在FireSIGHT系统配置示例的URL过滤

目录

简介

本文描述步骤配置在FireSIGHT系统的URL过滤。在FireSIGHT管理中心的URL过滤功能允许您写入在访问控制规则的一个条件为了确定穿程根据不可加密的URL请求的网络由受监视主机的流量。

先决条件

要求

本文有URL过滤许可证和端口的一些一些特定需求。

URL过滤许可证的需求

FireSIGHT管理中心要求URL过滤许可证为了周期地与网云联系在URL信息的一次更新的。您能添加类别，并且对访问控制规则的基于名誉的URL条件没有URL过滤准许;然而您不能运用访问控制策略，直到您首先添加一个URL过滤许可证到FireSIGHT管理中心，然后请启用它在策略瞄准的设备。

如果URL过滤许可证超时，访问控制规定与类别，并且基于名誉的URL情况停止过滤URL，并且FireSIGHT管理中心不再与网云服务联系。没有URL过滤许可证， URL的各自的URL或组可以设置准许或阻塞，但是URL类别或名誉数据不可能用于为了过滤网络流量。

波尔特要求

FireSIGHT系统用途端口443/HTTPS和80/HTTP为了通信与网云服务。必须打开波尔特443/HTTPS双向，并且在FireSIGHT管理中心必须允许对端口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伊莱克斯：7000系列， 8000系列
- 下一代入侵防御系统(NGIPS)虚拟设备
- 可适应安全工具(ASA) Firepower
- Sourcefire软件版本5.2或以上

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

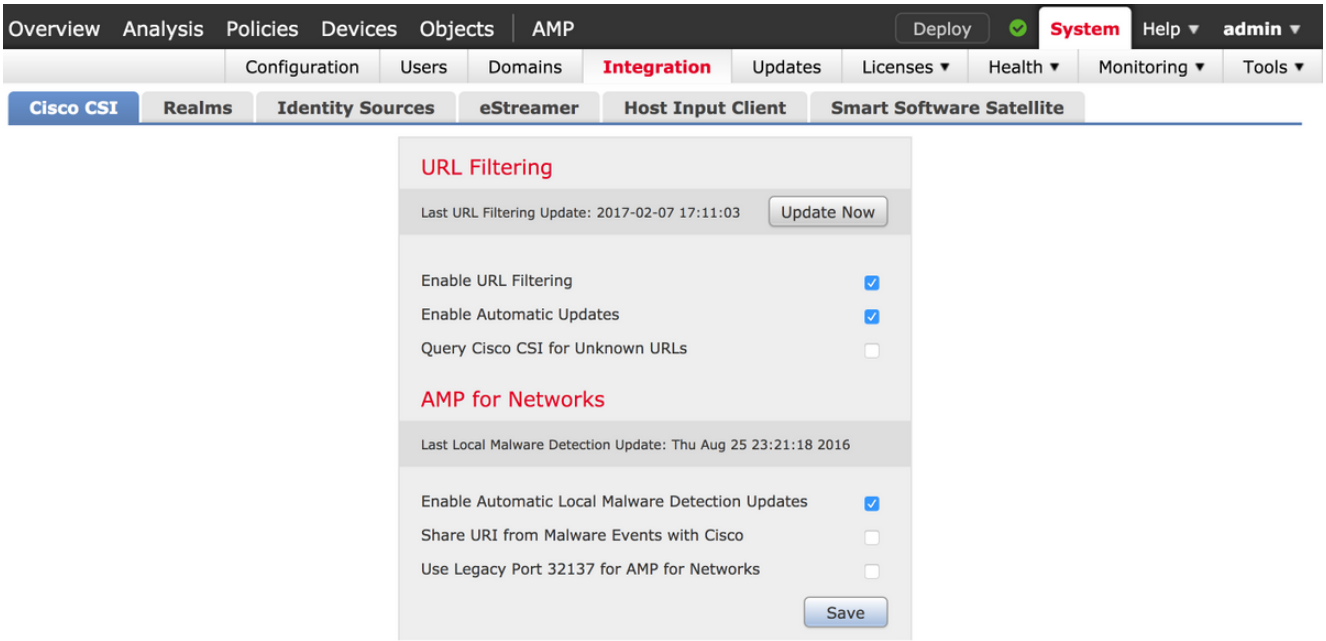
启用在FireSIGHT管理中心的URL过滤

为了启用URL过滤，请完成这些步骤：

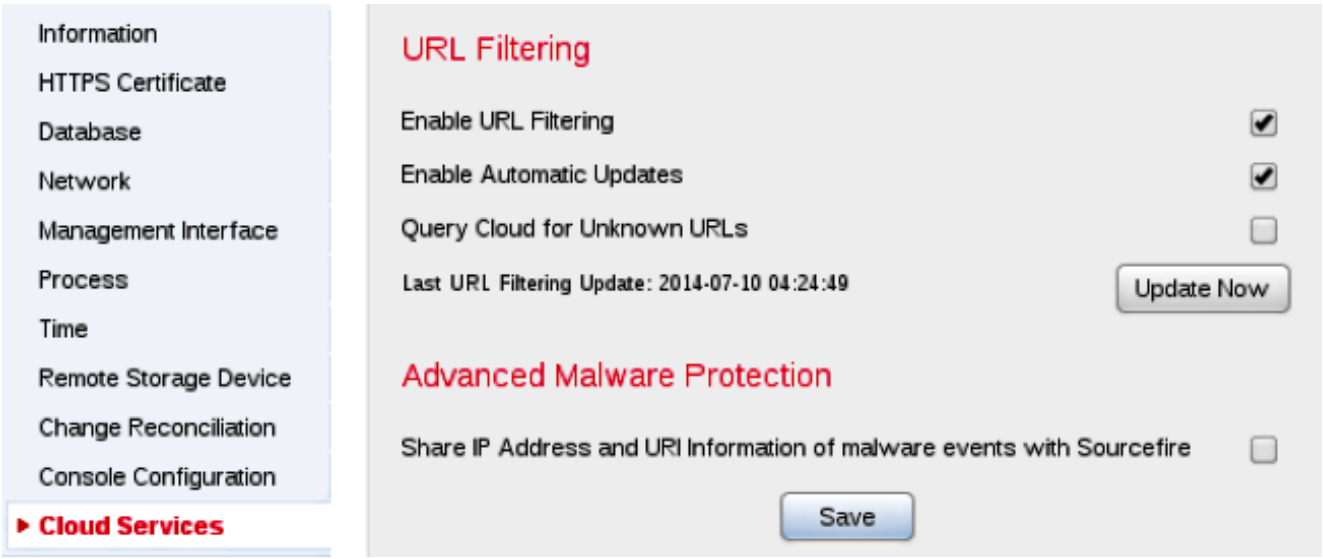
1. 登录FireSIGHT管理中心的网页用户界面。

2. 根据您运行的软件版本不同的定位：

   在版本6.1.x，请选择**系统>集成> Cisco CSI**。



   在版本5.x，请选择**系统>本地>配置**。选择**Cloud服务**。



3. 检查**Enable (event) URL过滤**复选框为了启用URL过滤。
4. 随意地，请检查**Enable (event)自动更新**复选框为了启用自动更新。此选项允许系统经常与网云服务联系为了得到更新到在设备的本地数据数据集的URL数据。

   Note:虽然网云服务典型地更新其数据一次每天，如果启用自动更新它强制FireSIGHT管理中心检查每30分钟为了确保，信息总是当前。虽然每天更新倾向于小，如果是超过五天从最近一次更新，新建的URL过滤数据也许花费20分钟下载。一旦更新下载，它也许花费30分钟执行更新。

5. 随意地，请检查**查询Cloud**未知URL复选框的**未知URL**为了查询网云服务未知URL。此选项允许系统查询Sourcefire网云，当某人不在本地数据数据集的您的受监视网络的尝试浏览到URL时。如果网云不认识URL的类别或名誉，或者，如果FireSIGHT管理中心不能与网云联系，URL不匹配访问控制规则以类别或基于名誉的URL情况。

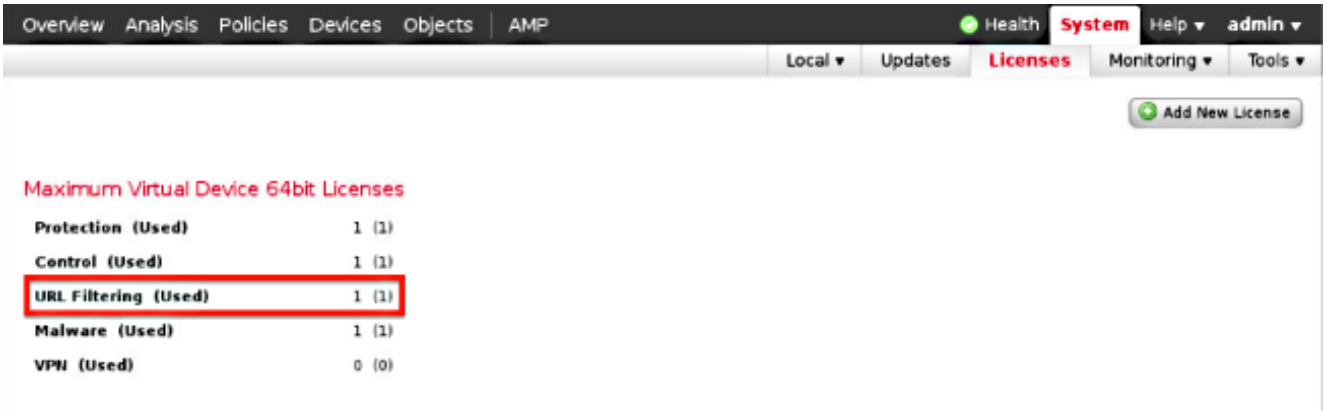
   Note:您不能手工分配类别或名誉到URL。如果不希望您的uncategorized URL由Sourcefire网云编目，例如，保密性原因的，请禁用此选项。

6. Click **Save**.URL过滤设置保存。

   Note:基于时间长度，因为URL过滤是启用的为时，或者，如果这第一次是您启用URL过滤，FireSIGHT管理中心从网云服务获取URL过滤数据。

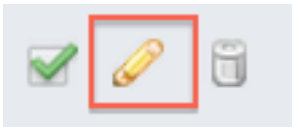
应用在受管理设备的URL过滤许可证

1. 检查URL过滤许可证是否在FireSIGHT管理中心安装。去**系统>许可证**页为了查找许可证列表。

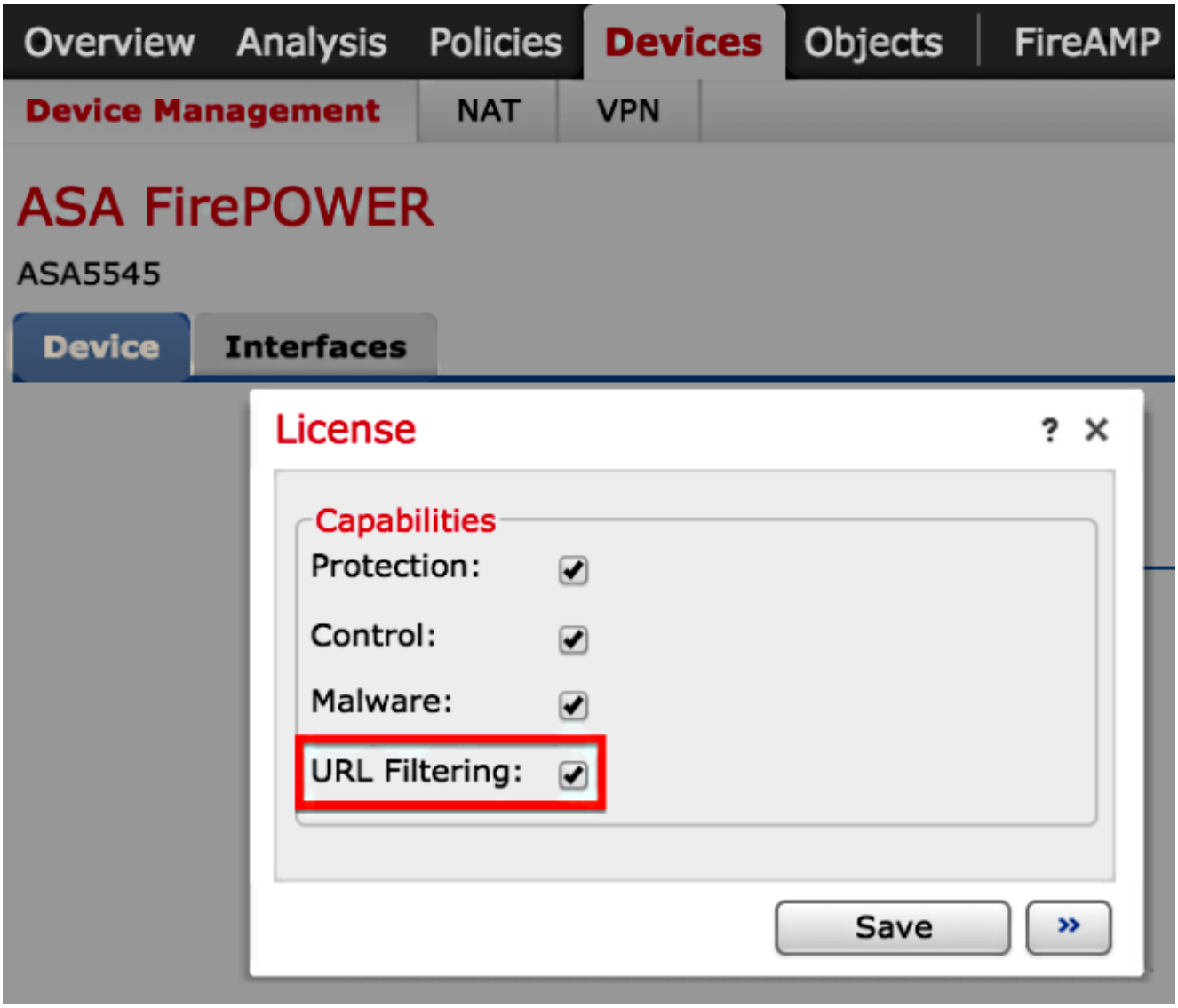


2. 请去**设备>设备管理**页，并且验证，如果URL过滤许可证在监控流量的设备应用。

3. 如果URL过滤许可证在设备没有应用，请点击**铅笔**图标为了编辑设置。图标在设备名旁边查找。



4. 您能启用在一个设备的URL过滤许可证从**Devices选项**。



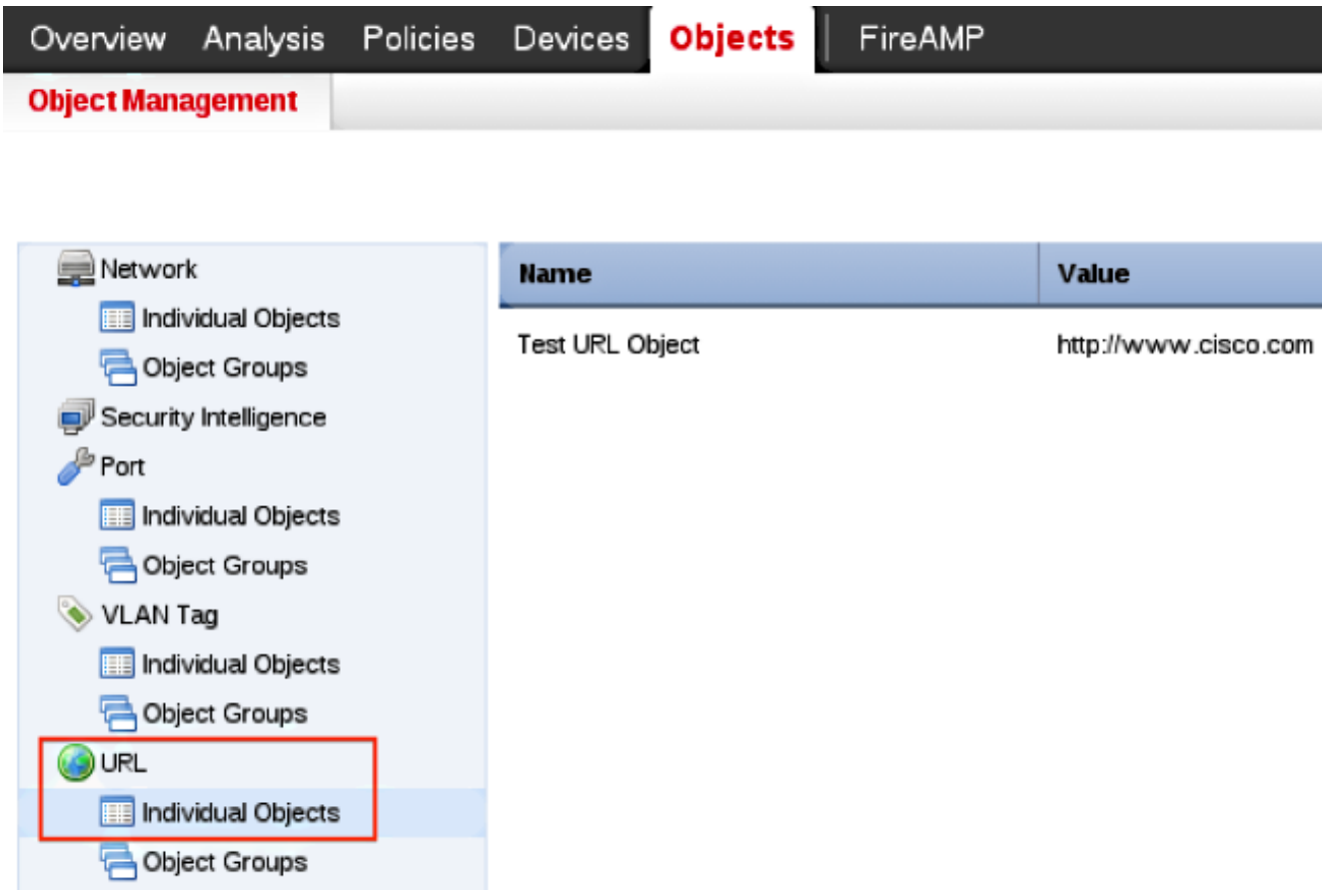
5. 在您启用许可证并且保存您的更改后，您必须也单击**应用更改**为了应用在您的受管理设备的许可证。

特定站点的排除从阻止URL类别的

FireSIGHT管理中心不允许您有改写默认Sourcefire提供的类别规定值URL的本地利率。为了完成此任务，您必须使用访问控制策略。这些说明在访问控制规则描述如何使用URL对象为了从块类别排除一个特定站点。

1. 去**对象>对象管理**页。

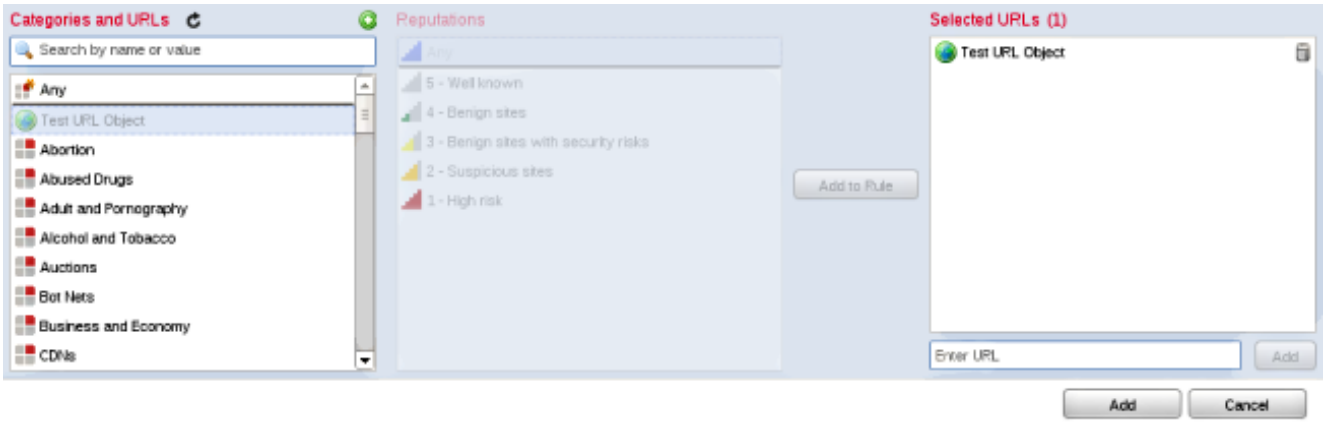
2. **选择**URL的**各自的对象**，并且点击**添加URL**按钮。**URL对象**窗口出现。



3. 在您保存更改后，请选择**策略>访问控制**并且点击**铅笔**图标为了编辑访问控制策略。

4. 单击**增加规则**。

5. 添加您的对规则的URL对象与**允许**操作并且在URL类别规则上放置它，因此其规则操作首先被评估。



6. 在您增加规则后，请点击**“Save”并且应用**。它保存新的更改并且适用于访问控制策略被管理的设备。

验证

Verify或Troubleshoot信息，参考**与URL过滤的排除故障问题在FireSIGHT**在相关信息部分连接的**系统**条款。

故障排除

Verify或Troubleshoot信息，参考**与URL过滤的排除故障问题在FireSIGHT**在相关信息部分连接的**系统**条款。

相关信息

- 排除故障与URL过滤的问题在FireSIGHT系统
- 技术支持和文档 - Cisco Systems