排除FireSIGHT系统上的URL过滤问题

目录

简介
URL过滤查找过程
云连接问题
步骤 1：检查许可证
许可证是否已安装？
许可证是否过期？
步骤 2：检查运行状况警报
步骤 3：检查DNS设置
步骤 4：检查与所需端口的连接
访问控制和错误分类问题
问题 1：允许或阻止未选择信誉级别的URL
规则操作为Allow
规则操作为Block
URL选择矩阵
问题 2：通配符在访问控制规则中不起作用
问题 3：URL类别和信誉未填充
相关信息

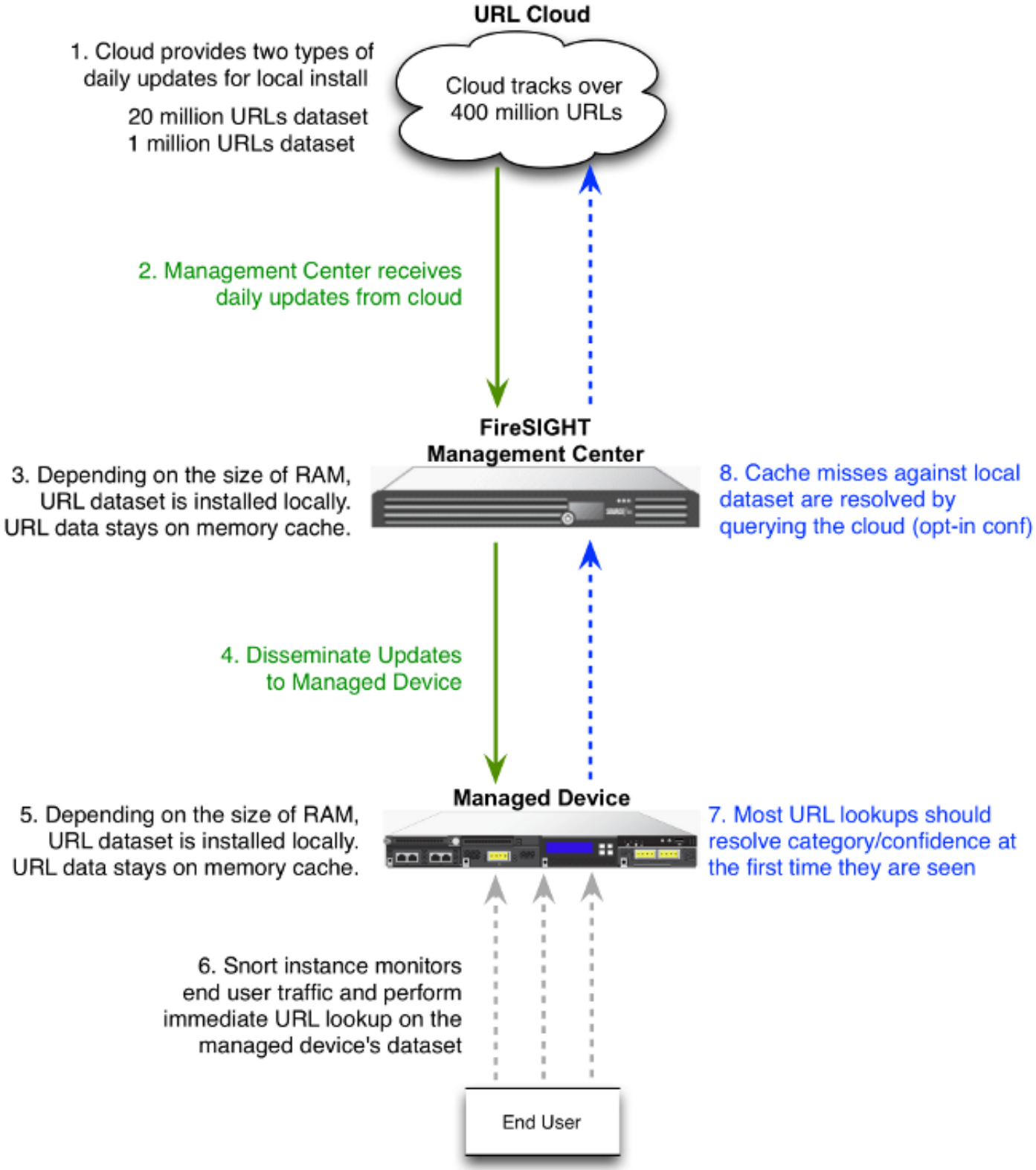
简介

本文档介绍URL过滤的常见问题。FireSIGHT管理中心上的URL过滤功能可对受监控主机的流量进行分类，并允许您根据信誉在访问控制规则中写入条件。

URL过滤查找过程

为了加速URL查找过程，URL过滤提供本地安装在Firepower系统上的数据集。根据设备上可用的内存量(RAM)，有两种类型的数据集：

数据集类型	内存要求 在5.3版上	内存要求 在5.4或更高版本上
2000万个URL数据集	>2GB	>3.4 GB
100万个URL数据集	<= 2GB	<= 3.4 GB



云连接问题

步骤 1：检查许可证

许可证是否已安装？

您可以向没有URL过滤许可证的访问控制规则添加基于类别和信誉的URL条件，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。

许可证是否过期？

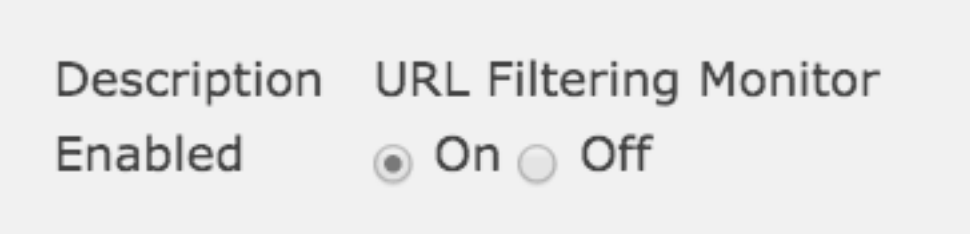
如果URL过滤许可证过期，具有基于类别和信誉的URL条件的访问控制规则将停止过滤URL，并且FireSIGHT管理中心不再联系云服务。

> **提示：**阅读FireSIGHT系统上的URL过滤配置示例，以了解如何在FireSIGHT系统上启用URL过滤功能并在受管设备上应用URL过滤许可证。

步骤 2：检查运行状况警报

URL过滤监控模块跟踪FireSIGHT管理中心与思科云之间的通信，在该云中，系统获取常见受访URL的URL过滤（类别和信誉）数据。URL过滤监控模块还跟踪FireSIGHT管理中心与已启用URL过滤的任何受管设备之间的通信。

要启用URL过滤监控器模块，请转至**运行状况策略配置**页面，选择**URL过滤监控**。单击**Enabled**选项的**On**单选按钮，以便允许使用该模块进行运行状况测试。如果希望设置生效，必须将运行状况策略应用到FireSIGHT管理中心。



- **关键警报:**如果FireSIGHT管理中心无法成功与云通信或从云中检索更新，该模块的状态分类将更改为*严重*。
- **警告性警报:**如果FireSIGHT管理中心成功与云通信，如果管理中心无法将新的URL过滤数据推送到其受管设备，则模块状态更改为*警告*。

步骤 3：检查DNS设置

FireSIGHT管理中心在云查找期间与这些服务器通信：

```
database.brightcloud.com
service.brightcloud.com
```

确保防火墙允许两台服务器后，在FireSIGHT管理中心运行以下命令，并验证管理中心是否能够解析名称：

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

步骤 4：检查与所需端口的连接

FireSIGHT系统使用端口443/HTTPS和80/HTTP与云服务通信。

确认管理中心能够成功执行nslookup后，使用telnet检验到端口80和端口443的连接。URL数据库通过database.brightcloud.com在端口443下载，而未知URL查询在service.brightcloud.com的端口

80上完成。

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

以下输出是成功通过telnet连接到database.brightcloud.com的示例。

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

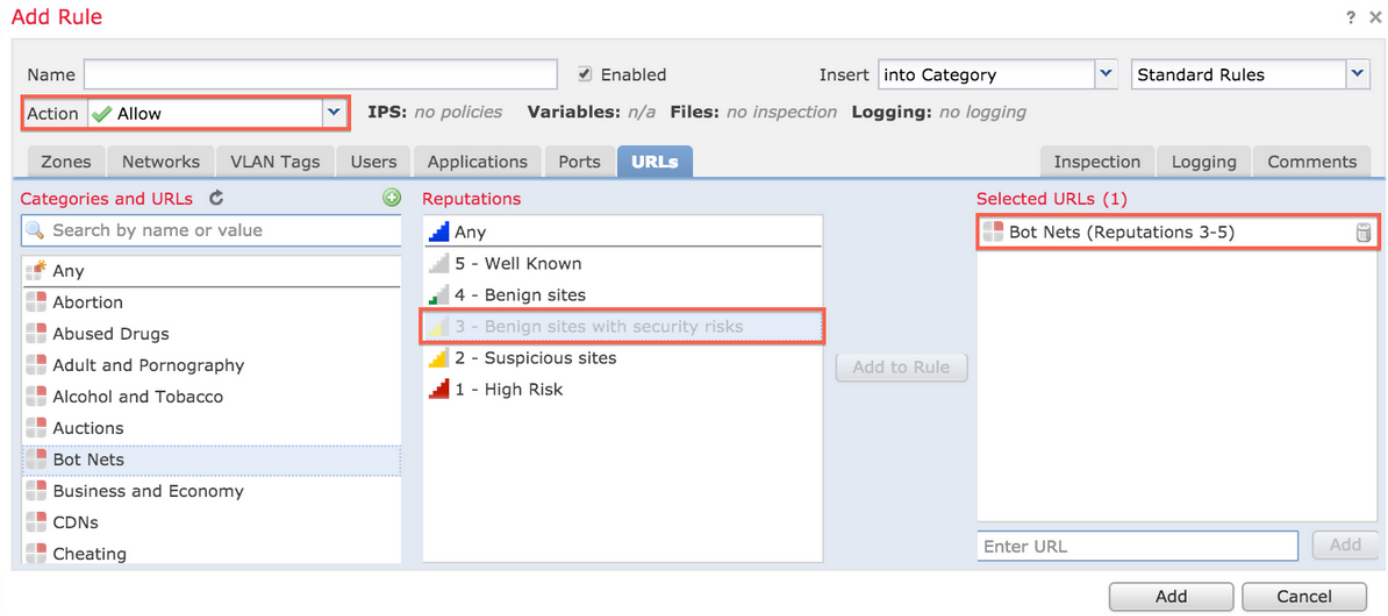
访问控制和错误分类问题

问题 1：允许或阻止未选择信誉级别的URL

如果您注意到某个URL被允许或阻止，但您没有在访问控制规则中选择该URL的信誉级别，请阅读本节以了解URL过滤规则的工作原理。

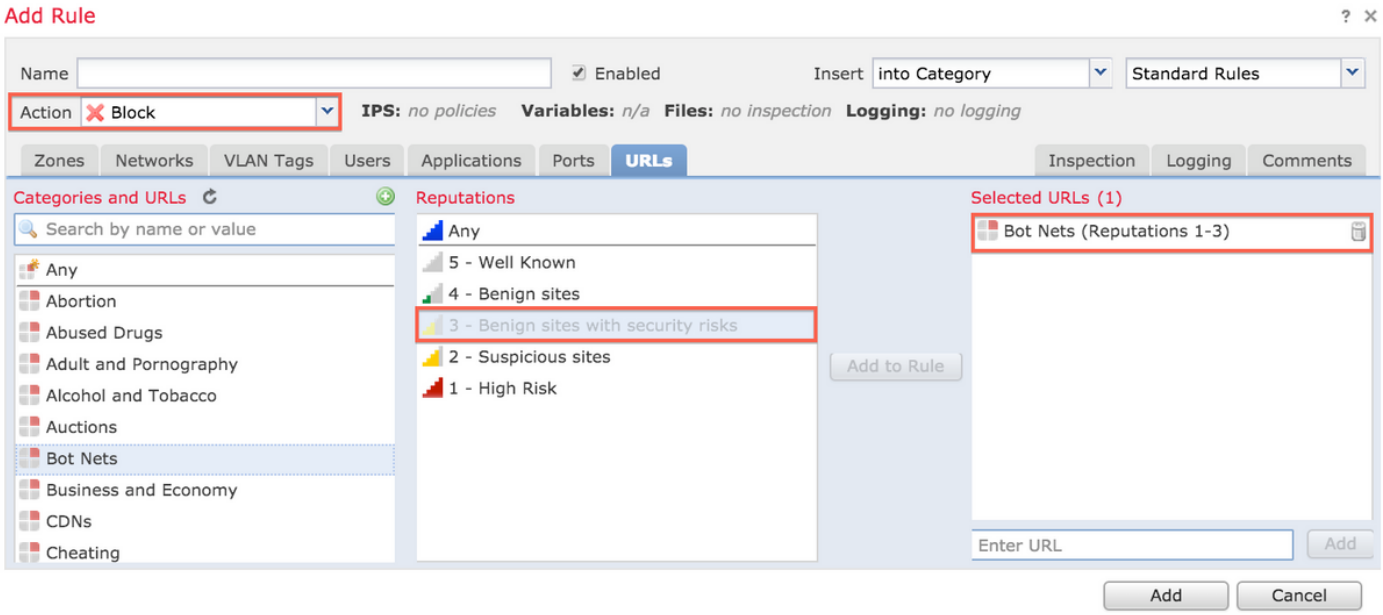
规则操作为Allow

当您根据信誉级别创建规则以**Allow**流量时，选择信誉级别还会选择比您最初选择的级别安全的所有信誉级别。例如，如果将规则配置为允许*Benign sites with security risks*（级别3），则它还会自动允许*Benign sites*（级别4）和*Well known*（级别5）站点。



规则操作为Block

当您创建基于信誉级别的**Block**流量的规则时，选择信誉级别还会选择比您最初选择的级别更严重的所有信誉级别。例如，如果将规则配置为阻止*Benign Sites with security risks*（级别3），则它还会自动阻止*Suspicious sites*（级别2）和*High risk*（级别1）站点。



URL选择矩阵

所选信誉级别

1 — 高风险
2 — 可疑站点
3 — 存在安全风险的良性站点
4 — 良性站点
5 — 已知

所选规则操作
高风险 可疑站点 存在安全风险的良性站点 良性站点 广为人知

问题 2：通配符在访问控制规则中不起作用

FireSIGHT系统不支持在URL条件中指定通配符。这种情况可能无法在cisco.com上发出警报。

```
*cisco*.com
```

此外，不完整的URL可能会与其他流量匹配，从而导致意外结果。在URL条件中指定单个URL时，必须仔细考虑可能受影响的其他流量。例如，请考虑想要明确阻止cisco.com的场景。但是，子字符串匹配意味着阻止cisco.com也会阻止sanfrancisco.com，这可能不是您的意图。

输入URL时，请输入域名并忽略子域信息。例如，键入cisco.com，而不是 www.cisco.com。在 允许规则中使用 cisco.com时，用户可以浏览到以下任一URL:

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

问题 3：URL类别和信誉未填充

如果URL不在本地数据库中，并且它是第一次在流量中看到该URL，则可能无法填充类别或信誉。这意味着首次看到未知URL时，它与AC规则不匹配。 有时，在首次看到URL时，经常访问的URL的URL查找可能无法解决。此问题已在版本5.3.0.3、5.3.1.2和5.4.0.2、5.4.1.1中得到修复。

相关信息

- 在FireSIGHT系统上配置URL过滤
- 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）。