

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, Yeraldin Sanchez，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 初级了解思科网络安全设备

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。思科的安全情报和研究小组Talos会不断跟踪一系列广泛的属性，以评估有关给定主机的结论。

有时，您可能希望对URL/域/IP地址进行不同的分类，并在您的设备中本地自定义分类。您可以通过

自定义URL类别实现此目标。

当URL过滤引擎将URL类别与客户端请求中的URL匹配时，它首先会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

如果您信任网站，可以通过以下流程允许它。

创建新的自定义URL

1. 创建新的自定义URL类别，导航至GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name:允许的URL。
2. 在站点部分(company.com、.company.com)中添加要控制的站点。

Custom and External URL Categories: Edit Category

Category Name: Allowed URLs

Comments: ?

List Order: 1

Category Type: Local Custom Category

Sites: ? company.com, .company.com

Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Regular Expressions: ?

Enter one regular expression per line.

Cancel Submit

3. 3.
4. 请注意，“domain.com”将仅与“domain.com”匹配，而不与www.domain.com或“host.domain.com”匹配。为了允许站点和所有子域，它需要“站点”部分下的两个条目：“domain.com, domain.com”。
5. 单击“Submit”。

编辑全局访问策略

1. 打开Web安全管理器>访问策略>全局策略> URL过滤。
2. 单击“Select Custom Categories(选择自定义类别)”。
3. 单击“允许的URLs”下拉箭头，选择“在策略中包括”，然后单击“应用”。
4. 在“允许”框中加上复选标记。
5. 单击Submit和Commit Changes。

Custom and External URL Category Filtering		Block	Redirect	Allow (?)	Monitor	Warn (?)	Quota-Based	Time-Based
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Category	Category Type	Select all	Select all	Select all	Select all	Select all		
Allowed URLs	Custom (Local)			<input checked="" type="checkbox"/>				

阻止URL

如果您不信任网站,可以通过以下流程阻止它。

创建新的自定义URL

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

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:

Comments: (?)

List Order:

Category Type: Local Custom Category

Sites: (?) Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Regular Expressions: (?)
Enter one regular expression per line.

3. 请注意，“domain.com”将仅与“domain.com”匹配，而不与www.domain.com或“host.domain.com”匹配。要阻止站点和所有子域，它需要“站点”部分下的两个条目：“domain.com, domain.com”。
4. 单击“Submit”。

编辑全局访问策略

1. 打开Web安全管理器>访问策略>全局策略> URL过滤。
2. 单击“Select Custom Categories...(选择自定义类别.....)”
3. 单击“Blocked URLs”下拉箭头，选择“Include in policy”，然后单击“Apply”。
4. 在“阻止”(Block)的框中加上复选标记。
5. 单击“提交并提交更改”。

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering								
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.								
Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
Blocked URLs	Custom (Lock)	Select all <input checked="" type="checkbox"/>	Select all <input type="checkbox"/>	Select all <input type="checkbox"/>	Select all <input type="checkbox"/>	Select all <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Select Custom Categories...](#)

注意：上述更改可以对任何访问策略进行，而不只是全局策略。同样的过程也可应用于解密策略。

请查看本[指南](#)，了解广泛部署的使用案例。