型的选项卡。



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。