在FireSIGHT系统配置示例的URL过滤

Contents

Introduction

本文描述步骤配置在FireSIGHT系统的URL过滤。在FireSIGHT管理中心的URL过滤功能在访问控制规则允许您写情况为了确定穿程根据不可加密的URL请求的网络由被监控的主机的数据流。

Prerequisites

Requirements

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管理中心要求一个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，然后在设备由策略瞄准的enable (event)。

如果URL过滤许可证到期，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，可以设置各自的URL或组URL准许或阻拦，但是URL类别或名誉数据不可能用于为了过滤网络流量。

端口需求

FireSIGHT系统使用端口443/HTTPS和80/HTTP为了与网云服务联络。必须打开端口443/HTTPS双向，并且在FireSIGHT管理中心必须允许对端口80/HTTP的Inbound访问。

Components Used

本文档中的信息基于下列硬件和软件版本：

- Firepower工具：7000系列， 8000系列
- 下一代入侵防御系统(NGIPS)虚拟工具
- 可适应的安全工具(ASA) Firepower
- Sourcefire软件版本5.2或以上

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

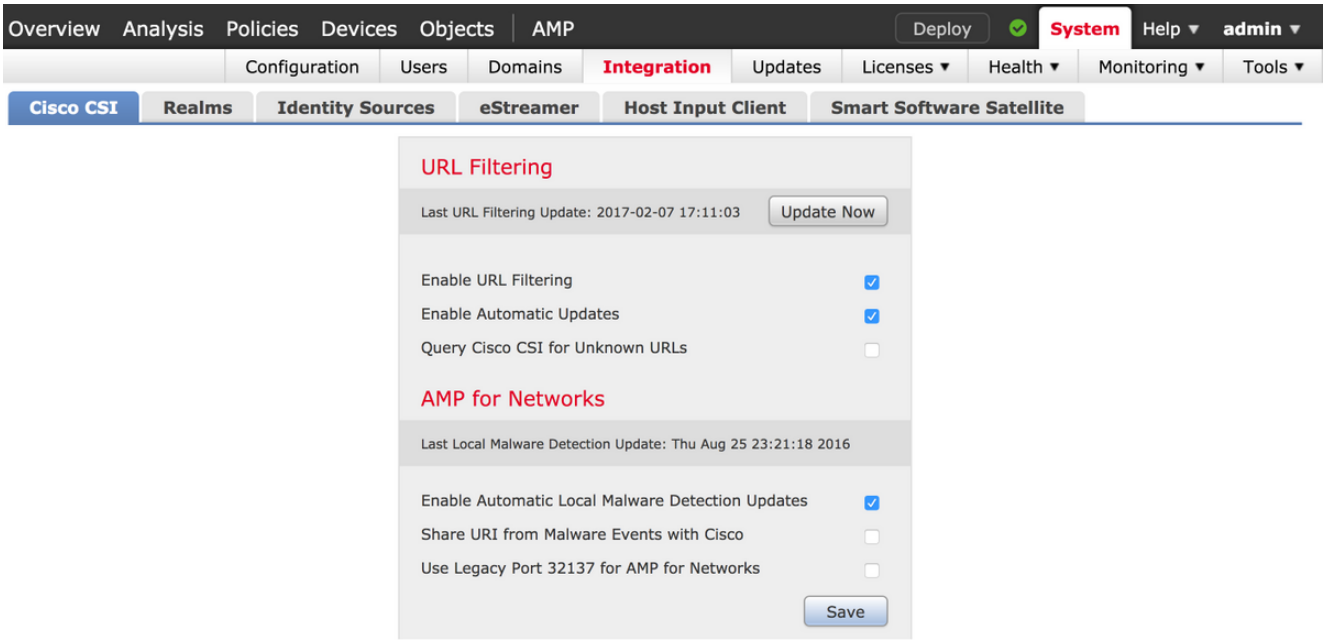
在FireSIGHT管理中心的Enable (event) URL过滤

为了enable (event) URL过滤，完成这些步骤：

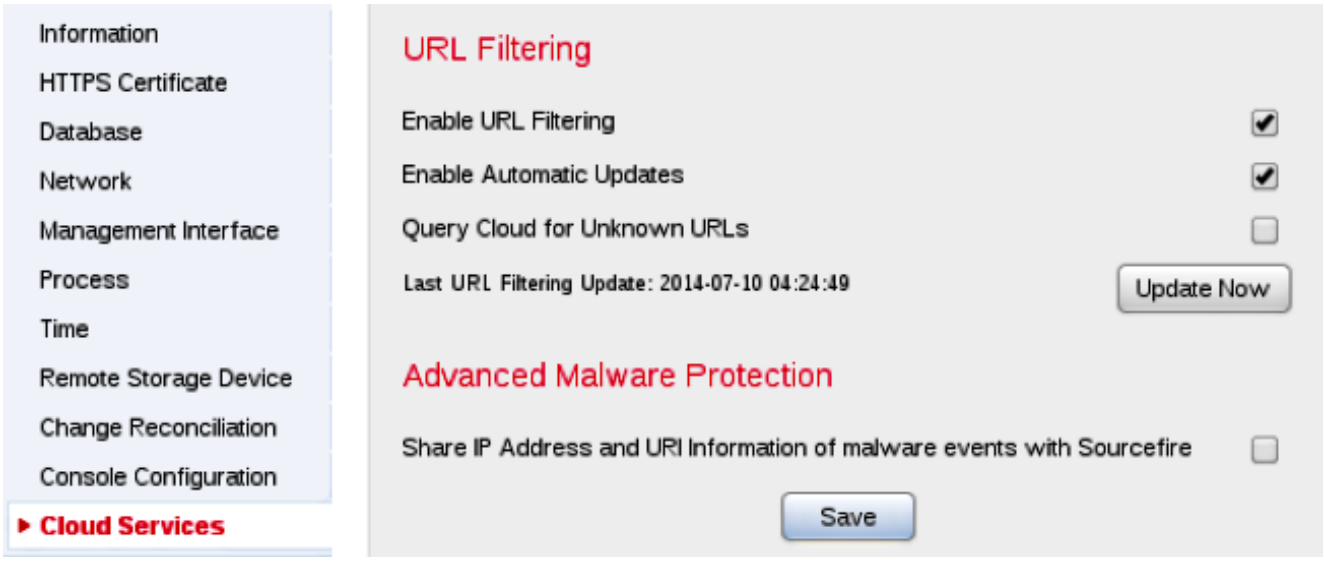
1. 日志到FireSIGHT管理中心的网页用户界面里。

2. 根据您运行的软件版本是不同的定位：

   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enable (event) URL过滤。
4. 随意地，请检查**Enable (event)自动更新**复选框为了enable (event)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工具的本地数据集的URL数据。

   Note:虽然网云服务典型地更新其数据一次每天，如果自动的enable (event)更新强制FireSIGHT管理中心检查每30分钟为了确信，信息总是当前的。虽然每日更新倾向于是小的，如果是超过五天从最近一次更新，新的URL过滤数据也许花费20分钟下载。一旦下载了更新，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集的您的被监控的网络的尝试访问到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。

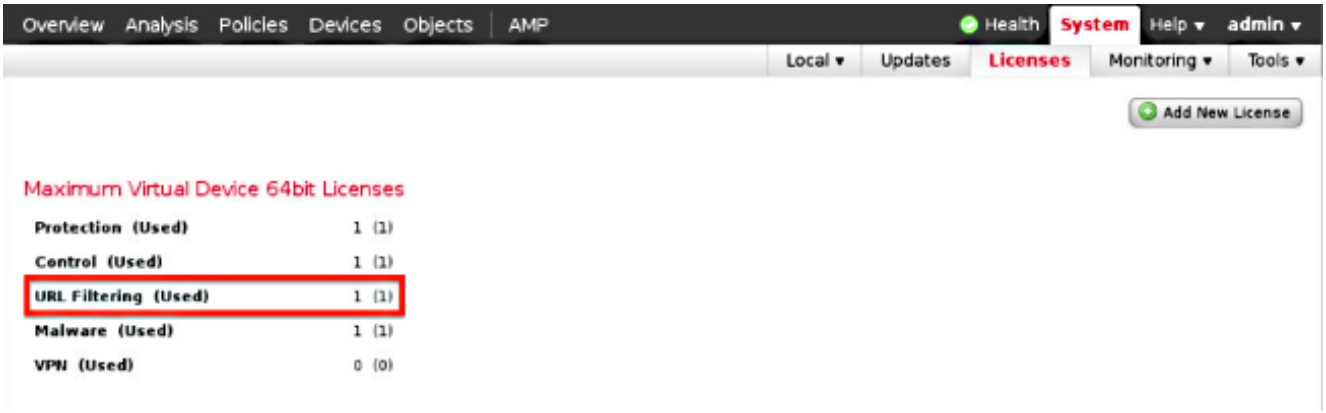
   Note:您不能手工分配类别或名誉到URL。如果不希望您的uncategorized URL由Sourcefire网云编目，例如，保密性原因的，请禁用此选项。

6. Click **Save**.URL过滤设置被保存。

   Note:基于时间长度，因为URL过滤最后被启用了，或者，如果这第一次是您允许URL过滤，FireSIGHT管理中心从网云服务检索URL过滤数据。

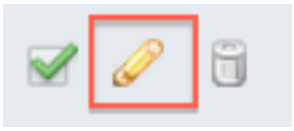
应用在可管理的设备的URL过滤许可证

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

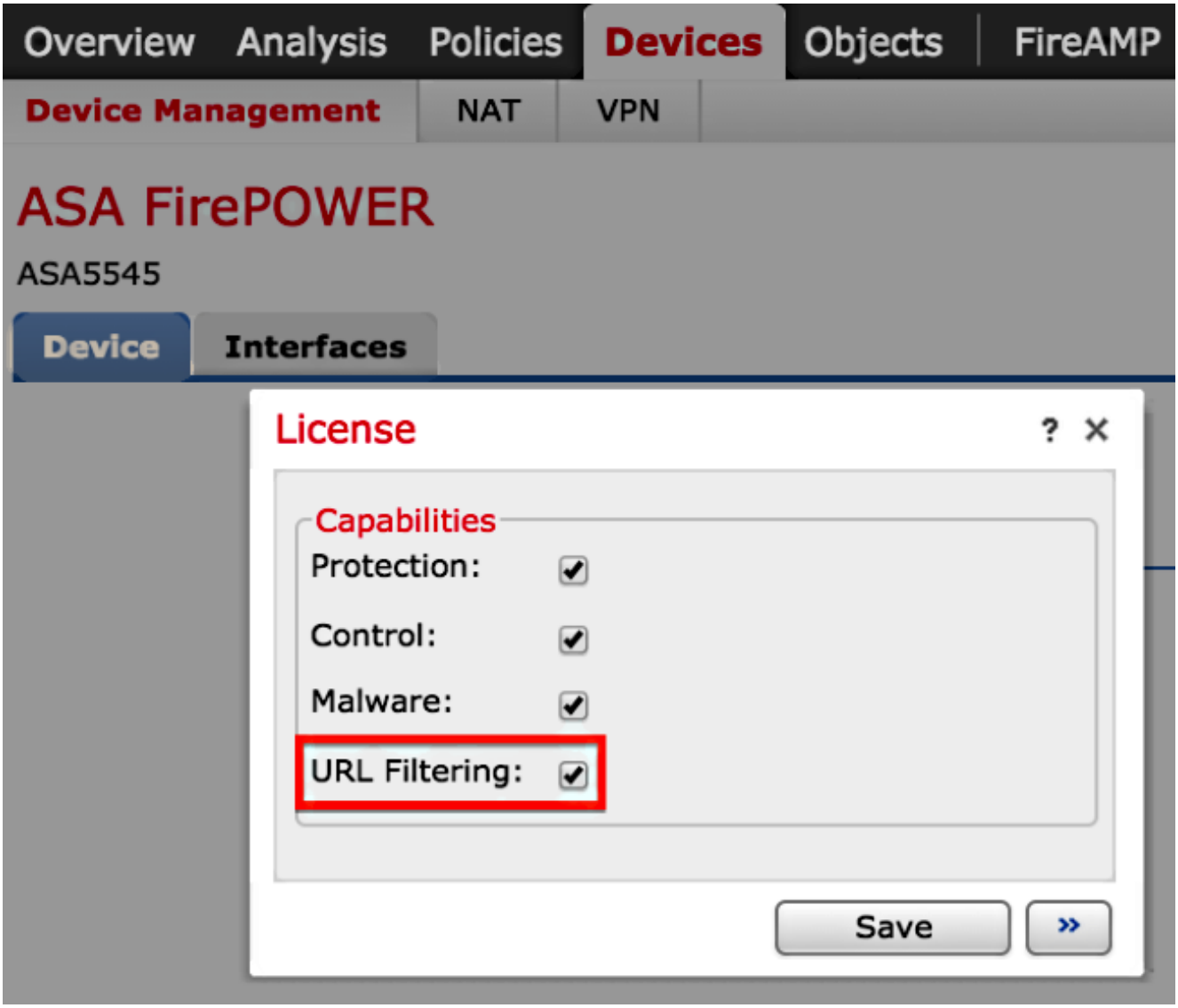


2. 去**设备>设备管理**页，并且验证URL过滤许可证是否在监控数据流的设备被应用。

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



4. 您能enable (event)在一个设备的URL过滤许可证从**Devices选项**。



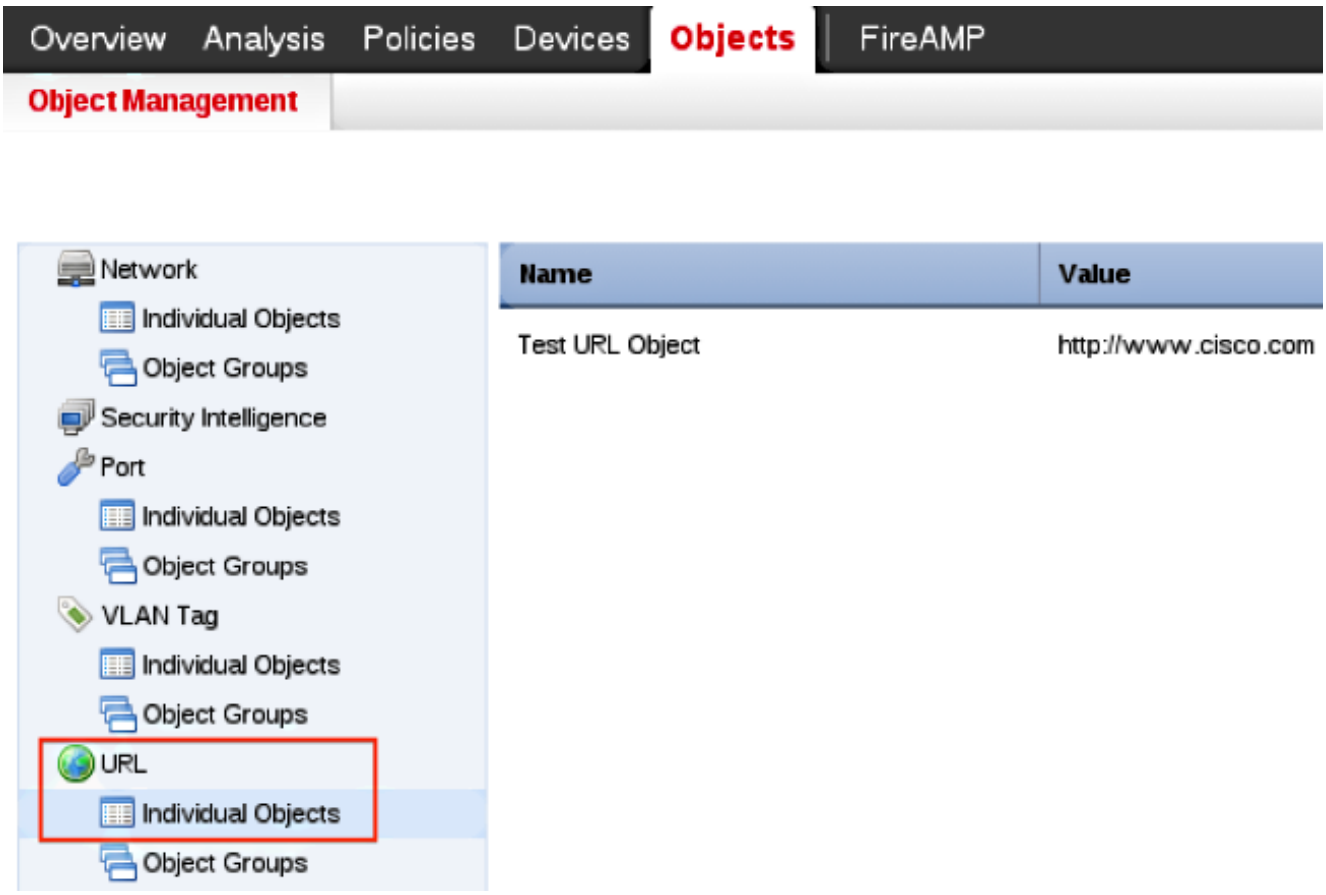
5. 在您enable (event)许可证和保存您的更改，您必须也点击**应用更改**为了应用在您的可管理的设备后的许可证。

特定站点的排除从封锁的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的本地规定值。为了完成此任务，您必须使用访问控制策略。这些指令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。

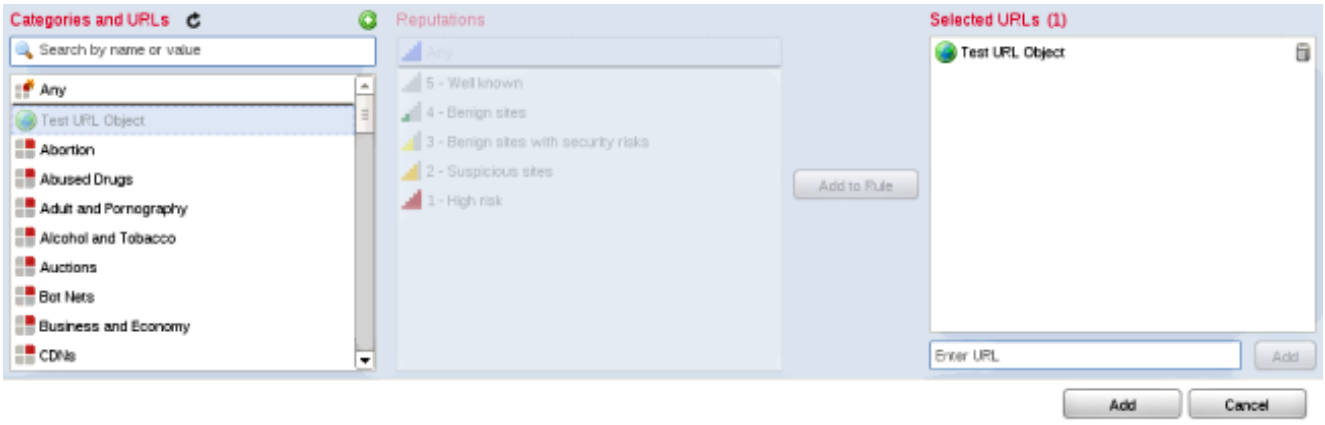
2. **选择**URL的**各自的对象**，并且点击**添加URL**按钮。**URL对象**窗口出现。



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. 点击**增加规则**。

5. 添加您的URL对象到与**允许**动作的规则并且在URL类别规则上放置它，因此其规则动作首先被评估。



6. 在您增加规则后，请点击**“Save”并且适用**。它保存新的更改并且运用访问控制策略于被管理的工具。

Verify

Verify或Troubleshoot信息，请参见**URL过滤的故障排除问题在FireSIGHT**在相关信息部分连接的**系统**条款。

Troubleshoot

Verify或Troubleshoot信息，请参见**URL过滤的故障排除问题在FireSIGHT**在相关信息部分连接的**系统**条款。

Related Information

- [用在FireSIGHT系统的URL过滤排除问题故障]
- [Technical Support & Documentation - Cisco Systems]