FireSIGHT系统上的URL过滤配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[URL过滤许可证的要求](#)
[端口要求](#)
[使用的组件](#)
[配置](#)
[在FireSIGHT管理中心上启用URL过滤](#)
[在受管设备上应用URL过滤许可证](#)
[从阻止的URL类别排除特定站点](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文档介绍在FireSIGHT系统上配置URL过滤的步骤。FireSIGHT管理中心的URL过滤功能允许您在访问控制规则中写入条件，以便根据受监控主机的非加密URL请求确定流经网络的流量。

先决条件

要求

本文档对URL过滤许可证和端口有一些特定要求。

URL过滤许可证的要求

FireSIGHT管理中心需要URL过滤许可证，以便定期联系云以更新URL信息。您可以将基于类别和信誉的URL条件添加到没有URL过滤许可证的访问控制规则；但是，必须先将URL过滤许可证添加到FireSIGHT管理中心，然后在策略所针对的设备上启用该许可证，才能应用访问控制策略。

如果URL过滤许可证过期，具有基于类别和信誉的URL条件的访问控制规则将停止过滤URL，并且FireSIGHT管理中心不再联系云服务。如果没有URL过滤许可证，可以将单个URL或URL组设置为允许或阻止，但无法使用URL类别或信誉数据来过滤网络流量。

端口要求

FireSIGHT系统使用端口443/HTTPS和80/HTTP与云服务通信。必须双向打开端口443/HTTPS，并且必须在FireSIGHT管理中心上允许对端口80/HTTP的入站访问。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- FirePOWER设备：7000系列、8000系列
- 下一代入侵防御系统(NGIPS)虚拟设备
- 自适应安全设备(ASA)FirePOWER
- Sourcefire软件5.2版或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。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。

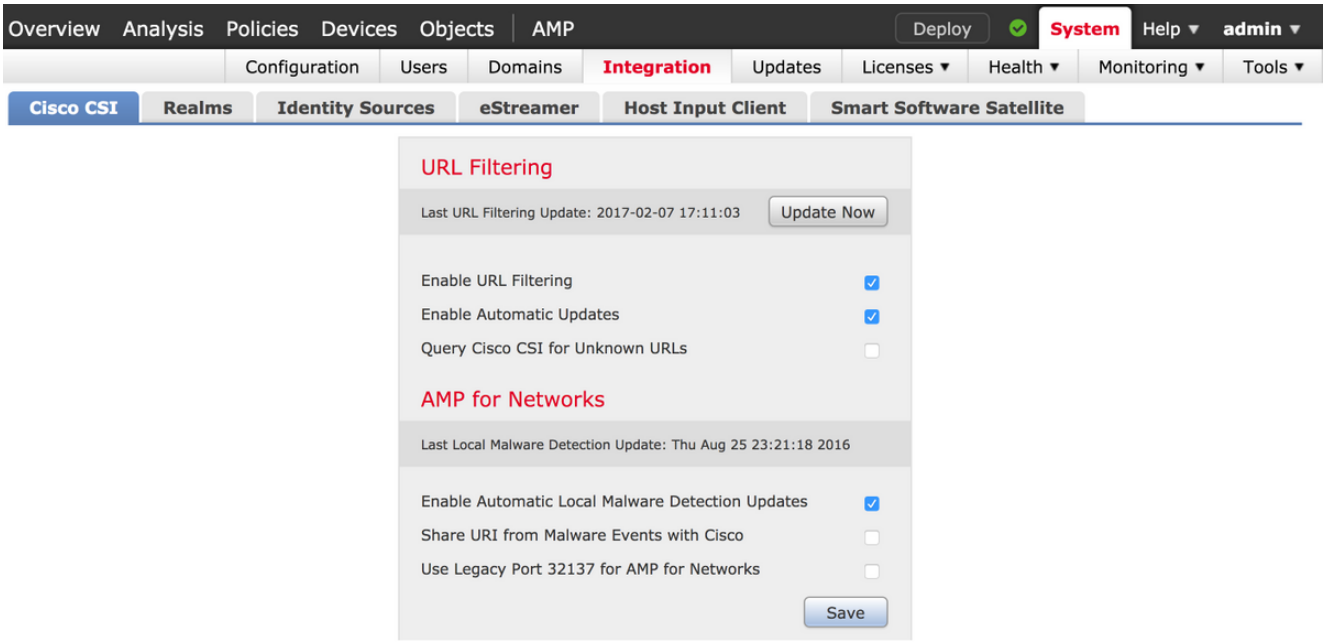
配置

在FireSIGHT管理中心上启用URL过滤

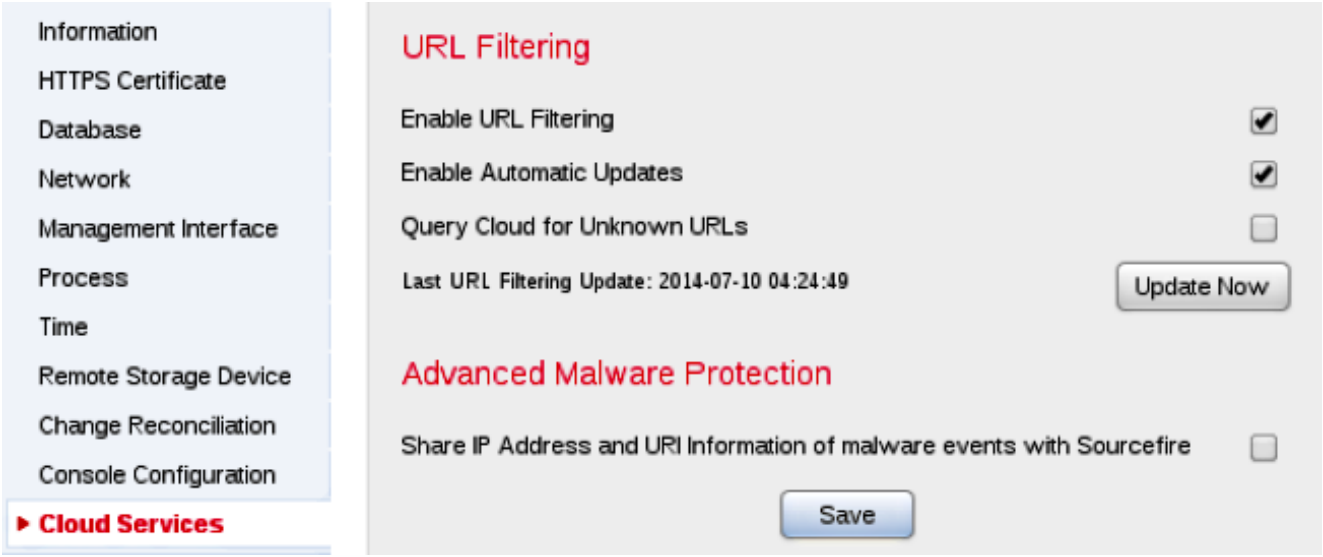
要启用URL过滤，请完成以下步骤：

1. 登录到FireSIGHT管理中心的Web用户界面。
2. 根据您运行的软件版本，导航有所不同：

   在6.1.x版本上，选择**System > Integration > Cisco CSI**。



   在5.x版本上，选择**System > Local > Configuration**。选择**Cloud Services**。



3. 选中**Enable URL Filtering**复选框以启用URL过滤。
4. 或者，选中**启用自动更新**复选框以启用自动更新。此选项允许系统定期联系云服务，以获取设备本地数据集中URL数据的更新。

   注意：虽然云服务通常每天更新一次数据，但如果启用自动更新，将强制FireSIGHT管理中心每30分钟检查一次以确保信息始终最新。虽然每日更新量通常较小，但如果自上次更新以来已超过五天，则下载新的URL过滤数据可能需要长达20分钟。下载更新后，执行更新本身可能需要30分钟。

5. 或者，选中**Query Cloud for Unknown URLs**复选框以查询云服务中的未知URL。当受监控网络上的某人尝试浏览到不在本地数据集中的URL时，此选项允许系统查询Sourcefire云。如果云不知道URL的类别或信誉，或者如果FireSIGHT管理中心无法联系云，则URL不会将访问控制规则与基于类别或信誉的URL条件相匹配。

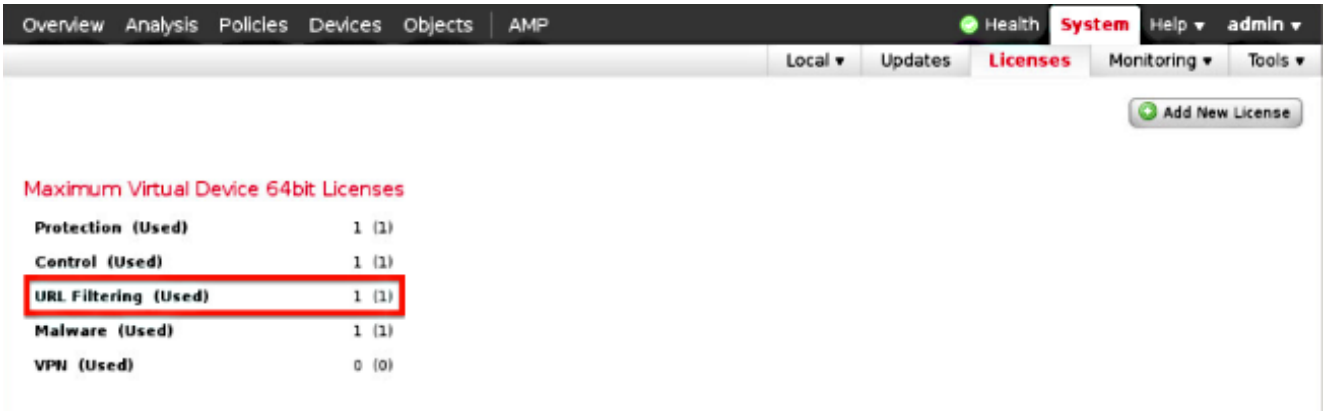
   注意：不能手动为URL分配类别或信誉。如果您不希望未分类的URL由Sourcefire云进行编录（例如，出于隐私原因），请禁用此选项。

6. Click **Save**.URL过滤设置已保存。

   注意：根据自上次启用URL过滤以来的时间长度，或者如果这是第一次启用URL过滤，FireSIGHT管理中心将从云服务检索URL过滤数据。

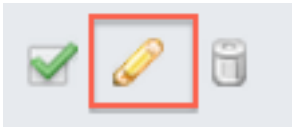
在受管设备上应用URL过滤许可证

1. 检查URL过滤许可证是否已安装在FireSIGHT管理中心上。转至**System > Licenses**页面以查找许可证列表。

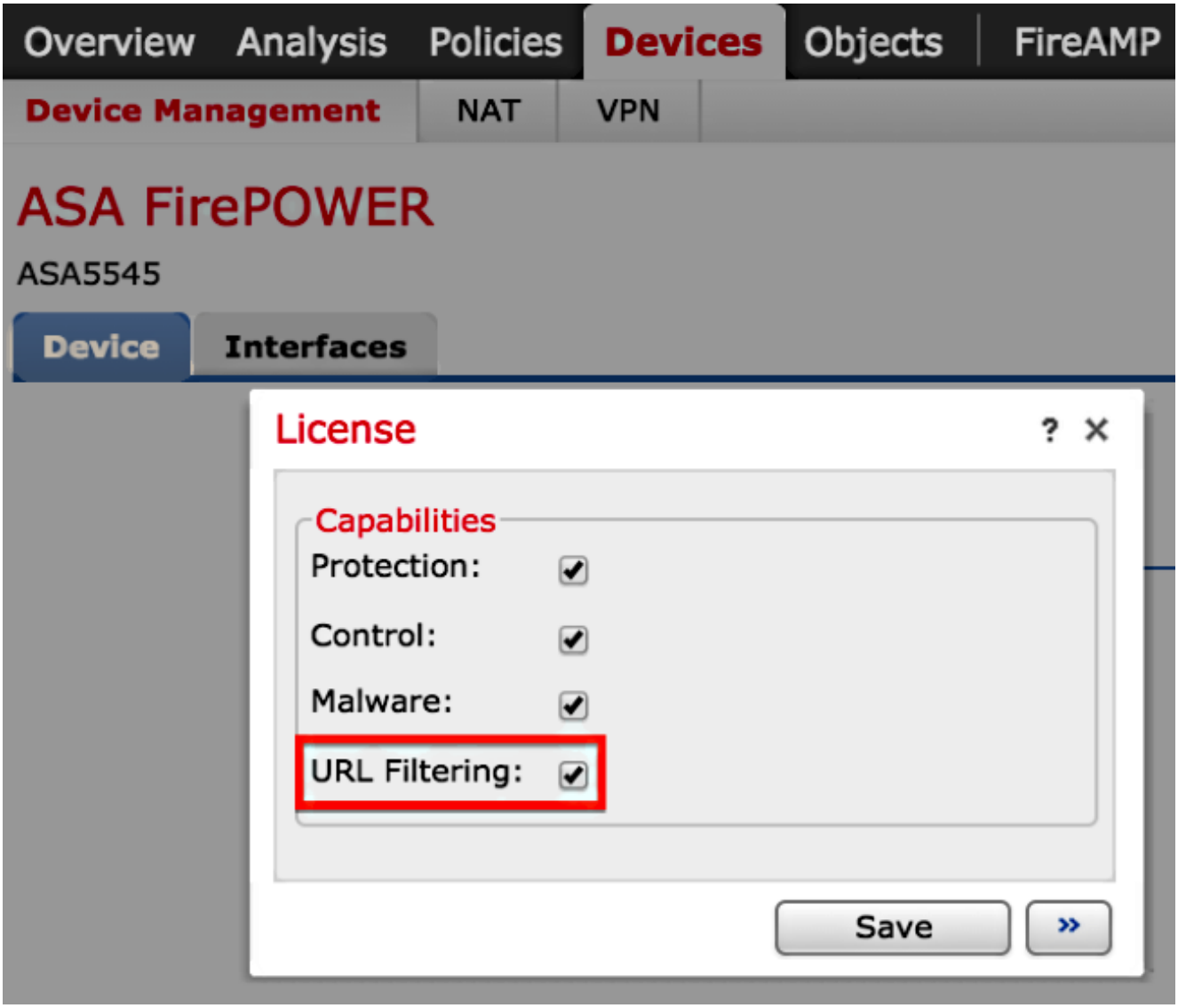


2. 转至**Devices > Device Management**页，验证是否在监控流量的设备上应用URL过滤许可证。

3. 如果URL过滤许可证未应用于设备，请单击**铅笔**图标以编辑设置。图标位于设备名称旁边。



4. 您可以从**Devices**选项卡在设备上启用URL过滤许可证。



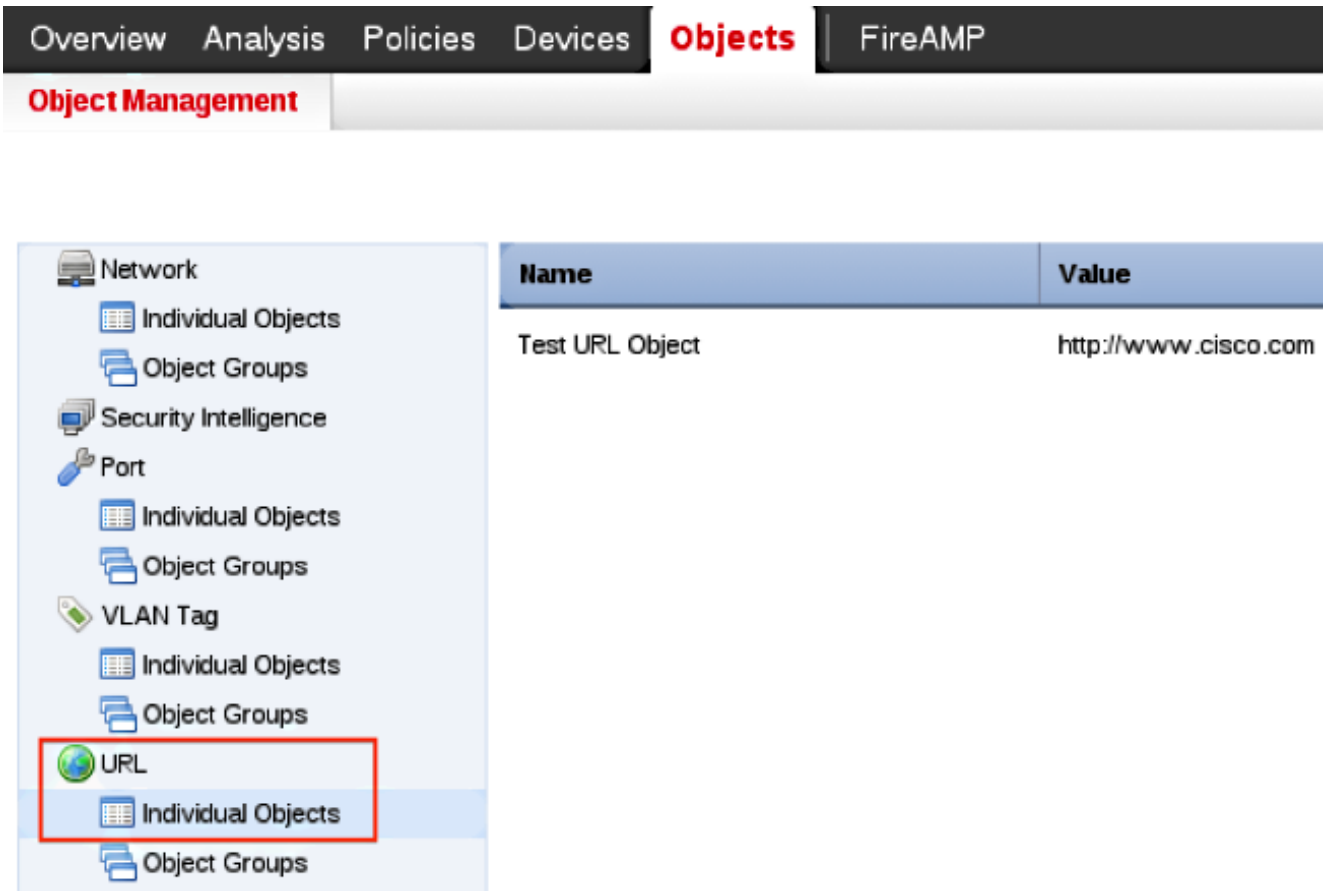
5. 启用许可证并保存更改后，您还必须点击**Apply Changes**以在受管设备上应用许可证。

从阻止的URL类别排除特定站点

FireSIGHT管理中心不允许您拥有覆盖默认Sourcefire提供的类别分级的本地URL分级。要完成此任务，必须使用访问控制策略。以下说明介绍如何在访问控制规则中使用URL对象以从阻止类别中排除特定站点。

1. 转至**Objects > Object Management**页。

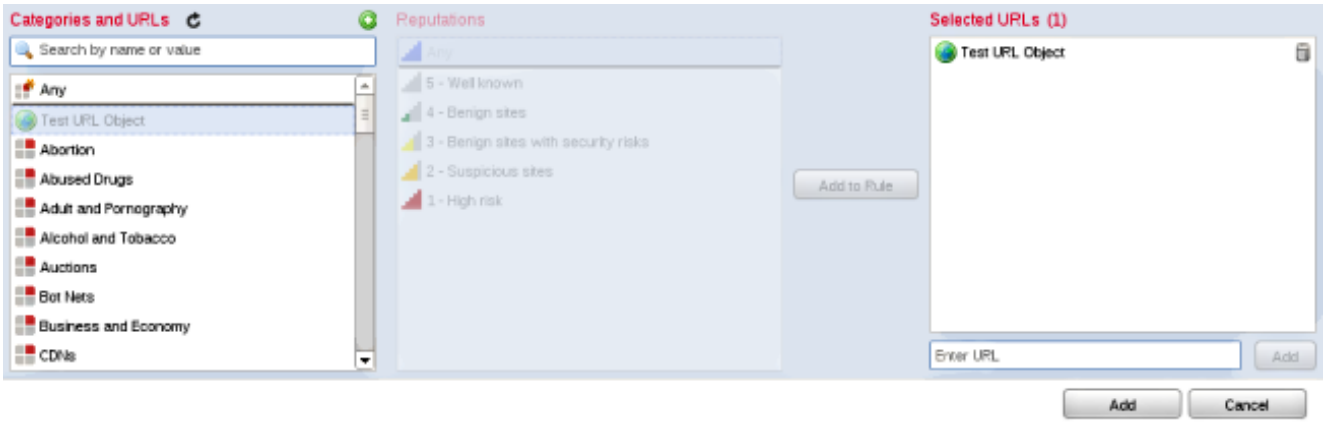
2. **选择Individual Objects** for URL，然后点击**Add URL按**钮。系统将显示**URL Objects**窗口。



3. 保存更改后，选择**Policies > Access Control**，然后单击**铅笔图标**以编辑访问控制策略。

4. 单击**Add Rule**。

5. 使用**Allow**操作将URL对象添加到规则，并将其置于URL Category规则上方，以便首先评估其规则操作。



6. 添加规则后，单击**Save and Apply**。它保存新更改并将访问控制策略应用于受管设备。

验证

有关验证或故障排除信息，请参阅相关信息部分中链接的**Troubleshoot Issue with URL Filtering on FireSIGHT System**文章。

故障排除

有关验证或故障排除信息，请参阅 **排除FireSIGHT系统上的URL过滤问题** 链接在“相关信息”部分中的文章。

相关信息

- **排除FireSIGHT系统上的URL过滤问题**
- **技术支持和文档 - Cisco Systems**

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）。