在WSA中定义自定义URL类别

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 允许URL
  - 创建新的自定义URL
  - 编辑全局访问策略
- 阻止URL
  - 创建新的自定义URL
  - 编辑全局访问策略

简介

本文档介绍如何定义自定义URL类别在网络安全设备(WSA)中工作。

作者：Shikha Grover，编辑者：Yeraldin Sanchez，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 初学者对思科网络安全设备的了解

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

URL所属的类别由过滤类别数据库确定。网络安全设备收集信息并为每个URL过滤引擎维护一个单独的数据库。过滤类别数据库定期从思科更新服务器接收更新，并由Cisco TALOS维护。Talos是思科的安全情报和研究小组，它不断跟踪各种属性以评估有关特定主机的结论。

有时您可能想要以不同方式对URL/域/Ip地址进行分类，并在本地设置自定义分类。您可以通过自定义URL类别实现这一点。

当URL过滤引擎将URL类别与客户端请求中的URL匹配时，它首先根据策略组中包含的自定义URL类别评估URL。如果请求中的URL与包含的自定义类别不匹配，则URL过滤引擎会将其与预定义的URL类别进行比较。

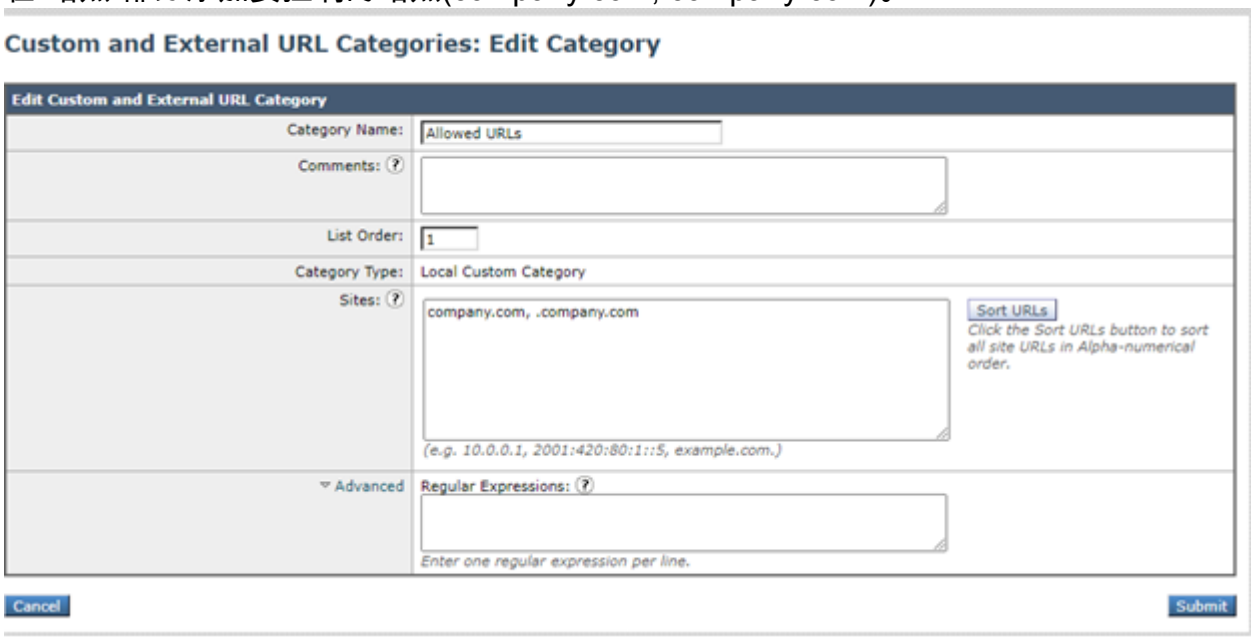
配置

允许URL

如果您信任该网站，可以通过以下过程允许它。

创建新的自定义URL

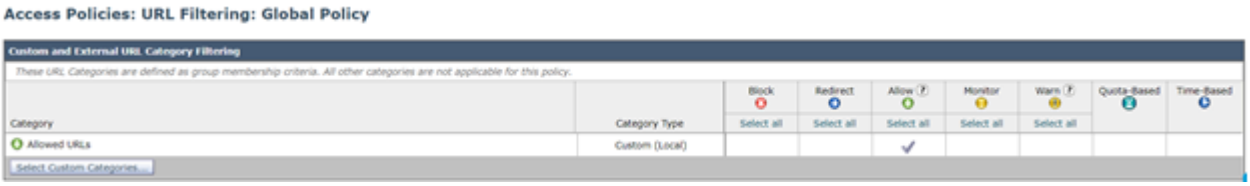
1. 创建新的自定义URL类别，导航到GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name:允许的URL。
2. 在“站点”部分添加要控制的站点(company.com,.company.com)。



3.
4. 请注意，“domain.com”将仅匹配“domain.com”，而不是www.domain.com或“host.domain.com”。为了允许站点和所有子域，在“站点”部分下需要两个条目："。domain.com, domain.com"。
5. 单击 submit。

编辑全局访问策略

1. 打开Web Security Manager > Access Policies> Global Policy > URL Filtering。
2. 点击选择自定义类别。
3. 点击Allowed URLs下拉箭头，选择Include in policy，然后点击Apply。
4. 选中“允许”复选框。
5. 单击Submit和Commit Changes。

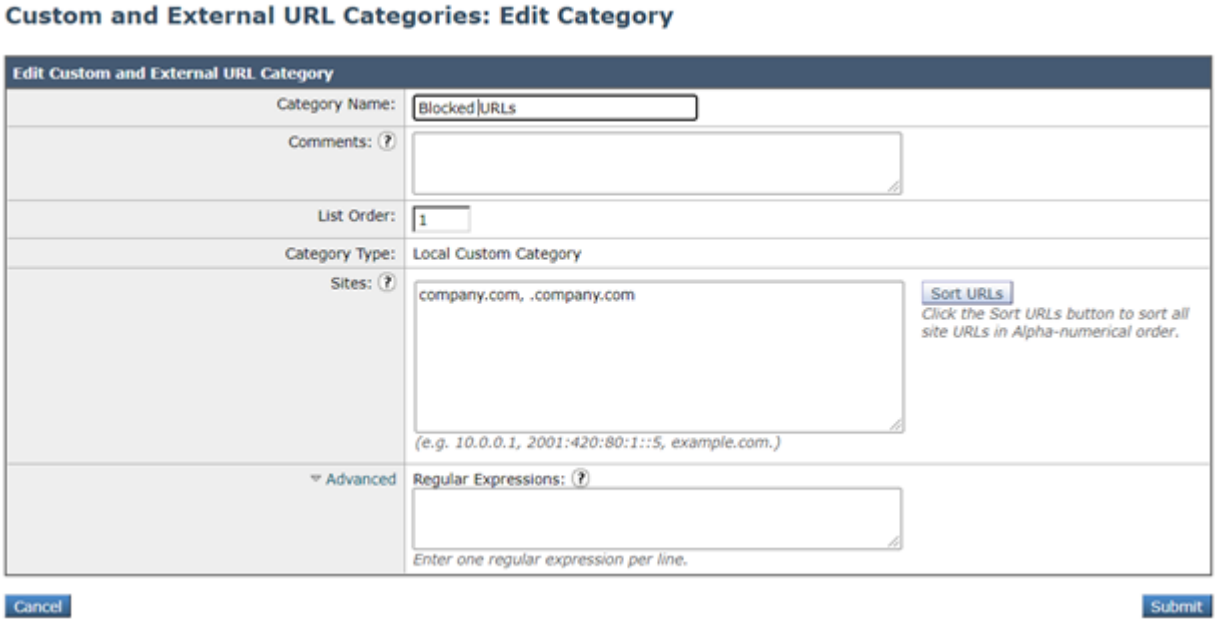


阻止URL

如果您不信任该网站，可通过以下流程将其阻止。

创建新的自定义URL

1. 创建新的自定义URL类别，导航到GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name:阻止的URL。
2. 在“站点”部分添加要控制的站点(company.com、.company.com)。



3. 请注意，“domain.com”将仅匹配“domain.com”，而不是www.domain.com或“host.domain.com”。要阻止站点和所有子域，它需要在“站点”部分下有两个条目："。domain.com, domain.com"。
4. 单击 submit。

编辑全局访问策略

1. 打开Web Security Manager > Access Policies> Global Policy > URL Filtering。
2. 单击Select Custom Categories...
3. 点击Blocked URLs下拉箭头，选择Include in policy，然后点击Apply。
4. 选中“阻止”复选框。
5. 单击Submit和Commit Changes。



注意：上述更改可以针对任何访问策略，而不仅仅是全局策略。相同的过程可以应用于解密策略。

请查看此指南，了解广泛部署的使用案例。

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）。