

在安全Web设备中配置自定义URL类别

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[自定义URL类别](#)

[实时源URL类别](#)

[创建自定义URL类别的步骤](#)

[定义使用正则表达式](#)

[限制和设计问题](#)

[在策略中使用自定义URL类别](#)

[为访问策略配置URL过滤器的步骤](#)

[为解密策略配置URL过滤器的步骤](#)

[为数据安全策略组配置URL过滤器的步骤](#)

[配置使用自定义URL类别控制上传请求的步骤](#)

[在外部DLP策略中配置控制上传请求的步骤](#)

[旁路和直通URL](#)

[为Web请求配置Web代理旁路](#)

[报告](#)

[查看访问日志中的自定义URL类别](#)

[故障排除](#)

[类别不匹配](#)

[参考](#)

简介

本文档介绍安全网络设备(SWA)中的自定义统一资源定位符(URL)类别的结构。

先决条件

要求

Cisco 建议您了解以下主题：

- 代理的工作原理。
- 安全网络设备(SWA)管理。

Cisco 建议您：

- 已安装物理或虚拟安全网络设备(SWA)。

- 许可证已激活或已安装。
- 安装向导已完成。
- 对SWA的管理权限。

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。

自定义URL类别

URL过滤引擎允许您过滤访问、解密和数据安全策略中的事务。为策略组配置URL类别时，可以为自定义URL类别（如果定义了任何类别）和预定义URL类别配置操作。

您可以创建描述特定主机名和Internet协议(IP)地址的自定义和外部实时源URL类别。此外，还可以编辑和删除URL类别。

当将这些自定义URL类别包含在同一个访问、解密或思科数据安全策略组中，并向每个类别分配不同的操作时，包含级别较高的自定义URL类别的操作优先。

 **注意：**如果域名系统(DNS)将多个IP解析到某个网站，并且如果其中一个IP是自定义阻止列表，则网络安全设备会阻止所有IP的网站，无论这些IP是否在自定义阻止列表中列出。

实时源URL类别

外部实时源类别用于提取来自特定站点的URL列表，例如从Microsoft获取Office 365 URL。

如果在创建和编辑自定义和外部URL类别时为“类别类型”选择“外部动态源类别”，则必须选择源格式（思科源格式或Office 365源格式），然后提供到相应源文件服务器的URL。

以下是每个源文件的预期格式：

- 思科源格式 -必须是逗号分隔值(.csv)文件；即扩展名为.csv的文本文件。.csv文件中的每个条目都必须位于单独的行上，格式设置为地址/逗号/地址类型（例如：www.cisco.com, site或ad2.*\com, regex)。有效地址类型为站点和正则表达式。

下面是摘自思科源格式.csv文件的摘要：

```
www.cisco.com,site
\.xyz,regex
ad2.*\com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Office 365源格式 -这是一个XML文件，位于Microsoft Office 365服务器或您保存文件的本地服务器上。它由Office 365服务提供，无法修改。

文件中的网络地址由XML标记括起来，此结构为：products > product > address list > address。在当前实现中，“地址列表类型”可以是IPv6、IPv4或URL [其中可以包括域和正则表达式(regex)模式]。

以下是Office 365源文件的代码段：

```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
</products>
```

 注意：请勿将http://或https://作为任何站点条目的一部分包括在文件中，否则会发生错误。换句话说，www.cisco.com被正确分析，而<http://www.cisco.com>产生错误

创建自定义URL类别的步骤

步骤1: 依次选择Web Security Manager > Custom and External URL Categories。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention


Web Traffic Tap Policies

SOCKS Policies

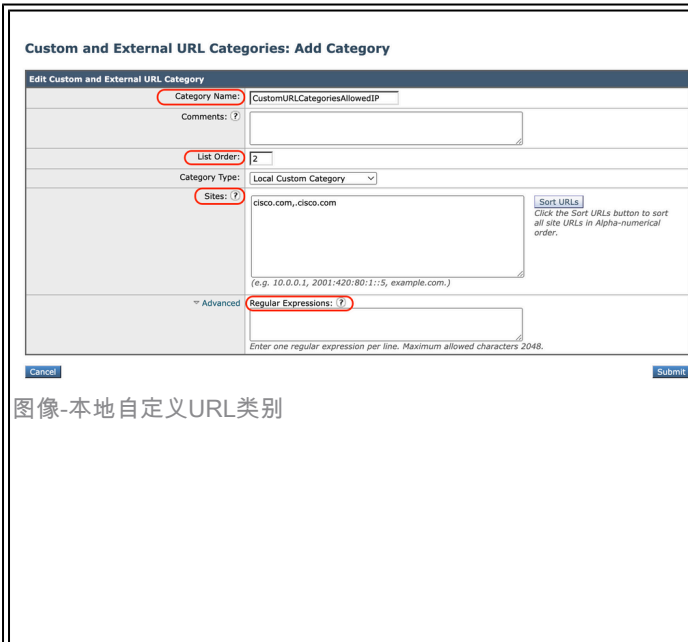
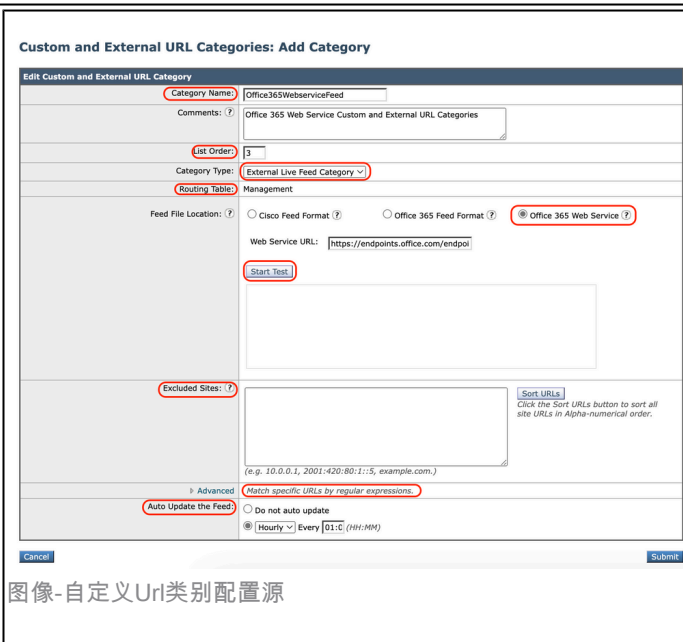
Custom Policy Elements

Custom and External URL Categories

URL过滤引擎根据自定义URL类别按指定顺序评估客户端请求。

 注意：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。如果URL不匹配任何包含的自定义或预定义的URL类别，则请求会取消分类。


- Category Type：选择Local Custom Category或External Live Feed Category。
- 路由表：选择管理或数据。此选项仅在启用“拆分路由”时可用；也就是说，它不适用于本地自定义类别。

 <p>图像-本地自定义URL类别</p>	 <p>图像-自定义Url类别配置源</p>
本地自定义类别	外部实时源类别


定义使用正则表达式


安全网络设备使用的正则表达式语法与其他Velocity模式匹配引擎实现所使用的正则表达式语法略有不同。

此外，设备不支持使用反斜杠转义正斜杠。如果您需要在正则表达式中使用正斜杠，只需键入正斜杠而不使用反斜杠。

 注意：严格来说，AsyncOS for Web使用Flex正则表达式分析器


要测试正则表达式，您可以使用此链接：[flex lint - Regex测试器/调试器](#)

 注意：返回超过63个字符的正则表达式失败并产生无效条目错误。请务必形成不可能返回63个字符以上的正则表达式

 注意：执行大量字符匹配的正则表达式会消耗资源并可能影响系统性能。因此，可以谨慎应用正则表达式。


您可以在以下位置使用正则表达式：

- 访问策略的自定义URL类别。创建用于访问策略组的自定义URL类别时，可以使用正则表达式指定与输入模式匹配的多个Web服务器。
- 要阻止的自定义用户代理。编辑访问策略组要阻止的应用时，可以使用正则表达式输入要阻止的特定用户代理。

 提示：不能为正则表达式设置Web代理绕行。

以下是Flex正则表达式中的字符类列表

字符类	
.	除换行符以外的任何字符
\w \d \s	单词、数字、空格
\W \D \S	不是单词、数字、空格
[abc]	任何a、b或c
[^abc]	不是a、b或c
[a-g]	a与g之间的字符
锚点	
^abc\$	字符串的开始/结束
\b	字边界
转义字符	
\. * \	转义的特殊字符
\t \n \r	制表符、换行符、回车符
\u00A9	unicode转义©
组和环顾	
(abc)	捕获组
\1	返回组#1引用
(? : abc)	非捕获组
(?=abc)	正面展望
(?!abc)	负面展望
量词和替代词	
a* a+ a?	0或更多、1或更多、0或1
a{5} a{2 , }	恰好五、二或更多
a{1,3}	1到3之间
a+? a{2 , }?	匹配尽可能少
ab cd	match ab或cd

 注意：请注意长模式中的非转义点，特别是在较长模式的中间，并注意此元字符（星号*），尤其是与点字符结合使用。任何模式都包含一个未转义的点，该点在禁用后返回超过63个字符。

始终转义*(star)和。(点)加上\ (反斜线)*和\。

如果在正则表达式中使用.cisco.local，则域Xcisco.local也是一个匹配项。

非转义字符会影响性能，而且会导致Web浏览速度变慢。这是因为模式匹配引擎必须经历数千或数百万种可能性，直到找到正确条目的匹配项，并且它可能会对允许的策略的类似URL产生一些安全隐患

可以使用命令行界面(CLI)选项advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex, to enable or disable default regex conversion to lower case for case-insensitive matches。如果存在区分大小写的问题，请使用。

限制和设计问题

- 这些URL类别定义中只能使用30个外部实时源文件，并且每个文件包含的条目不能超过5000个。
- 如果外部馈送条目数增加，则会导致性能下降。
- 可以在多个自定义URL类别中使用相同的地址，但所列类别的顺序是相关的。

如果将这些类别包括在同一策略中，并为每个类别定义不同的操作，则会应用为自定义URL类别表中列出的最高类别定义的操作。

- 当本地文件传输协议(FTP)请求透明地重定向到FTP代理时，它不包含FTP服务器的主机名信息，只包含其IP地址。

因此，某些仅包含主机名信息的预定义URL类别和Web信誉过滤器与本地FTP请求不匹配，即使请求发往这些服务器。

如果要阻止对这些站点的访问，必须创建自定义URL类别，使它们使用其IP地址。

- 未分类的URL是不匹配任何预定义URL类别或包括的自定义URL类别的URL

在策略中使用自定义URL类别

URL过滤引擎允许您过滤访问、解密和数据安全策略中的事务。为策略组配置URL类别时，可以为自定义URL类别（如果定义了任何类别）和预定义URL类别配置操作。

为访问策略配置URL过滤器的步骤

步骤1: 选择网络安全管理器>访问策略。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

操作	描述
阻止	Web代理拒绝与此设置匹配的事务。
重定向	将最初发往此类别中URL的流量重定向到您指定的位置。选择此操作后，系统将显示Redirect To字段。输入要将所有流量重定向到的URL。
允许	始终允许此类别中网站的客户端请求。 允许的请求会绕过所有进一步的过滤器和恶意软件扫描。 仅将此设置用于受信任的网站。您可以将此设置用于内部站点。
监控	Web代理既不允许也不阻止请求。相反，它会继续根据其他策略组控制设置（如Web信誉过滤器）评估客户端请求。
警告	Web代理最初会阻止请求并显示警告页面，但允许用户通过点击警告页面中的超文本链接继续操作。
基于配额的	当单个用户接近您指定的数量或时间配额时，会显示警告。达到配额时，将显示阻止页面。
基于时间的	Web代理在您指定的时间范围内阻止或监控请求。

第 5 步：在Predefined URL Category Filter部分中，为每个类别选择以下操作之一：

- 使用全局设置
- 监控
- 警告
- 阻止
- 基于时间的
- 基于配额的

Predefined URL Category Filtering						
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.						
Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.						
Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
Animals and Pets	Select all	Select all	Select all	Select all		
Arts			✓			
Predefined Quota Profile: 10GBdailyLimit Astrology In time range: MorningShift Action: Warn Otherwise: Block					✓	
						✓

图像-为预定义类别选择操作

步骤 6 在未分类 URL 部分中，选择要对不属于预定义或自定义 URL 类别的网站的客户端请求采取的操作。此设置还确定由 URL 类别集更新产生的新的和合并的类别的默认操作。

Uncategorized URLs	
Specify an action for urls that do not match any category.	
Uncategorized URLs:	Monitor
Default Action for Update Categories: ?	Most Restrictive

图像-为未分类的 URL 选择操作

步骤 7. 提交并确认更改。

为解密策略配置 URL 过滤器的步骤

步骤 1: 选择网络安全管理器 > 解密策略。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

操作	描述
通过	通过客户端和服务端之间的连接，而不检查流量内容。
监控	Web代理既不允许也不阻止请求。相反，它会继续根据其他策略组控制设置（如Web信誉过滤器）评估客户端请求。
解密	允许连接，但检查流量内容。设备解密流量并将访问策略应用于已解密流量，就好像它是纯文本超文本传输协议(HTTP)连接一样。当连接已解密且访问策略已应用时，您可以扫描流量中的恶意软件。
丢弃	丢弃连接，并且不将连接请求传递给服务器。设备不会通知用户已断开连接。

第五步：在未分类 URL 部分中，选择要对不属于预定义或自定义 URL 类别的网站的客户端请求采取的操作。

此设置还确定由 URL 类别集更新产生的新的和合并的类别的默认操作。

图像-未分类解密策略

步骤 6 提交并确认更改。

⚠ 注意：如果要阻止超文本传输协议安全(HTTPS)请求的特定URL类别，请选择对“解密策略”(Decryption Policy)组中的该URL类别进行解密，然后选择阻止访问策略组中的同一URL类别。

为数据安全策略组配置URL过滤器的步骤

步骤1: 选择Web Security Manager > Cisco Data Security。

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies




Custom Policy Elements

Custom and External URL Categories

操作	描述
允许	始终允许此类别网站的上传请求。仅适用于自定义URL类别。 允许的请求会绕过所有进一步的数据安全扫描，并根据访问策略评估该请求。 仅将此设置用于受信任的网站。您可以将此设置用于内部站点。
监控	Web代理既不允许也不阻止请求。相反，它会继续根据其他策略组控制设置（例如Web信誉过滤器）评估上传请求。
阻止	Web代理拒绝与此设置匹配的事务。

第 5 步：在Predefined URL Category Filtering部分中，为每个类别选择以下操作之一：

- 使用全局设置
- 监控
- 阻止

Predefined URL Category Filtering		
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.		
Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.		
Category	Use Global Settings	Override Global Settings
		Monitor 
	Select all	Select all
 Hunting		<input checked="" type="checkbox"/> <input type="checkbox"/>
 Illegal Activities		<input type="checkbox"/> <input checked="" type="checkbox"/>

图像-数据安全预定义URL选择操作


步骤 6 在未分类 URL 部分中，选择要对不属于预定义或自定义URL类别的网站的上传请求采取的操作。

此设置还确定由URL类别集更新产生的新的和合并的类别的默认操作。

Uncategorized URLs	
Specify an action for urls that do not match any category.	
Uncategorized URLs:	<input type="text" value="Block"/>
Default Action for Update Categories: (?)	<input type="text" value="Least Restrictive"/>

图像-未分类的数据安全

步骤 7. 提交并确认更改。

 注意：如果不禁用最大文件大小限制，网络安全设备将在URL过滤中选择“允许”(Allow)或“监控”(Monitor)选项后继续验证最大文件大小。

配置使用自定义URL类别控制上传请求的步骤

每个上传请求都分配给“出站恶意软件扫描”策略组，并继承该策略组的控制设置。

Web代理收到上传请求报头后，它拥有必要的信息，可以确定它是否必须扫描请求正文。

DVS引擎扫描请求并将判定返回到Web代理。如果适用，阻止页面将会显示给最终用户。

第 1 步	选择网络安全管理器>出站恶意软件扫描。								
步骤 2	在目标列中，点击要配置的策略组的链接。								
步骤 3	在编辑目标设置部分，从下拉菜单中选择定义目标扫描自定义设置。								
步骤 4	在要扫描的目标部分，选择以下选项之一： <table border="1"><thead><tr><th>选项</th><th>描述</th></tr></thead><tbody><tr><td>不扫描任何上传</td><td>DVS引擎不扫描任何上传请求。根据访问策略评估所有上传请求</td></tr><tr><td>扫描所有上传</td><td>DVS引擎扫描所有上传请求。上传请求会根据访问策略被阻止或评估，具体取决于DVS引擎扫描判定</td></tr><tr><td>扫描上传到指定的自定义URL类别</td><td>DVS引擎扫描属于特定自定义URL类别的上传请求。上传请求根据访问策略被阻止或评估，具体取决于DVS引擎扫描判定。 点击编辑自定义类别列表以选择要扫描的URL类别</td></tr></tbody></table>	选项	描述	不扫描任何上传	DVS引擎不扫描任何上传请求。根据访问策略评估所有上传请求	扫描所有上传	DVS引擎扫描所有上传请求。上传请求会根据访问策略被阻止或评估，具体取决于DVS引擎扫描判定	扫描上传到指定的自定义URL类别	DVS引擎扫描属于特定自定义URL类别的上传请求。上传请求根据访问策略被阻止或评估，具体取决于DVS引擎扫描判定。 点击编辑自定义类别列表以选择要扫描的URL类别
选项	描述								
不扫描任何上传	DVS引擎不扫描任何上传请求。根据访问策略评估所有上传请求								
扫描所有上传	DVS引擎扫描所有上传请求。上传请求会根据访问策略被阻止或评估，具体取决于DVS引擎扫描判定								
扫描上传到指定的自定义URL类别	DVS引擎扫描属于特定自定义URL类别的上传请求。上传请求根据访问策略被阻止或评估，具体取决于DVS引擎扫描判定。 点击编辑自定义类别列表以选择要扫描的URL类别								
步骤 5	提交您的更改。								
步骤 6	在防恶意软件过滤列中，点击策略组的链接。								
步骤 7	在Anti-Malware Settings部分中，选择Define Anti-Malware Custom Settings。								

步骤 8	在Cisco DVS Anti-Malware Settings部分，选择要为此策略组启用的防恶意软件扫描引擎。
步骤 9	在恶意软件类别部分，选择是监控还是阻止各种恶意软件类别。 此部分列出的类别取决于您启用的扫描引擎。
步骤 10	提交并确认更改。

在外部DLP策略中配置控制上传请求的步骤

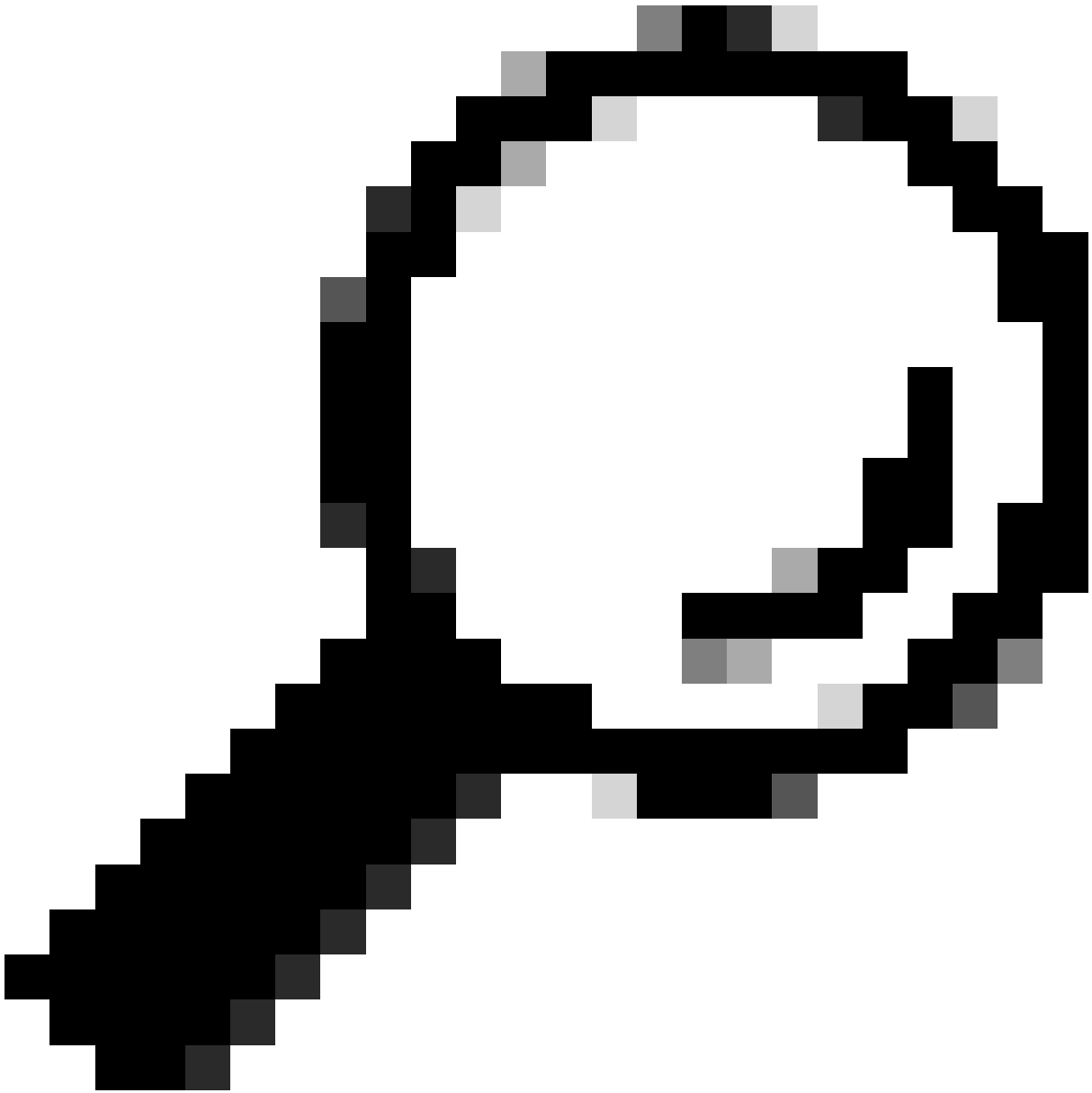
Web代理收到上传请求报头后，它便拥有了必要的信息，可以确定该请求是否可以转到外部DLP系统进行扫描。

DLP系统扫描请求并将判定返回到Web代理，阻止或监控（根据访问策略评估请求）。

第 1 步	选择网络安全管理器 > 外部防数据丢失。
步骤 2	点击要配置的策略组的Destinations列下的链接。
步骤 3	在Edit Destination Settings部分下，选择“Define Destinations Scanning Custom Settings”。
步骤 4	<p>在要扫描的目标部分，选择以下选项之一：</p> <ul style="list-style-type: none"> • 不扫描任何上传。不会将任何上传请求发送到已配置的数据丢失防护(DLP)系统进行扫描。所有上传请求都将根据访问策略进行评估。 • 扫描所有上传。所有上传请求都将发送到已配置的DLP系统进行扫描。上传请求会被阻止或根据访问策略进行评估，具体取决于DLP系统扫描判定。 • 扫描除了指定的自定义和外部URL类别以外的上传。DLP扫描策略中排除属于特定自定义URL类别的上传请求。点击编辑自定义类别列表以选择要扫描的URL类别。
步骤 5	提交并确认更改。

旁路和直通URL

您可以在透明代理实施中配置安全Web设备，以绕过来自特定客户端或特定目标的HTTP或HTTPS请求。



提示：对于需要流量通过设备的应用，无需对目标服务器进行任何修改或证书检查，即可使用直通

⚠ 注意：域映射功能在HTTPS透明模式下工作。在显式模式中，此功能不适用于HTTP流量。

- 必须配置本地自定义类别(Local Custom Category)以允许流量使用此功能。
- 启用此功能后，它会根据域映射中配置的服务器名称修改或分配服务器名称，即使服务器名称指示(SNI)信息可用也是如此。
- 如果流量与域映射匹配且配置了相应的自定义类别、解密策略和直通操作，则此功能不会根据域名阻止流量。

- 身份验证不使用此直通功能。身份验证需要解密，但在此情况下，流量不会被解密。
- 流量不受监控。您必须将UDP数据流配置为不到达网络安全设备，而是必须直接通过防火墙到达Internet（针对WhatsApp、Telegram等应用）。
- WhatsApp、Telegram和Skype在透明模式下工作。但是，由于对应用的限制，WhatsApp等一些应用在“显式”模式下无法工作。

确保您为需要将流量传递到特定服务器的设备定义了标识策略。具体来说，您必须：

- 选择Exempt from authentication/identification。
- 指定必须应用此标识配置文件的地址。您可以使用IP地址、无类域间路由(CIDR)块和子网。


第 1 步	启用HTTPS代理。						
步骤 2	<p>选择网络安全管理器 > 域映射。</p> <ol style="list-style-type: none"> 选择添加域。 输入域名或目标服务器。 如果指定了某些域，请选择优先级的顺序。 输入IP地址。 单击“Submit”。 						
步骤 3	<p>选择网络安全管理器 > 自定义和外部URL类别。</p> <ol style="list-style-type: none"> 选择Add Category。 提供这些信息。 <table border="1" data-bbox="336 1536 1484 2051"> <thead> <tr> <th data-bbox="336 1536 464 1653">设置</th> <th data-bbox="464 1536 1484 1653">描述</th> </tr> </thead> <tbody> <tr> <td data-bbox="336 1653 464 1816">类别名称</td> <td data-bbox="464 1653 1484 1816">输入此URL类别的标识符。为策略组配置URL过滤器时，会显示此名称。</td> </tr> <tr> <td data-bbox="336 1816 464 2051">列表顺序</td> <td data-bbox="464 1816 1484 2051">指定此类别在自定义URL类别列表中的顺序。为列表中的第一个URL类别输入“1”。 URL过滤引擎根据自定义URL类别按指定顺序评估客户端请求。</td> </tr> </tbody> </table>	设置	描述	类别名称	输入此URL类别的标识符。为策略组配置URL过滤器时，会显示此名称。	列表顺序	指定此类别在自定义URL类别列表中的顺序。为列表中的第一个URL类别输入“1”。 URL过滤引擎根据自定义URL类别按指定顺序评估客户端请求。
设置	描述						
类别名称	输入此URL类别的标识符。为策略组配置URL过滤器时，会显示此名称。						
列表顺序	指定此类别在自定义URL类别列表中的顺序。为列表中的第一个URL类别输入“1”。 URL过滤引擎根据自定义URL类别按指定顺序评估客户端请求。						


	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%; text-align: center;">设置</th> <th style="text-align: center;">描述</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">类别类型</td> <td>选择Local Custom Category。</td> </tr> <tr> <td style="text-align: center;">高级</td> <td>您可以在此部分输入正则表达式，以指定其他地址集。 可以使用正则表达式指定多个匹配所输入模式的地址。</td> </tr> </tbody> </table> <p>c. 提交并确认更改。</p>	设置	描述	类别类型	选择Local Custom Category。	高级	您可以在此部分输入正则表达式，以指定其他地址集。 可以使用正则表达式指定多个匹配所输入模式的地址。
设置	描述						
类别类型	选择Local Custom Category。						
高级	您可以在此部分输入正则表达式，以指定其他地址集。 可以使用正则表达式指定多个匹配所输入模式的地址。						
<p>步骤 4</p>	<p>选择网络安全管理器 > 解密策略。</p> <ol style="list-style-type: none"> a. 创建新的解密策略。 b. 选择您为特定应用绕过HTTPS流量创建的标识配置文件。 c. 在高级面板中，单击URL类别链接。 d. 在Add列中，点击以添加在步骤3中创建的自定义URL类别。 e. 选择Done。 f. 在“解密策略”页中，单击URL过滤链接。 g. 选择Pass Through。 h. 提交并确认更改。 <p>(可选) 您可以使用%(格式说明符查看访问日志信息。</p>						

为Web请求配置Web代理旁路

将自定义URL类别添加到代理绕行列表后，系统会为源和目标绕行自定义URL类别的所有IP地址和域名。

<p>第 1 步</p>	<p>选择网络安全管理器>绕行设置。</p>
<p>步骤 2</p>	<p>单击Edit Bypass Settings。</p>
<p>步骤 3</p>	<p>输入要绕过Web代理的地址。</p>

	 注意：将/0配置为旁路列表中的任何IP的子网掩码时，设备会绕过所有网络流量。在这种情况下，设备会将配置解释为0.0.0.0/0。
步骤 4	选择要添加到代理绕行列表的自定义URL类别。
步骤 5	提交并确认更改。

 注意：无法为正则表达式设置Web代理绕行。

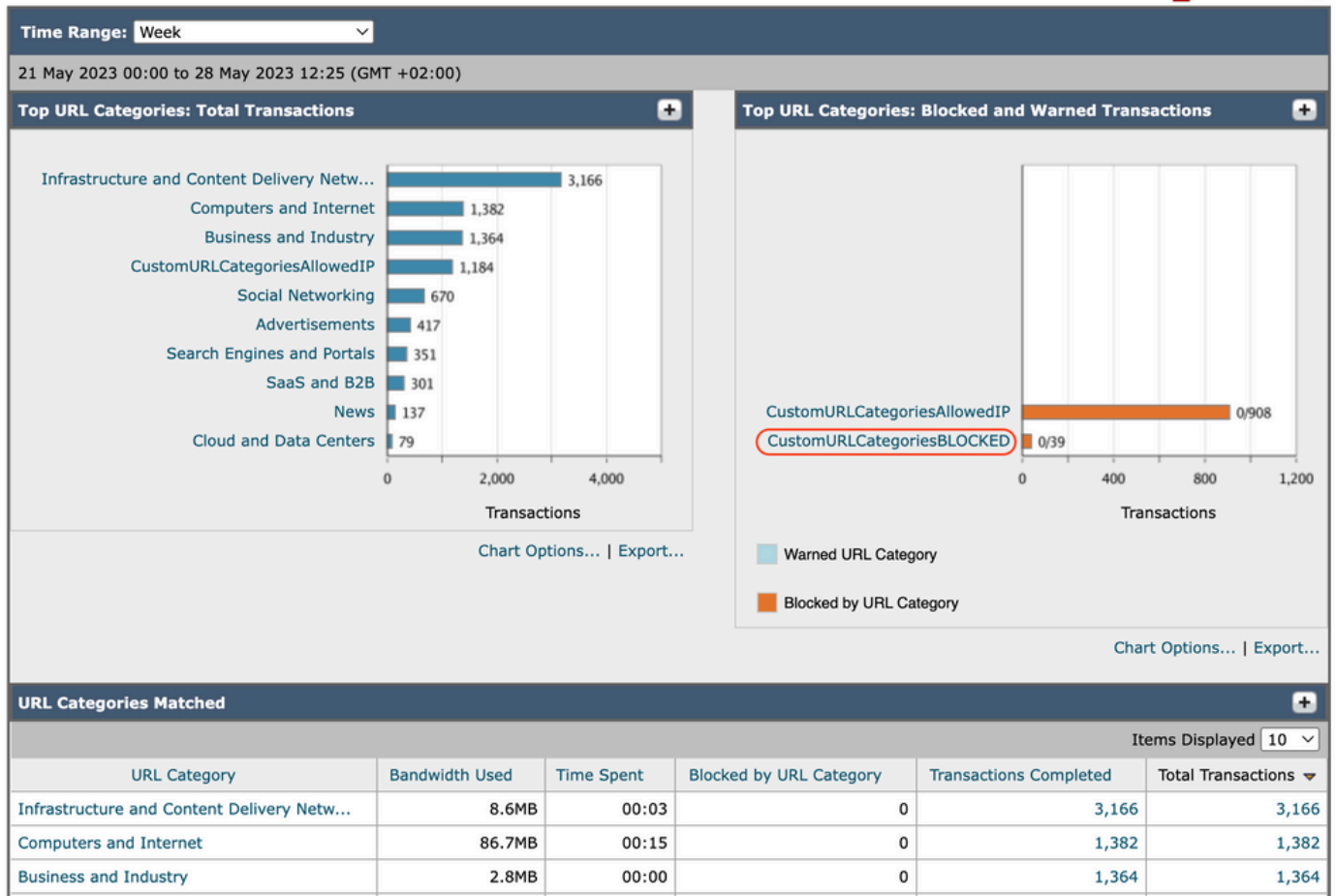
报告

在“报告”(Reporting) >>“URL类别”(URL Categories)页面中，会显示URL统计信息的综合显示，其中包括有关匹配的排名靠前的URL类别和阻止的排名靠前的URL类别的信息。

此页显示带宽节省和网络事务的特定类别数据。

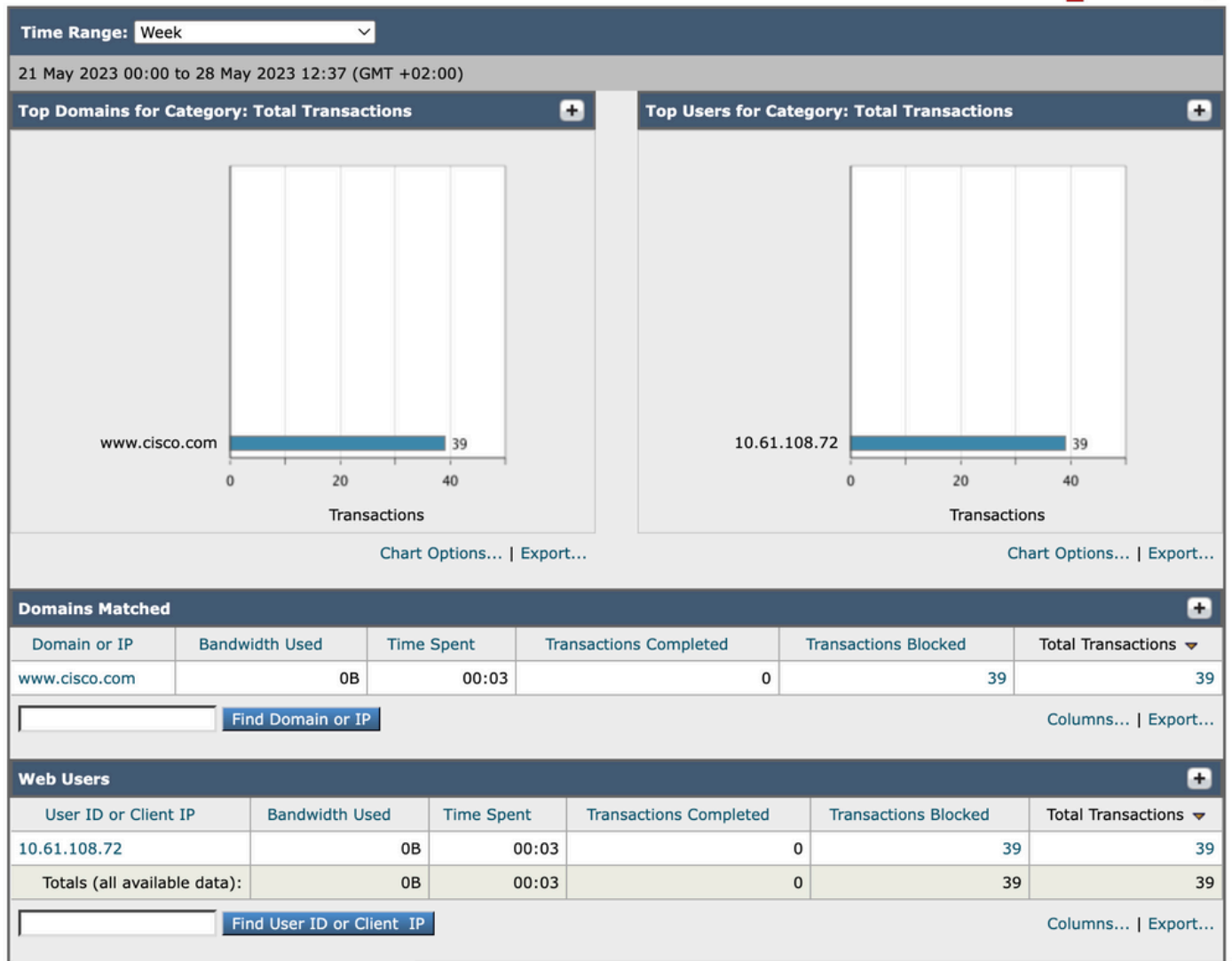
部分	描述
时间范围（下拉列表）	选择报告的时间范围。
按事务总数排名靠前的URL类别	本部分以图形格式列出站点上访问过的排名靠前的URL类别。
按阻止和警告的事务数排名靠前的URL类别	以图形格式列出触发每个事务发生的阻止或警告操作的排名靠前的URL。
匹配的URL类别	<p>按URL类别显示指定时间范围内的事务处理情况，以及每个类别中使用的带宽和花费的时间。</p> <p>如果未分类URL的百分比高于15-20%，请考虑以下选项：</p> <ul style="list-style-type: none"> • 对于特定的本地化URL，可以创建自定义URL类别并将其应用于特定用户或组策略。 • 您可以向思科报告未分类和分类错误以及URL，以便进行评估和数据库更新。 • 验证网络信誉过滤器和防恶意软件过滤器是否已启用。

URL-Categories



图像URL类别报告

您可以点击任何类别名称查看与该类别相关的更多详细信息，例如“匹配的域”或“用户列表”。



图像-详细报告页面

预定义的URL类别集可以在网络安全设备上定期自动更新。

当这些更新发生时，旧的类别名称将继续出现在报告中，直到与旧类别关联的数据太旧，无法包括在报告中。

URL类别集更新后生成的报告数据使用新类别，因此可以在同一报告中同时查看旧类别和新类别。

在报告的URL Categories页面上的URL统计信息中，了解如何解释以下数据非常重要：

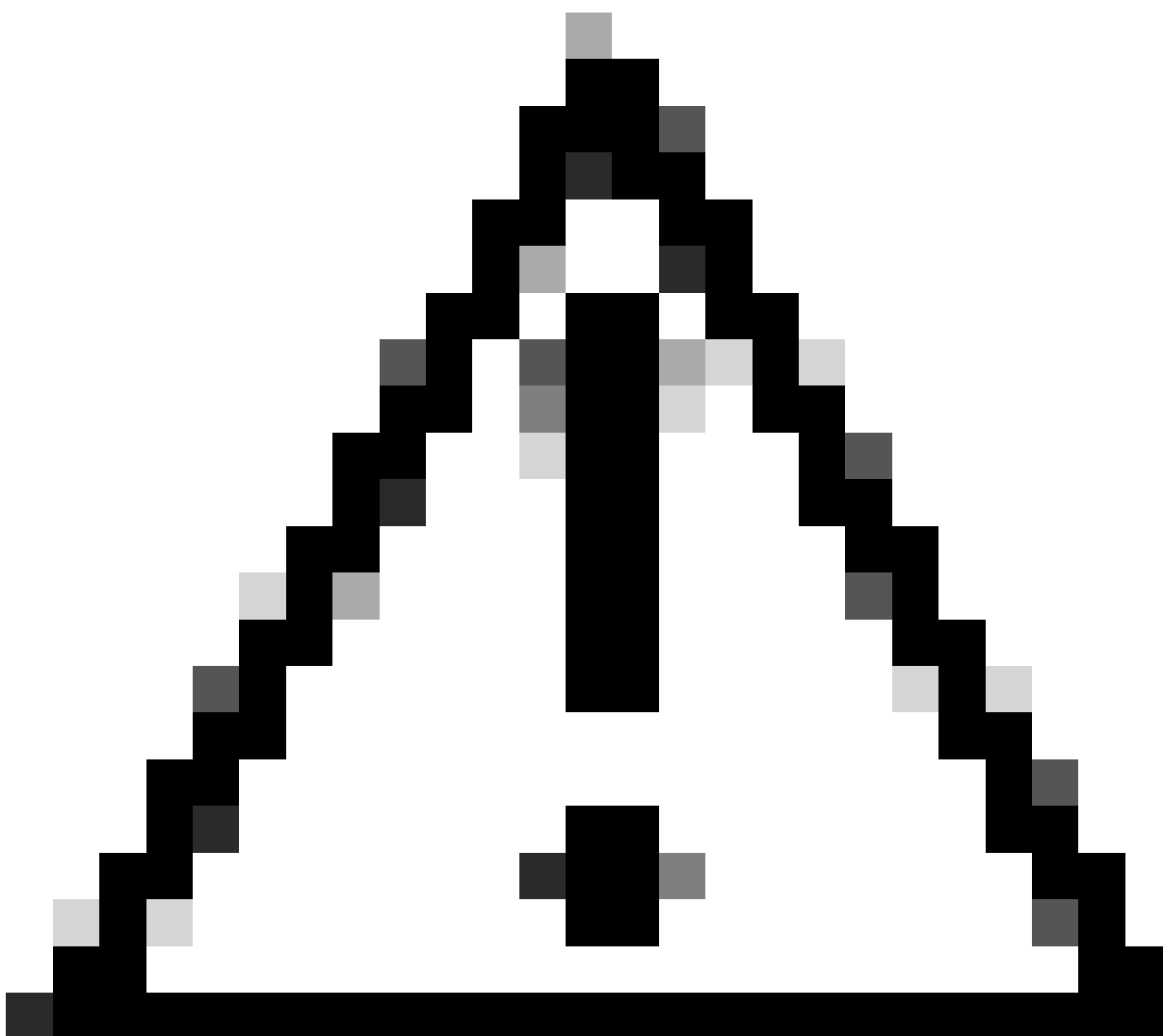
数据类型	描述
绕过的URL过滤	表示在URL过滤之前阻止的策略、端口和管理员用户代理。
未分类的URL	表示查询URL过滤引擎但未匹配任何类别的所有事务。

查看访问日志中的自定义URL类别

安全网络设备在访问日志中使用前面带有“c_”的自定义URL类别名称的前四个字符。

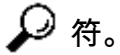
在本示例中，类别名称为CustomURLCategoriesBLOCKED，并且在aceslog中可以看到C_Cust：

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



注意：如果使用Sawmill分析访问日志，请考虑自定义URL类别名称。如果自定义URL类别的前四个字符包含空格，Sawmill将无法正确解析访问日志条目。相反，仅在前四个字符中使用支持的字符。

 提示：如果要在访问日志中包含自定义URL类别的全名，请向访问日志中添加%X格式说明



当Web访问策略组将自定义URL类别设置为监控时，并且某些其他组件(如Web信誉过滤器或不同裁决扫描(DVS)引擎)做出允许或阻止自定义URL类别中URL请求的最终决定，则请求的访问日志条目显示预定义的URL类别而不是自定义URL类别。

有关如何配置访问日志中的自定义字段的详细信息，请访问：[配置访问日志中的性能参数- Cisco](#)

故障排除

类别不匹配

从访问日志中，您可以看到请求属于哪个自定义URL类别（如果选择与预期不同）：

- 如果请求分类为其他自定义URL类别，请检查是否存在重复的URL或其他类别中的匹配正则表达式，或将自定义URL类别移到顶部并再次测试。最好仔细检查匹配的自定义URL类别。
- 如果请求归类为预定义类别，请检查现有自定义URL类别中的条件，如果所有条件都匹配，请尝试添加IP地址并进行测试，或确保使用拼写错误且正确的正则表达式（如果有）。

预定义的类别不是最新的

如果预定义的类别(Predefined Categories)不是最新的，或者在accesslogs中您在URL类别(URL category)部分看到“err”，请确保为Updater启用TLSv1.2。

要更改更新程序SSL配置，请在GUI中使用以下步骤：

步骤1:在System Administration中，选择SSL Configuration

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

映像- ssl配置

第二步：选择Edit Settings。

第三步：在更新服务部分，选择TLSv1.2

SSL Configuration

SSL Configuration	
<p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p>	
Appliance Management Web User Interface:	<p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
Proxy Services:	<p>Proxy services include HTTPS Proxy and credential encryption for secure client.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.3 <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> <p><input checked="" type="checkbox"/> Disable TLS Compression (Recommended) TLS compression should be disabled for best security.</p> <p>Cipher(s) to Use: EECDH:DSS:RSA:NULL:NULL:NULL:EXPORT:3DES:SEED:CAMELLIA</p>
Secure LDAP Services:	<p>Secure LDAP services include Authentication, External Authentication, SaaS SSO, and Secure Mobility.</p> <p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
RADSEC Services:	<p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1</p>
Secure ICAP Services (External DLP):	<p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
Update Service:	<p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>

Cancel Submit

映像-更新服务TLSv1.2

第四步：提交并提交更改

要更改更新程序SSL配置，请从CLI执行以下步骤：

步骤1:从CLI运行sslconfig

第二步：键入version，然后按Enter

第三步：选择Updater

第四步：选择TLSv1.2

第五步：按Enter键退出向导

步骤6.提交更改。

```
SWA_CLI> sslconfig
```

Disabling SSLv3 is recommended for best security.

Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential 1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:

- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.

[> versions

SSL/TLS versions may be enabled or disabled for the following services:

- LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secure Client)
- Updater - Update Service
- WebUI - Appliance Management Web User Interface
- RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
- SICAP - Secure ICAP Service
- Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

	LDAPS	Updater	WebUI	RADSEC	SICAP	Proxy
TLSv1.0	N	N	N	N/A	N	N
TLSv1.1	Y	Y	N	Y	Y	N
TLSv1.2	N	N	Y	Y	Y	Y
TLSv1.3	N/A	N/A	N/A	N/A	N/A	Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services

[> 2

Currently enabled protocol(s) for Updater are TLSv1.1.

To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2

[> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y

Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.

参考

[思科网络安全设备最佳实践指南-思科](#)

[BRKSEC-3303 \(ciscolive\)](#)

[思科安全网络设备AsyncOS 14.5用户指南- GD \(通用部署 \) -连接、安装和配置\[思科安全网络设备\]-思科](#)

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）。