

在CSF中排除故障并验证URL类别

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[背景信息](#)

[架构](#)

[步骤 1：在FMC中查找URL类别](#)

[步骤 2：查看URL过滤集成设置](#)

[步骤 3：使用系统支持跟踪确认设备上的URL类别](#)

[步骤 4：将类别编号解析为类别名称](#)

[验证](#)

[争议按钮](#)

[故障排除](#)

简介

本文档介绍如何验证安全防火墙和FMC上的URL类别分配，以确保设备使用相同的URL分类。

先决条件

您必须为设备启用URL过滤许可证，云服务集成处于正常状态，且访问控制策略包含URL过滤并在配置URL条件后已部署。

要求

Cisco 建议您了解以下主题：

- Firepower管理中心(FMC)URL过滤和类别查找
- 思科安全防火墙(CSF)流量检测和策略评估
- URL分类和信誉行为，基于Talos，从CSF版本6.5开始

使用的组件

本文档介绍思科安全防火墙和FMC版本6.5及更高版本中可用的功能。本指南中的示例使用7.6.5版。

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。

相关产品

本文档还可用于以下产品和版本：

- Secure Firewall Management Center (FMC)
- 思科安全防火墙(CSF)
- URL过滤和云服务集成

背景信息

URL过滤依赖于在流量检测期间评估的类别数据库。FMC存储目标的URL类别信息，并且设备会在检查流量时执行运行时查找。当FMC、设备或云数据库之间不匹配时，即使访问控制策略配置正确，策略结果也可能不一致。

验证的一个重要部分是确认URL类别分配在FMC和设备之间是一致的。URL类别查找受云服务集成设置和设备缓存的影响。如果缓存刷新设置被禁用或条目生命周期过长，则在Talos更新分类后，旧类别数据可以继续使用。

架构

启用URL过滤时，设备首先检查本地URL缓存。如果缓存中不存在该类别，则设备可以查询本地数据库或思科云。设备在检测期间使用其本地URL数据库和查找缓存，并且与Talos通信以下载和更新URL过滤数据。在FMC管理的设备上，beakerd在FMC上运行，并在CSF上处于等待状态。如果CSF在本地进行管理，则进程在设备本身上运行。

Talos发送多个大小的完整数据库包，这些数据库包存储在/var/sf/cloud_download/cisco下。

以下是Talos中的数据库文件可能具有的一些示例：

- cisco_uridb_large_1541554243(500 MB)
- cisco_uridb_medium_1541553645(125 MB)
- cisco_uridb_small_1541553061(33 MB)



注意：数据库文件以cisco_uridb开头，然后列出大小（小、中或大）。大小因使用的硬件而异。

步骤 1：在FMC中查找URL类别

FMC维护本地URL数据库，该数据库将URL目标映射到其分配的类别。这是验证URL分类方式时建议采取的第一步。

在FMC中导航至位置Analysis > Advanced > URL。

输入要调查的URL，并查看其分配的类别。

在下面显示的示例中，www.cisco.com列在“Computers and Internet”类别下。

步骤 2：查看URL过滤集成设置

URL过滤集成设置确定FMC和CSF设备从何处获取其URL类别数据库。每台设备维护自己的本地数据库以进行URL查找，并可查询思科云以获取其他或更新的URL情报。

在FMC中导航到集成>其他集成>云服务以查看这些设置。

URL Filtering

Last URL Filtering Update: 2026-08-26 10:28:52 [Update Now](#)

Enable Automatic Updates

URL Query Source

☐ Local Database Only

☒ Local Database and Cisco Cloud

☐ Cisco Cloud Only

Cached URLs Expire

After 2 hours

[Dispute URL categories and reputations](#)

Save

验证集成是否正常以及URL查找缓存是否配置为根据预期策略计时进行刷新。



警告：URL查找缓存可以保留先前检索的类别和信誉结果。如果缓存过期被禁用或配置了较长的生存期，设备可以在Talos更新分类后继续使用缓存信息，这可能导致设备结果与当前FMC或Talos查找暂时不同。

步骤 3：使用系统支持跟踪确认设备上的URL类别

要验证CSF设备对URL的分类方式是否与FMC相同，请从设备CLI运行system support trace。这显示了Snort检测引擎如何评估流量，以及在检测连接时返回的URL类别。

在FTD CLI中，输入system support trace命令并响应交互式提示：

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```



注意：在本示例中，173.37.145.84是www.cisco.com的IP地址。使用与您正在调查的URL对应的目标IP地址。

示例输出：

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 2003
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90, 2003
```

在此输出中，URL返回类别ID 2003。下一步说明如何将该数值解析为相应的类别名称。

步骤 4：将类别编号解析为类别名称

设备上的URL类别查找返回数字类别ID。要将该编号映射到人类可读的类别名称，请在设备上打开aup_categories.json文件。

在专家模式下导航到CSF上的/var/sf/cloud_download/目录。确保您处于根用户模式。

打开类别定义文件：

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

搜索跟踪输出中返回的类别ID。类别2003的条目示例：

```
{
  "id": 2003,
  "uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
  "mnemonic": "comp",
  "name": "Computers and Internet",
```

```
"type": "aup_cats",
"state": "active"
}
```



注意：所有CSF设备的类别ID号一致。在每个CSF设备上，相同的数字ID映射到相同的类别名称。

验证

使用步骤1至4的输出确认FMC数据库与设备上的Snort引擎之间的URL类别分配是一致的。

在本例中：

- FMC数据库将www.cisco.com列为Computers and Internet。
- 设备CLI返回类别ID 2003，该类别映射到“计算机”和“互联网”。

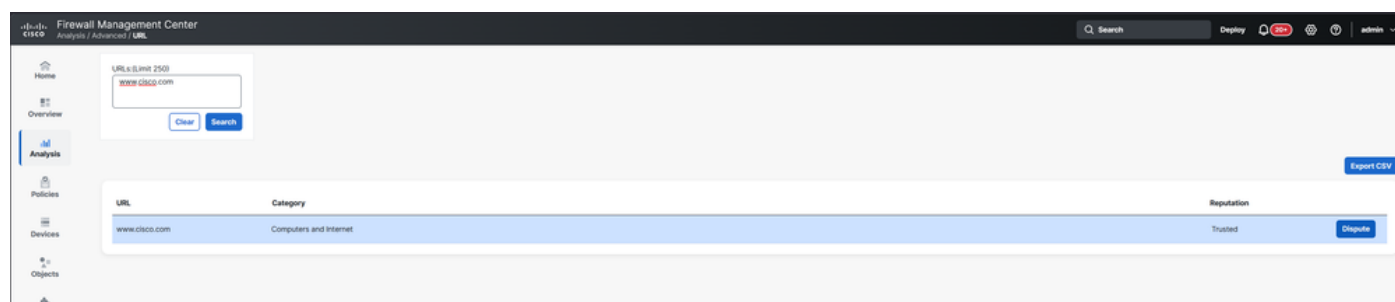
两个来源都同意，这证实了所应用的URL过滤策略对于此URL是一致的。

争议按钮

如果您认为某个URL被归类为不正确的类别，您可以向Talos提交争议。

在FMC中导航到分析>高级> URL：

键入URL，单击Search，然后将鼠标悬停在URL条目上，然后选择Disrupt。



这将打开Talos争议页面，以便适当的来源可以审核和更正分类。

故障排除

如果分类与预期不符，请查看以下方面：

- 确认已启用URL过滤许可证并已将其分配给设备。
- 验证云服务的运行状况和与Talos的连接。
- 检查设备缓存和缓存刷新设置，确认过时条目不会被重复使用。
- 检查FMC上是否正在为FMC管理的设备运行Beakerd进程。

对于FMC管理的设备，请在FMC专家模式下运行此命令以确认进程处于活动状态：

```
pmtool status | grep beakerd
```



注意：如果在由FMC管理的安全防火墙中运行此命令，则进程在等待状态下可见。如果安全防火墙在本地进行管理，则进程处于运行状态。

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）。