排除故障与URL过滤的问题在FireSIGHT系统

目录

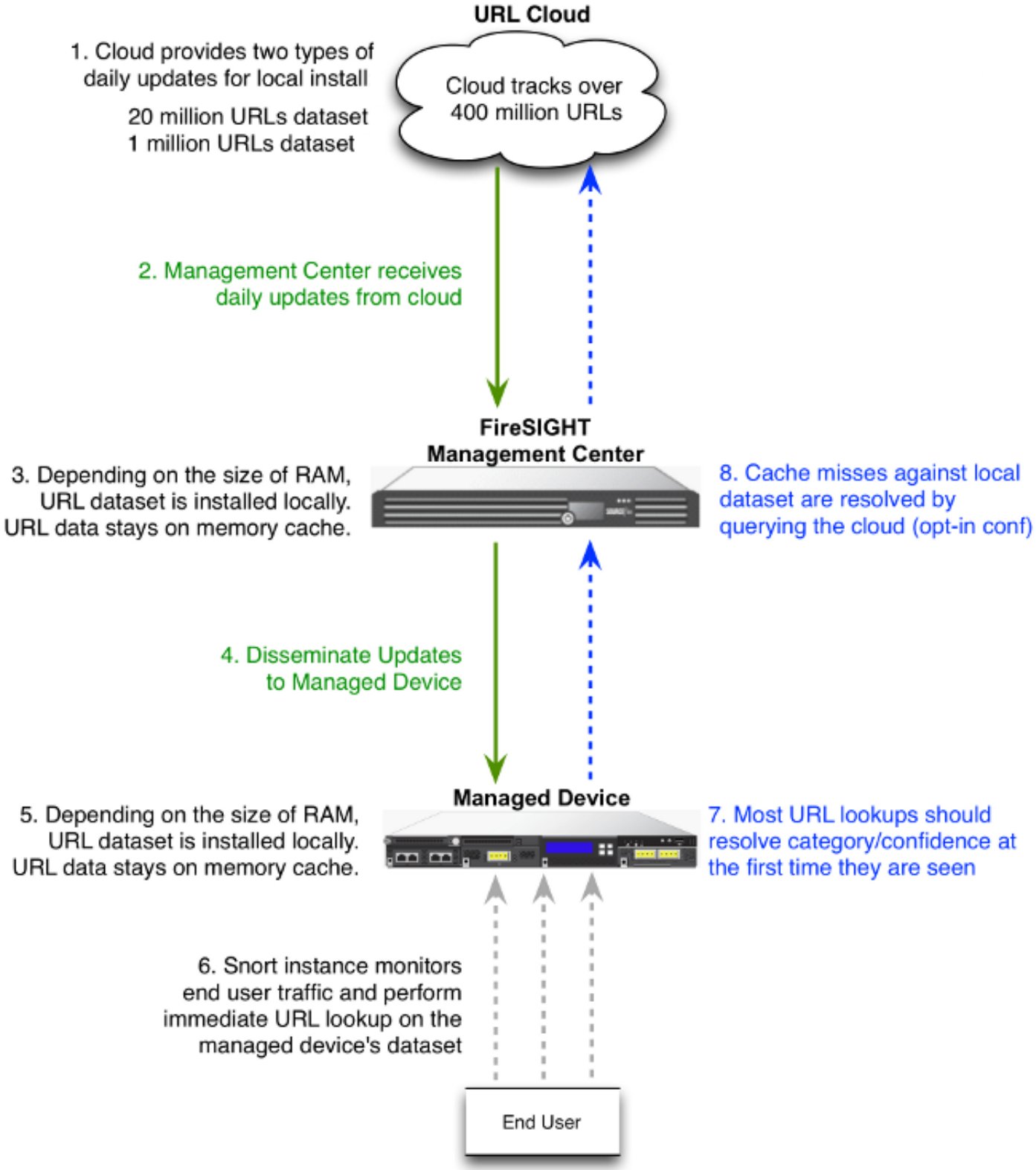
简介

本文描述与URL过滤的常见问题。在FireSIGHT管理中心的URL过滤功能分类受监视主机流量并且允许您写入在根据名誉的访问控制规则的一个条件。

URL过滤查找进程

为了加速URL查找进程， URL过滤提供在Firepower系统安装本地的数据集。从属在内存数量(RAM)联机于设备，有数据集的两种类型：

数据集的类型	内存要求	
	在版本5.3	在版本5.4或以上
20百万URL数据集	>2GB	>3.4 GB
1百万URL数据集	<= 2GB	<= 3.4 GB



Cloud连通性问题

步骤 1：检查许可证

许可证安装？

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，然而您在策略瞄准的设备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，然后启用它。

许可证超时？

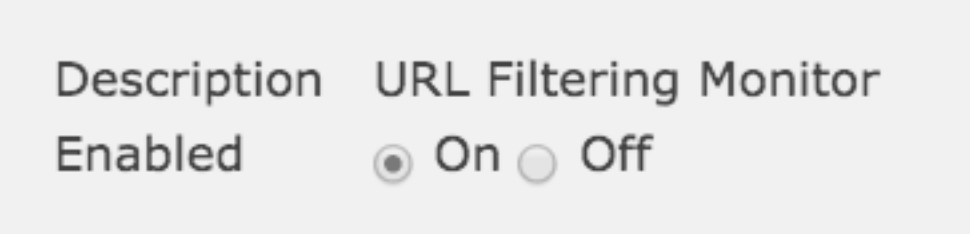
如果URL过滤许可证超时，访问控制规定与类别，并且基于名誉的URL情况停止过滤URL，并且FireSIGHT管理中心不再与网云服务联系。

> **提示**：读URL过滤在FireSIGHT系统配置示例为了学习如何启用在FireSIGHT系统的URL过滤功能和应用在受管理设备的URL过滤许可证。

步骤 2：检查健康警报

FireSIGHT管理中心和思科之间的URL过滤箴言报模块跟踪通信覆盖，其中系统得到其URL过滤(类别和名誉)数据为通常被访问的URL。URL过滤箴言报模块也跟踪FireSIGHT管理中心和您启用URL过滤的所有受管理设备之间的通信。

为了启用URL过滤箴言报模块，请去**健康策略配置**页，选择**URL过滤箴言报**。点击**已启用**选项的单选按钮为了启用使用健康状态测试的模块。如果希望您的设置生效，您必须运用卫生政策到FireSIGHT管理中心。



- **重要告警**：如果FireSIGHT管理中心不能成功通信与或从网云获取更新，该模块更改的状态分类对*关键*。
- **警告警报**：如果FireSIGHT管理中心成功通信与网云，模块状态更改对*警告*管理中心是否不能推送新建的URL过滤数据到其受管理设备。

步骤 3：检查DNS设置

在网云查找期间， FireSIGHT管理中心与这些服务器联络：

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

一旦确保，两个服务器在防火墙允许，请运行这些on命令FireSIGHT管理中心并且验证，如果管理中心能解析名称：

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

步骤 4：检查连接到需要的端口

FireSIGHT系统使用端口443/HTTPS和80/HTTP为了与网云服务联络。

一旦确认管理中心能执行一成功的`nslookup`，请验证连接到有`telnet`端口80和端口443。而未知URL查询被执行在端口80的`service.brightcloud.com` URL数据库下载与在端口443的`database.brightcloud.com`。

```
telnet database.brightcloud.com 443
```

```
telnet service.brightcloud.com 80
```
此输出是成功的Telnet示例对database.brightcloud.com。

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

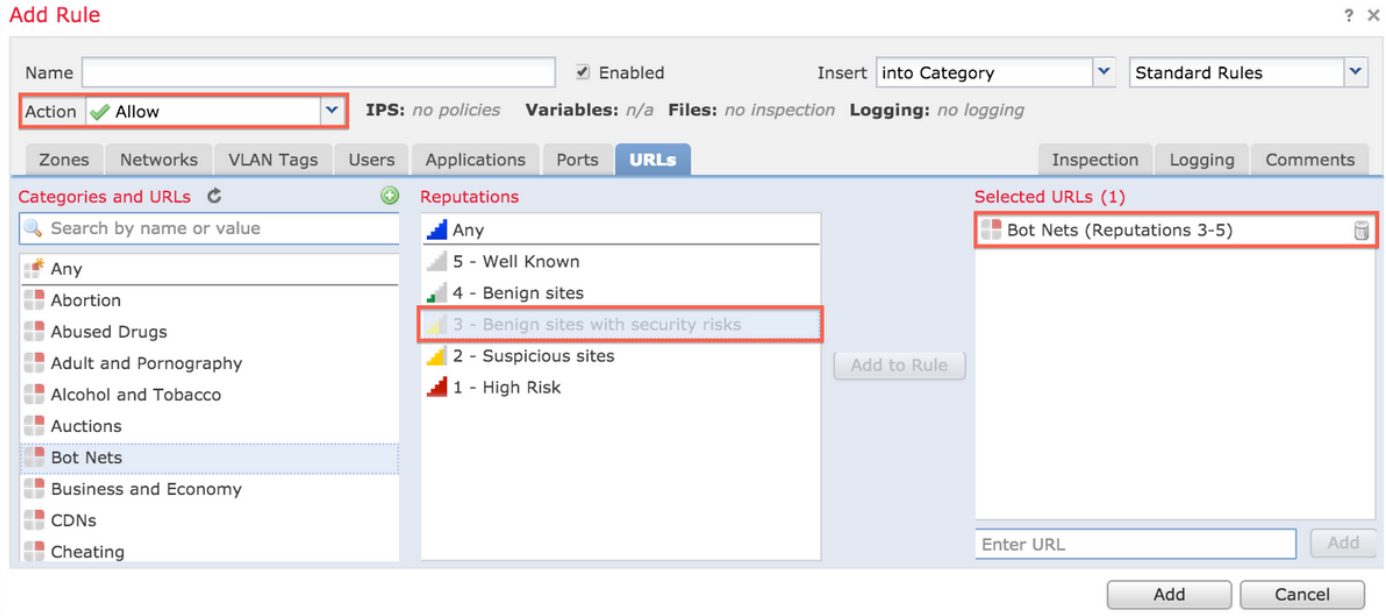
访问控制和Miscategorization问题

问题 1：与取消选择的名誉级别的URL允许/阻止

如果注意URL允许或阻塞，但是您没有选择名誉级在您的访问控制规则的该URL，阅读此部分为了知道URL过滤规则如何工作。

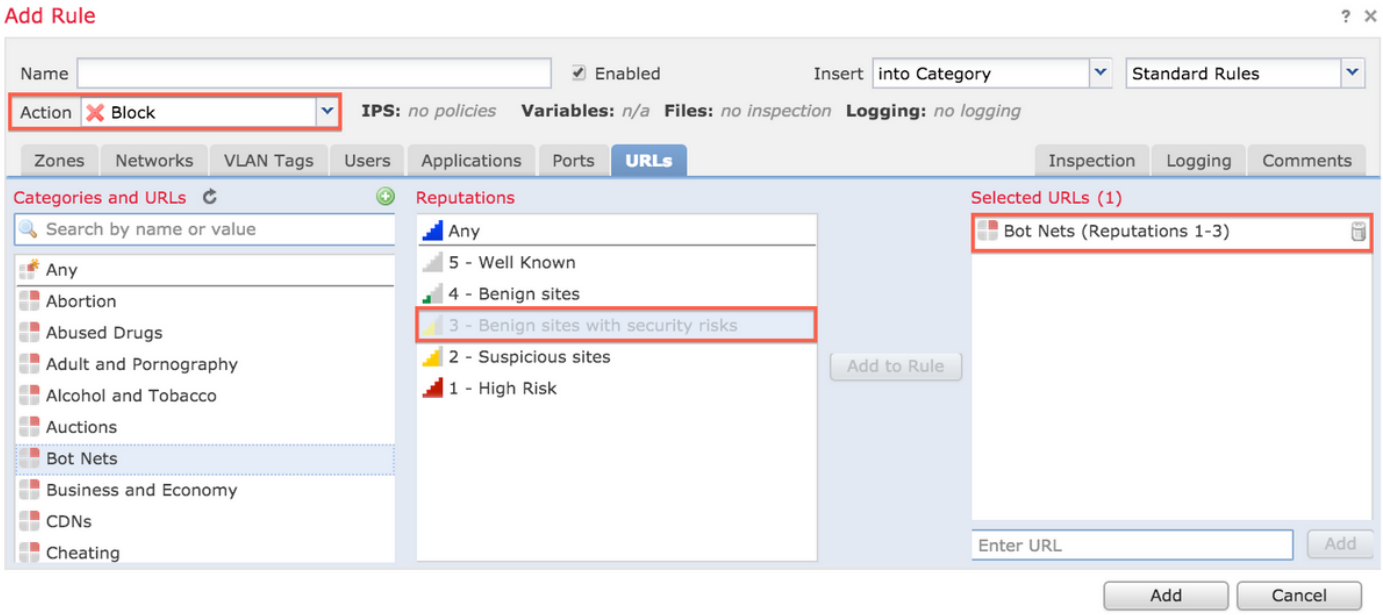
规则操作是准许

当您创建规则**允许**根据名誉级别时的流量，名誉级别的选择比您最初选择的级别也选择所有名誉级别安全的较少。例如，如果配置规则允许*有安全风险的*(级别3)*良性站点*，它自动地也允许*良性站点*(级别4)和*著名的*(级别5)站点。



规则操作是块

当您创建规则**阻塞**根据名誉级别时的流量，名誉级别的选择比您最初选择的级别也选择所有名誉级别严重。例如，如果配置规则阻塞*有安全风险的*(级别3)*良性站点*，它自动地也阻塞*可疑站点*(级别2)和*高危险*(级别1)站点。



URL选择矩阵

选定名誉级别

选定规则操作
高危险 可疑站点 有安全风险的良性站点 良性站点 著名的

1 -高危险
2 -可疑站点
3 -有安全风险的良性站点
4 -良性站点
5 -著名的

问题 2：通配符在访问控制规则不工作

FireSIGHT系统不支持一个通配符的规格在URL情况的。此情况在cisco.com也许不能警告。

```
*cisco*.com
```

另外，不完整URL也许配比导致一种不期望的结果的其他流量。当您指定在URL情况时的各自的URL，您必须认真考虑也许受影响的其他流量。例如，请考虑您要明确地阻塞cisco.com一个方案。然而，子链匹配意味着阻塞cisco.com也阻塞sanfrancisco.com，也许不是您的目的。

当您输入URL时，请输入域名并且省略子域信息。例如，请键入 cisco.com而不是 www.cisco.com。 当您在 **允许**规则时使用 cisco.com，用户可能浏览到任何这些URL ：

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

问题 3：URL类别和名誉没有填充

如果URL不在本地数据库，并且第一次是URL在流量被看到，类别或名誉也许不填充。这意味着，第一次未知URL被看到，不匹配AC规则。 有时，第一次URL被看到，通常被访问的URL的URL查找也许不解决在。此问题在版本5.3.0.3、5.3.1.2和5.4.0.2修复， 5.4.1.1。

相关信息

- URL过滤的配置在FireSIGHT系统的

- 技术支持和文档 - Cisco Systems