防御恶意或不需要的 URL

本章包含以下部分：

关于 URL 的保护和控制

在工作队列的反垃圾邮件、爆发、内容和邮件过滤过程中，已纳入对恶意或不需要链接的控制和防御。这些控制：

- 提高防止邮件和附件中出现恶意 URL 的效果。

  URL 过滤合并到病毒爆发过滤中。即使您所在的组织已拥有思科 Web 安全设备或对网络威胁的类似防御，这种增强保护仍然非常有用，因为它可在入口点阻止威胁。

  根据邮件中 URL 的网络信誉得分 (WBRS)，还可以使用内容或邮件过滤器采取措施。

Note 作为最佳实践，思科推荐重写信誉可疑、不确定、可靠或未知的URL，将它们重定向至思科 Web 安全代理进行点击时间安全评估。

- 更好地识别垃圾邮件

该邮件网关利用邮件中链接的信誉和类别以及其他垃圾邮件识别算法，帮助识别垃圾邮件。例如，如果邮件中的链接属于营销网站，则该邮件很可能是营销邮件。

- 支持执行公司可接受的使用策略

  URL 类别（例如，成人内容或非法活动）可以与内容和邮件过滤器搭配使用，共同来执行公司可接受的使用策略。

- 允许识别组织中最常点击邮件中经过重写保护的 URL 的用户，以及最常被点击的链接。

相关主题

- 评估的 URL , on page 2
- “网络交互跟踪”(Web Interaction Tracking) 页面

评估的 URL

评估传入和传出邮件中的 URL（包括附件）。评估 URL 的任何有效字符串，包括含以下内容的字符串：

- http、https 或 www
- 域或 IP 地址
- 前缀冒号 (:) 的端口号
- 大写或小写字母

在评估URL以确定邮件是否为垃圾邮件时，如果需要进行负载管理，系统会优先检查传入邮件，然后是外发邮件。

URL 追溯判定和 URL 补救

根据基于云的 Talos 情报服务提供的 URL 信誉和类别过滤 URL。随着新信息的出现可更改 URL 信誉。一个 URL 最初可能不会被评估为恶意，因此，该消息可能会被放行，发送给收件人。但是随后，这些 URL 在任何时候都可以变成恶意的，即使它已经到达用户的邮箱。Talos 情报服务监控沙盒服务器中的 URL 判定。在 168 小时内，邮件网关每两分钟轮询一次来自 Talos 的 URL 的追溯性判定更新。如果任何 URL 信誉更改为“恶意”，则 Talos 会将追溯性判定更新发送到邮件网关。邮件网关会发送有关追溯性判定更新的警报，以便可以采取必要的操作。

Cisco Secure Email Gateway 处理在 URL 送交分析后 7 天内生成的 URL 追溯判定。邮件网关不会对 7 天后收到的判定执行配置的策略操作。

此外，您可以将邮箱自动补救服务配置为使用用户邮箱中的恶意 URL 补救邮件。例如, 当 URL 的信誉更改为恶意时，您可以将邮件云网关配置为从收件人邮箱中删除消息。配置的策略操作仅应用于已传送的邮件。

Note URL 追溯判定和补救功能仅适用于传入邮件。

无法解密来自安全邮件云网关的URL追溯判定流量。仅支持传递代理模式。但是，可以解密轮询响应数据。

如果其中一封邮件包含恶意 URL，则所有具有相同主题行的邮件都将进行补救。

必须更新安全邮件云网关的防火墙规则，以允许以下主机名访问 URL 追溯全局注册和轮询服务：

- prod-register-api.uce.cmd.cisco.com
- prodap-retro-api.uce.cmd.cisco.com
- prodeu-retro-api.uce.cmd.cisco.com
- produs-retro-api.uce.cmd.cisco.com

根据为主机名 (prod-register-api.uce.cmd.cisco.com) 配置的 DNS 服务器，邮件网关会连接到其中一个地理区域（如亚太、欧盟和美洲）的 URL 追溯注册和轮询服务。

相关主题

- 补救邮箱中的恶意邮件, on page 14

设置 URL 过滤

URL 过滤要求

除了启用 URL 过滤之外，还必须根据所需功能启用其他特性。

要增强防御垃圾邮件，请执行以下操作：

- 必须对每个适用的邮件策略，全局启用反垃圾邮件扫描。可以启用 IronPort 反垃圾邮件，也可以启用智能多扫描功能。请参阅反垃圾邮件章节。

要增强防御恶意软件，请执行以下操作：

- 必须对每个适用的邮件策略，全局启用爆发过滤器功能。请参阅“爆发过滤器”一章。

要根据 URL 信誉采取操作，或要使用邮件过滤器和内容过滤器执行可接受的使用策略：

- 必须全局启用爆发过滤器功能。请参阅“爆发过滤器”一章。

启用 URL 过滤

可以在 Web 界面中使用**安全服务 (Security Services) > URL 过滤 (URL Filtering)** 页面启用 URL 过滤，也可以在 CLI 中使用 **websecurityconfig** 命令启用。

Note 如果启用了 URL 过滤，也会自动启用 URL 追溯服务。有关详细信息，请参阅URL 追溯判定和 URL 补救, on page 2。

准备工作

- 确保满足要使用的各项 URL 过滤功能的要求。请参阅 URL 过滤要求 , on page 3。
- （可选）创建一个希望所有 URL 过滤功能都忽略的 URL 列表。请参阅创建允许的 URL 过滤列表 , on page 7。

Procedure

步骤 1 依次选择**安全服务 (Security Services) > URL 过滤 (URL Filtering)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 选中**启用 URL 类别和信誉过滤器 (Enable URL Category and Reputation Filters)** 复选框。

步骤 4 （可选）在评估邮件是否为垃圾邮件和恶意软件时，如果已创建了免于执行URL过滤及所有内容和邮件过滤的 URL 列表，请选择该列表。

通常，此设置不会导致邮件绕过反垃圾邮件或爆发过滤器处理。

步骤 5 [可选]启用 **Web 交互跟踪**。请参阅Web 互动跟踪 , on page 6。

步骤 6 您还可以在“URL 过滤”(URL Filtering) 页面中查看 **URL 追溯服务状态**。要启用或禁用 URL 追溯服务，请参阅 CLI 中的 `urlretroservice` 命令。

步骤 7 [可选]点击**高级设置 (Advanced Settings)** 并输入下表中所述的必需参数，以配置高级 URL 过滤设置：

参数	说明
URL 查找超时	输入 URL 请求特定域名的 IP 地址所用的时间。
邮件正文中扫描的 URL 的最大数量	输入您希望电子邮件网关在邮件正文中扫描的最大 URL 数量
在邮件附件中扫描的 URL 的最大数量	输入您希望邮件网关在邮件附件中扫描的最大 URL 数量。

参数	说明
重写邮件中的 URL 文本和 HREF	如果要在邮件正文中显示整个重写的URL，请选择**是 (Yes)** 单选按钮。 或 如果您希望整个重写的 URL 仅显示在 HTML 消息的 HREF 中，请选择**否 (No)** 单选按钮。
URL 日志记录	如果要在邮件日志和邮件跟踪中显示URL详细信息，请选择**启用 (Enable)** 单选按钮。 URL详细信息会根据以下任一条件记录在邮件日志和邮件跟踪中： • 邮件中与 URL 类别过滤器匹配的任何 URL 的类别。 • 邮件中与 URL 信誉过滤器匹配的任何 URL 的信誉得分。 • 爆发过滤器（如已启用）将重写邮件中的任何 URL。

步骤 8 提交并确认更改。

如果符合相应的前提条件，并且已配置爆发过滤器和反垃圾邮件保护，则无需要进行其他配置，即可执行增强的垃圾邮件和恶意 URL 自动检测。

What to do next

- 要基于邮件中的 URL 信誉采取操作，请参阅根据邮件中 URL 的信誉或类别采取操作 , on page 10。
- 要使用内容和邮件过滤器中的URL类别（例如，执行可接受的使用策略），请参阅根据邮件中 URL 的信誉或类别采取操作 , on page 10。
- 要将可疑垃圾邮件中的所有 URL 重定向到思科 Web 安全代理服务，请参阅使用自定义信头将疑似垃圾邮件中的 URL 重定向到思科网络安全代理：配置示例。
- （可选）要自定义最终用户通知页面的外观，请参阅自定义最终用户访问恶意站点时看到的通知 , on page 9。
- 确保您收到与此功能相关的问题警报。请参阅将来的 URL 类别集变更 , on page 35、AsyncOS 版本的版本说明和添加警报收件人。

关于与Talos 情报服务的连接

URL 信誉和类别由基于云的Talos 情报服务提供。

邮件网关使用防火墙信息中指定用于 URL 过滤服务的端口，直接或通过 Web 代理连接到Talos 情报服务。使用双方证书身份验证，通过HTTPS进行通信。证书将自动更新（请参阅服务更新。）有关所需证书的其他信息，请参阅版本说明（可从适用于 URL 过滤功能的证书 , on page 6指定的位置获取）。

如果已在**安全服务 (Security Services) > > 服务更新 (Service Updates)**页面配置 HTTP 或 HTTPS 代理，邮件网关将使用它与Talos情报服务通信。有关使用代理服务器的详细信息，请参阅配置服务器设置以下载升级和更新。

Note 不随同配置文件保存证书。

相关主题

- 适用于 URL 过滤功能的证书 , on page 6
- 警报：Beaker 连接器：获取注册证书时出错 , on page 20
- 警报：Beaker 连接器：证书无效 , on page 20

适用于 URL 过滤功能的证书

AsyncOS 旨在自动部署和更新与用于URL过滤功能的云服务通信所需的证书。但是，如果系统因任何原因无法更新这些证书，您将会收到需要您采取行动的警报。

确保邮件网关配置为向您发送这些警报（“系统”类型、“警告”严重性）。有关说明，请参阅警报。

如果收到关于证书无效的风险通告，请联系 Cisco TAC，其中可提供所需的替换证书。有关使用替换证书的说明，请参阅手动配置与Talos 情报服务通信的证书 , on page 23。

Web 互动跟踪

网络交互跟踪功能提供有关点击重写的URL的最终用户的信息，以及每位用户点击的相关操作（允许、组织或未知）。启用此功能后，您可以使用 Web 互动跟踪报告查看很多信息，例如点击数最高的恶意 URL，点击恶意 URL 次数最多的用户，等等。有关网络交互跟踪报告的详细信息，请参阅“网络交互跟踪”(Web Interaction Tracking) 页面。

网络交互跟踪数据由基于云的思科聚合服务器 (Cisco Aggregator Server) 提供。

相关主题

- 配置网络交互跟踪, on page 6
- 关于与思科聚合器服务器的连接, on page 7

配置网络交互跟踪

根据您的需求，可以在其中一个全局设置页面中启用网络交互跟踪：

- **爆发过滤器**。跟踪点击了爆发过滤器重写的 URL 的最终用户。请参阅配置爆发过滤器全局设置。
- **URL 过滤**。跟踪点击了策略（使用内容和邮件过滤器）重写的 URL 的最终用户。请参阅启用 URL 过滤, on page 4。

关于与思科聚合器服务器的连接

邮件网关每隔 30 分钟（不可配置），使用防火墙信息中指定用于 URL 过滤的端口，直接或通过 Web 代理连接到思科聚合器服务器。使用双方证书身份验证，通过 HTTPS 进行通信。证书自动更新（请参阅服务更新。）

如果已在**安全服务 (Security Services)** > **服务更新 (Service Updates)** 页面上配置 HTTP 或 HTTPS 代理，则邮件网关将使用它来与思科聚合器服务器通信。有关使用代理服务器的详细信息，请参阅配置服务器设置以下载升级和更新。

Note 不随同配置文件保存证书。

集群配置中的 URL 过滤

- 您可以在计算机、组或集群级别启用 URL 过滤。
- 如果在计算机级别启用 URL 过滤，则可以在计算机、组或集群级别配置 URL 允许列表和 Web 交换跟踪。
- 如果在组级别启用 URL 过滤，则必须在组或集群级别配置 URL 允许列表和 Web 交换跟踪。
- 如果在集群级别启用 URL 过滤，则必须在集群级别配置 URL 允许列表和 Web 交换跟踪。
- 适用用于邮件过滤器和内容过滤器的集群的标准规则。

创建允许的 URL 过滤列表

如果在配置 URL 过滤功能时指定了全局允许列表，则不评估允许列表中 URL 的信誉或类别，不执行反垃圾邮件、爆发过滤或内容和邮件过滤。但是，反垃圾邮件扫描和爆发过滤器将正常评估包含这些 URL 的邮件。此外，还可以在每个 URL 过滤条件（规则）和内容与邮件过滤器操作中指定 URL 允许列表，以补充全局 URL 允许列表。

通常，要对爆发过滤中的允许列表 URL 进行归类，可使用在“邮件策略：爆发过滤器”(Mail Policies: Outbreak Filters) 页面配置的“绕过域扫描”(Bypass Domain Scanning) 选项。URL 过滤的 URL 允许列表与之类似，但与“绕过域扫描”(Bypass Domain Scanning) 无关。有关该功能的详细信息，请参阅URL 重写和绕行域。

此部分介绍的 URL 过滤允许列表与基于 IP 信誉得分的发件人信誉过滤所用的允许列表之间没有关系。

准备工作

请考虑导入 URL 列表，而不是在 Web 界面中创建 URL 列表。请参阅导入 URL 列表 , on page 8。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > URL 列表 (URL Lists)**。

步骤 2 选择**添加 URL 列表 (Add URL List)**，或点击一个列表进行编辑。

确保希望全局指定为允许列表的所有 URL 都在一个列表中。只能为 URL 过滤选择一个全局允许列表。

步骤 3 创建并提交该 URL 列表。

要查看支持的 URL 格式的列表，请向 **URL** 框中输入分号 (;)，并点击**提交 (Submit)**。然后，点击显示的**更多... (more...)** 链接。

每个 URL、域或 IP 地址可以单独为一行，或使用逗号相互隔开。

步骤 4 确认更改。

What to do next

- 要将 URL 列表指定为全局允许列表，请参阅启用 URL 过滤, on page 4。
- 要将URL指定为内容或邮件过滤器中特定条件（规则）或操作的允许列表，请参阅根据邮件中 URL 的信誉或类别采取操作 , on page 10和内容过滤器操作。对于邮件过滤器，另请参阅URL 类别操作和URL 类别规则。

相关主题

- 导入 URL 列表 , on page 8

导入 URL 列表

您可以导入 URL 列表，用作 URL 过滤的允许列表。

Procedure

步骤 1 创建要导入的文本文件：

- 第一行必须是 URL 列表的名称。
- 每个 URL 必须单独为一行。

步骤 2 将文件上传到设备的 `/configuration` 目录。

步骤 3 在命令行界面使用 `urllistconfig > new` 命令。

自定义最终用户访问恶意站点时看到的通知

如果最终用户点击了病毒爆发过滤或策略（使用内容或邮件过滤器）所识别的恶意 URL，思科 Web 安全代理将在最终用户的 Web 浏览器中显示通知。此通知将指出：该站点是恶意的，对该站点的访问已被阻止。

当最终用户点击使用爆发过滤重写的 URL 时，通知页面将显示 10 秒，然后会重定向到思科 Web 安全代理进行点击时评估。

您可以自定义此通知页面的外观，并显示您所在组织的品牌，例如公司徽标、联系信息等。

Note 如果您未自定义通知页面，则最终用户将看到思科品牌的通知页面。

准备工作

- 启用 URL 过滤。请参阅启用 URL 过滤, on page 4。

Procedure

步骤 1 依次选择**安全服务 (Security Services)** > **阻止页面自定义 (Block Page Customization)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 选中**启用阻止页面自定义 (Enable Block Page customization)** 复选框，并输入以下详细信息：

- 组织徽标的 URL。建议将徽标图像托管在可公开访问的服务器。
- 组织名称
- 组织的联系信息

步骤 4 选择通知的语言。可以选择 Web 界面支持的任何一种语言。

Note 最终用户的浏览器默认语言优先于您在此所选的语言。此外，如果 AsyncOS 不支持最终用户的浏览器默认语言，则以您在此所选的语言显示通知。

步骤 5 （可选）点击**预览阻止页面自定义 (Preview Block Page Customization)** 链接可预览通知页面。

步骤 6 提交并确认更改。

后续步骤

通过以下任一方式设置 URL 重写：

- 使用爆发过滤器。请参阅重定向 URL。
- 使用内容或邮件过滤器。请参阅根据邮件中 URL 的信誉或类别采取操作 , on page 10。

根据邮件中 URL 的信誉或类别采取操作

您可以在传入和传出邮件策略中使用邮件过滤器和内容过滤器，根据邮件正文或邮件附件中URL链接的信誉或类别来采取操作。

由于爆发过滤器在评估邮件是否为恶意软件时要考虑许多因素，而且单独URL信誉可能不会触发主动邮件处理，所以您可能希望基于 URL 信誉创建过滤器。

例如，您可以使用 URL 信誉过滤器：

- （仅用于邮件正文中的URL）重写信誉不确定或未知的URL，将它们重定向到思科云网络安全代理服务以进行点击时评估。
- 丢弃包含的 URL 的信誉得分属于不信任范围的邮件。

您可以使用 URL 类别过滤器：

- 过滤 URL 的类别，以执行组织可接受的 Web 使用策略，例如阻止用户在办公室访问成人或赌博站点。
- 增强防御存在时间不足以进行分类的恶意站点。（仅用于邮件正文中的 URL）当用户点击链接时，可以将未分类类别的所有 URL 都重定向到思科云网络安全代理服务进行评估。

相关主题

- 使用 URL 相关条件（规则）和操作 , on page 10
- 按 URL 信誉或 URL 类别过滤：条件和规则 , on page 11
- 修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作 , on page 11
- 重定向 URL：最终用户会有哪些体验？ , on page 13

使用 URL 相关条件（规则）和操作

要想	示例	操作
整体上针对邮件采取操作。	丢弃或隔离邮件。	创建 URL 信誉或 URL 类别条件或规则，然后将其与 URL 信誉或 URL 类别操作以外的任何操作配对。 例外：请勿将 URL 信誉条件或规则与退回操作配对。
（仅用于邮件正文中的 URL）修改邮件中的 URL 或修改其行为。	用文本说明替换邮件中的 URL，或将URL 设为不可点击状态。	仅创建URL 信誉或URL 类别操作；请勿使用单独的 URL 过滤条件。

一如既往，必须在邮件策略中指定内容过滤器，才能使用它。

相关主题

- 按 URL 信誉或 URL 类别过滤：条件和规则 , on page 11

- 修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作 , on page 11

按 URL 信誉或 URL 类别过滤：条件和规则

您可以根据邮件正文和邮件附件中 URL 的信誉或类别对邮件进行操作。如果您要执行修改 URL 或其行为以外的任何操作，请添加 **URL 信誉 (URL Reputation)** 或 **URL 类别 (URL Category)** 条件，然后选择要对其应用操作的信誉分数或 URL 类别。

例如，如果要对包含“成人”(Adult) 类别 URL 的所有邮件应用**丢弃**（**最终操作**）操作，请添加一个 **URL 类别 (URL Category)** 的条件，并选择**成人 (Adult)** 类别。

如果未指定类别，将对所有邮件应用您所选的操作。

信任、中性和不信任 URL 的 URL 信誉得分范围是预定义的，不可编辑。但是，您可以改为指定自定义范围。指定的终端包含在所指定的范围内。例如，如果创建了一个从 -8 到 -10 的自定义范围，则 -8 和 -10 包含在该范围内。对于信誉得分无法确定的 URL，请使用 “未知”(Unknown)。

Note 不确定的 URL 信誉表示这些 URL 目前是安全的，但将来可能会变为恶意的，因为它们容易受到攻击。对于此类URL，管理员可创建非阻止策略，例如将它们重定向到思科Web安全代理以进行点击时评估。

不评估特定 URL 允许列表或全局 URL 允许列表中包含的 URL。

如果邮件中的任何URL与在条件中指定的信誉分数或任何类别匹配，则采取与此条件配对的操作。

如果您要修改邮件中的 URL，或修改其行为，则仅配置 URL 信誉或 URL 类别操作即可。对此，您不需要单独的 URL 信誉或 URL 类别条件或规则。

Note 请勿将 URL 信誉条件与退回操作配对。

Tip 要检查特定 URL 的类别，请访问报告未分类和误分类的 URL , on page 35中的链接。

相关主题

- 创建允许的 URL 过滤列表 , on page 7
- 内容过滤器

修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作

根据 URL 的信誉或类别，使用 URL 信誉或 URL 类别操作修改邮件中的 URL 或其行为。

URL 信誉和 URL 类别操作不需要单独的条件。相反，系统会根据您在 URL 信誉或 URL 类别操作中选择的信誉或类别应用所选的操作。

仅对符合操作中指定条件的 URL 应用该操作。不会修改邮件中的其他 URL。

如果未指定类别，将对所有邮件应用您所选的操作。

信任、中性和不信任 URL 的 URL 信誉得分范围是预定义的，不可编辑。但是，您可以改为指定自定义范围。指定的终端包含在所指定的范围内。例如，如果创建了一个从 -8 到 -10 的自定义范围，则 -8 和 -10 包含在该范围内。对于信誉得分无法确定的 URL，请使用 “未知”(Unknown)。

Note 不确定的 URL 信誉表示这些 URL 目前是安全的，但将来可能会变为恶意的，因为它们容易受到攻击。对于此类URL，管理员可创建非阻止策略，例如将它们重定向到思科 Web 安全代理以进行点击时评估。

以下与 URL 相关的操作仅适用于邮件正文中的 URL：

- 去除 URL，使其不可点击。邮件收件人仍然可以查看和复制 URL。
- 重定向 URL，这样当邮件收件人点击链接，事务将路由到云中的思科网络安全代理；如果站点是恶意的，则阻止访问。

  示例：您可能希望将**未分类**类别中的所有URL都定向到思科云网络安全代理服务，因为网络钓鱼攻击中所用的恶意站点存在的时间通常不足以进行分类。

  另请参阅重定向 URL：最终用户会有哪些体验？ , on page 13。

  要将 URL 重新定向到不同的代理，请参阅以下项目中的示例。

Note 在此版本中，思科云网络安全代理服务没有可配置的选项。例如，没有威胁分数阈值供调整或基于威胁分数指定操作。

- 使用任何文本替换 URL。

  要在邮件显示的文本中包括原始 URL，请使用 $URL 变量。

  示例：

  - 使用以下注释替换**非法下载 (Illegal Downloads)** 类别的所有 URL：

    ```
    Message from your system administrator: A link to an illegal downloads web site has
    been removed from this message.
    ```

  - 包含原始 URL 及警告：

    ```
    WARNING! The following URL may contain malware: $URL
    ```

    这样将变成：WARNING: The following URL may contain malware: http://example.com。

  - 重定向到自定义代理或网络安全服务：

    ```
    http://custom_proxy/$URL
    ```

这样将变成：http://custom_proxy/http://example.com

不评估包含在所选 URL 允许列表或全局 URL 允许列表中的 URL 的信誉和类别。

如果要去除或替换 URL，可以选择忽略已签名邮件中的 URL。

不建议将 URL 信誉或 URL 类别操作与 URL 信誉或 URL 类别条件（或规则）配对。如果配对的条件（规则）和操作包括其他类别，则不会产生匹配。

Tip 要检查特定 URL 的类别，请访问报告未分类和误分类的 URL , on page 35中的链接。

相关主题

- 创建允许的 URL 过滤列表 , on page 7
- 使用自定义信头将疑似垃圾邮件中的 URL 重定向到思科网络安全代理：配置示例
- 内容过滤器
- URL 信誉规则
- URL 类别规则

重定向 URL：最终用户会有哪些体验？

根据思科云网络安全代理服务的评估：

- 如果站点是良性的，用户将定向到目标网站，并且不知道链接已被重定向。
- 如果站点是恶意的，用户将看到通知，表示该站点是恶意的，对该站点的访问已被阻止。

  您可以自定义最终用户通知页面的外观，并显示您所在组织的品牌，例如公司徽标、联系信息等。请参阅自定义最终用户访问恶意站点时看到的通知 , on page 9。
- 如果与思科云网络安全代理服务的通信超时，系统将允许用户访问目标网站。
- 如果出现任何其他错误，用户将看到通知。

相关主题

- 修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作 , on page 11

处理 URL 过滤的不可扫描邮件

在下列情况下，URL 过滤扫描会失败，并将信头 *X-URL-LookUp-ScanningError* 添加到邮件中：

- 无法获取 URL 信誉和类别
- 无法展开邮件中缩短的 URL
- 邮件正文或邮件附件中的 URL 数超过了最大 URL 扫描限制

可以添加内容过滤器，在“其他信头条件”中选择“*X-URL-LookUp-ScanningError*”信头，并配置要对邮件执行的相应操作。

补救邮箱中的恶意邮件

具有任何信誉的URL在任何时候都可以变成恶意的，即使它已经到达用户的邮箱。您可以在邮件云网关上配置 URL 过滤，以根据从 Talos 收到的 URL 追溯判定发送警报。您还可以配置您的电子邮件网关，当 URL 判定变为恶意时，对用户邮箱中的邮件执行自动补救行动。

准备工作

- 确保满足要使用的各项 URL 过滤功能的要求。请参阅 URL 过滤要求 , on page 3。
- 确保 URL 过滤已启用。请参阅启用 URL 过滤, on page 4。
- 确保在您的邮件云网关上激活用于访问云服务的许可证密钥。
- 确保在您的邮件云网关上启用了邮箱自动补救功能。请参阅在邮件网关上启用帐户设置。

Procedure

步骤 1 依次选择**安全服务 (Security Services) > URL 过滤 (URL Filtering)**。

步骤 2 选择 **邮箱自动补救**下的 **启用** 。

步骤 3 选择 **启用邮箱自动补救** 复选框。

步骤 4 当 URL 信誉判决更改为恶意时，对发送给最终用户的邮件将执行的配置补救操作。

- 转发至邮件地址 - 选择此选项可将包含恶意 URL 的邮件转发给指定用户，例如邮件管理员。
- 删除消息 - 选择此选项可从最终用户的邮箱中永久删除包含恶意 URL 的邮件。
- 转发到邮件地址并删除该邮件。选择此选项可将包含恶意URL的邮件转发给指定用户（例如邮件管理员），并从最终用户的邮箱中永久删除该邮件。

Note 由于Office 365服务不支持删除这些文件夹中的邮件，因此无法删除来自某些文件夹（例如，已删除邮件）的邮件。

Note 在配置“邮箱自动补救”设置之前，请查看 补救邮箱中的邮件。

步骤 5 提交并确认更改。

使用内容过滤器检测邮件中的恶意 URL

使用“URL 信誉”内容过滤器可检测被 ETF 引擎归类为恶意的邮件中的 URL，并对此类邮件执行适当的操作。

您可以通过以下任何一种方式配置 ETF 的“URL 信誉”内容过滤器：

- 请将“URL 信誉”条件与任何适当的操作结合使用。
- 将“URL 信誉”操作与任何或不条件结合使用。
- 将“URL 信誉”条件和操作结合使用。

以下过程用于使用“URL 信誉”条件和操作检测恶意 URL：

注释

- 如果您只想将“URL 信誉”条件与任何适当的操作结合使用，请勿执行该过程的步骤 11-20。
- 如果您只想将“URL 信誉”操作与任何条件结合使用或不与任何条件结合使用，请勿执行该过程的步骤 4-10。

开始之前

- 确保您已在邮件网关上启用 URL 过滤。要启用 URL 过滤，请转到 Web 界面中的安全服务 *(Security Services)* > *URL* 过滤 *(URL Filtering)* 页面。有关详细信息，请参阅防御恶意或不需要的 URL，第 1 页。
- 确保您已在邮件网关上启用爆发过滤器。要启用病毒爆发过滤器，请转到 Web 界面中的安全服务 *(Security Services)* > 病毒爆发过滤器 *(Outbreak Filters)*页面。有关详细信息，请参阅爆发过滤器。
- 确保您已在邮件网关上启用反垃圾邮件引擎。要启用反垃圾邮件引擎，请转到 Web 界面中的安全服务 *(Security Services)* > 反垃圾邮件 *(Anti-Spam)*页面。有关详细信息，请参阅管理垃圾邮件和灰色邮件。
- （可选）创建 URL 列表。要创建一个，请转到 Web 界面中的邮件策略 *(Mail Policies)* > *URL* 列表 *(URL Lists)* 页面。有关详细信息，请参阅防御恶意或不需要的 URL，第 1 页。

过程

步骤 1 转到**邮件策略 (Mail Policies) > 传入内容过滤器 (Incoming Content Filters)**。

步骤 2 点击**添加过滤器 (Add Filter)**。

步骤 3 输入内容过滤器的名称和描述。

步骤 4 点击**添加条件 (Add Condition)**。

步骤 5 点击 **URL 信誉 (URL Reputation)**。

步骤 6 选择**外部威胁源 (External Threat Feeds)**。

步骤 7 选择要检测恶意 URL 的 ETF 源。

步骤 8 （可选）选择您不希望邮件网关检测威胁的已列入允许列表的 URL 列表。

步骤 9 选择所需的**检查 URL (Check URLs within)** 选项，以检测“邮件正文和主题”和/或“邮件附件”中的恶意 URL。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**添加操作 (Add Action)**。

步骤 12 点击 **URL 信誉 (URL Reputation)**。

步骤 13 选择**外部威胁源 (External Threat Feeds)**。

步骤 14 请确保选择您在条件中所选（第7步）的相同 ETF 源。

步骤 15 （可选）选择您在第 8 步中所选的已列入允许列表的相同 URL 列表。

步骤 16 选择所需的**检查 URL (Check URLs within)** 选项，以检测“邮件正文和主题”和/或“邮件附件”中的恶意 URL

步骤 17 在邮件正文、主题和/或邮件附件中，选择要在 URL 上执行的所需操作。

注释 在第 16 步中，如果您将“检查 URL”(Check URLs within) 选项选择为“附件”(Attachments)，则只能删除该邮件的附件。

步骤 18 选择是否要对所有邮件或未签名的邮件执行操作。

步骤 19 点击**确定 (OK)**。

步骤 20 提交并确认更改。

注释 如果您在邮件网关上为基于 Web 信誉得分 (WBRS) 和 ETF 配置了“URL 信誉”内容过滤器，建议将 WBRS URL 信誉内容过滤器的顺序设置为高于 ETF URL 信誉过滤器的顺序，以提高邮件网关的性能。

使用邮件过滤器检测邮件中的恶意域

例如，使用“URL 信誉”邮件过滤器规则语法来检测使用 ETF 引擎的邮件中的恶意 URL，并去除该 URL。

语法：

```
 defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
 <'URL_allowedlist'>,
<’ message_attachments'> , <’ message_body_subject’ > ,))
 { url-etf-defang(['etf-source1'], "", 0); } <’ URL_allowedlist’ > ,
<’ Preserve_signed’ >)}
```

位置

- ‘url-external-threat-feeds’ 是 URL 信誉规则。
- ‘etf_source1’ 是用于检测邮件或邮件附件中的恶意 URL 的 ETF 源。
- “URL_allowedlist”是 URL 允许列表的名称。如果 URL 允许列表不存在，则显示为“”。
- ‘message_attachments’ 用于检查邮件附件中是否存在恶意 URL。值 "1" 用于检测邮件附件中的恶意 URL。

- ‘message_body_subject’ 用于检查邮件正文和主题中是否存在恶意 URL。值“1”用于检测邮件正文和主题中的恶意 URL。

注释 值“1,1”用于检测邮件正文、主题和邮件附件中的恶意 URL。

- ‘url-etf-defang’ 是您可以对包含恶意 URL 的邮件执行的操作之一。

  以下示例是您可以在包含恶意 URL 的邮件上应用的基于 ETF 的操作：

  - url-etf-strip(['etf_source1'], "None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-重定向条（[' etf_source1 ']，"None"，1）
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- "Preserve_signed"由 "1" 或 "0" 表示。"1" 表示此操作仅适用于未签名邮件，"0" 表示此操作适用于所有邮件。

在以下示例中，如果邮件附件中的 URL 被 ETF 引擎检测为恶意，则该附件将被删除。

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

监控 URL 过滤结果

要查看有关检测到的恶意和不确定 URL 的数据，请选择**监控 (Monitor)** > **URL 过滤 (URL Filtering)**。有关此页面中数据的重要信息，请参阅“URL 过滤”(URL Filtering) 页面。

要查看有关从用户邮箱进行补救的具有恶意 URL 的邮件的数据，请参阅 “URL 追溯”(URL Retrospection) 页面。

在邮件跟踪中显示 URL 详细信息

要显示爆发过滤器和相关内容过滤器所捕获 URL 的邮件跟踪的详细信息，请执行以下操作：

- 必须启用邮件跟踪。
- 基于 URL 信誉或 URL 类别的爆发过滤器和/或内容过滤器器必须是可操作的。
- 对于爆发过滤器，必须启用 URL 重写。请参阅URL 重写和绕行域。
- 必须启用 URL 日志记录。请参阅启用 URL 日志记录和 URL 邮件跟踪详细信息。
- 必须启用邮箱补救，才能在邮件跟踪中显示有关基于URL追溯判定更新从用户邮箱补救的邮件的详细信息。请参阅补救邮箱中的邮件。

有关所显示数据的详细信息，请参阅邮件跟踪详细信息。

若要管理对这些潜在敏感的详细信息的管理用户访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限。

URL 过滤故障排除

相关主题

- 查看日志 , on page 20
- 警报：Beaker 连接器：获取注册证书时出错 , on page 20
- 警报：Beaker 连接器：证书无效 , on page 20
- 无法连接Talos 情报服务, on page 20
- 警报：无法连接到思科聚合服务器, on page 21
- 警报：无法从思科聚合服务器检索网络交互跟踪信息, on page 21
- 使用 websecurityadvancedconfig 命令 , on page 22
- 邮件跟踪搜索未找到指定类别的邮件 , on page 22
- 反垃圾邮件或病毒爆发过滤器不会捕获恶意 URL 和营销邮件 , on page 22
- 过滤类别中的 URL 未得到正确处理 , on page 23
- 最终用户通过重写的 URL 访问恶意站点 , on page 23
- 手动配置与Talos 情报服务通信的证书 , on page 23

查看警报

下表包含 URL 引擎生成的系统警报的列表，包括对警报和警报严重性的说明。

组件/警报名称	邮件和描述	参数
ECS REMEDIATION_INITIATION	警报文本：“已为包含恶意URL的邮件发起邮件补救：$message_id : $url” 信息：当补救服务发起的对已传送到用户邮箱的恶意 URL 进行补救的邮箱补救成功或失败时发送的警报。	• **message_id**- 包含 URL 的邮件的邮件 ID。 • **url** - 收到追溯判定的URL。
ECS 信息	警报文本：“从 URL 追溯服务收到判定更新。邮件 ID、MID 和 URL 的格式如下：$message_id : $mid : $url" 信息：当您的邮件网关收到来自追溯服务器的 URL 追溯判定时发送的警报。	• **message_id** - 包含 URL 的邮件的邮件 ID。 • **mid** - 消息标识符号。 • **url** - 收到追溯判定的URL。
ECS 关键	警报文本：轮询接收有关 URL 信誉的追溯性判定失败，出现证书无效错误。如需帮助，请与 Cisco TAC 联系。 警告：当您的邮件网关由于证书无效而无法从追溯服务器接收URL追溯判定时发送警报。如需帮助，请与 Cisco TAC 联系。	不适用
ECS 警告	警报文本：重新启动 URL 追溯轮询服务以修复不正确的请求格式。 警告：已发送警报以重新启动URL追溯轮询服务，以更正轮询请求的格式。	不适用
ECS 关键	连接错误：无法连接到追溯注册服务。如需帮助，请与 Cisco TAC 联系。 失败的原因： • 证书无效错误。 • 云服务不可用。 • 连接请求被拒绝（例如，证书密钥无效）。	不适用

查看日志

URL 过滤信息将发布到以下日志：

- 邮件日志 (mail_logs)。有关 URL 扫描结果（根据 URL 对邮件采取的操作）的信息将发布到此日志。
- URL 过滤日志 (web_client)。尝试查找 URL 时，有关错误、超时、网络问题等的信息将发布到此日志。
- 补救日志。与基于 URL 追溯服务的邮箱补救相关的信息将发布到此日志。
- 邮件云扫描程序日志。与从追溯性云扫描程序接收的 URL 追溯性判定相关的信息。

大多数信息处于信息或调试级别。有关登录的详情，请参阅 日志记录。

日志中不包括有关用户点击邮件中重定向的链接时所发生状况的信息。

日志中的“SDS”是指 URL 信誉服务。“Breaker 连接器”是指 Talos 引擎。

警报：Beaker 连接器：获取注册证书时出错

问题

关于获取注册客户端证书时出现的错误，您将会收到参考级别的风险通告。

解决方案

要连接到以下基于云的服务，需要使用此证书：Talos 情报服务（获取 URL 信誉和类别）和思科聚合服务器（获取 Web 交换跟踪数据）。请尝试以下操作：

1. 检查网络连接问题，例如代理设置不正确或防火墙问题。
2. 确认您的 URL 过滤功能密钥是否有效且处于活动状态。
3. 如果问题仍然存在，请联系 Cisco TAC。

警报：Beaker 连接器：证书无效

问题

您将收到有关无效 Beaker 连接器证书的严重警报。

解决方案

要连接到云中的Talos 情报服务以获取 URL 信誉和类别，需要使用此证书。

要获取和手动安装证书，请参阅手动配置与Talos 情报服务通信的证书 , on page 23。

无法连接Talos 情报服务

问题

安全服务 (Security Services) > URL 过滤 (URL Filtering) 页面将持续指示连接到Talos 情报服务的问题。

解决方案

- 如果已启用 URL 过滤，但尚未确认更改，请确认更改。
- 检查最近有关连接Talos 情报服务的警报。请参阅查看最近的警报。如果适用，请参阅警报：Beaker 连接器：获取注册证书时出错 , on page 20和警报：Beaker 连接器：证书无效 , on page 20。
- 如果要通过**安全服务 (Security Services) > 服务更新 (Service Updates)**指定的代理连接，请确认已配置代理并且代理工作正常。
- 检查可能会阻止连接的其他网络问题。
- 如果在 URL 过滤日志中看到有关请求连接 Talos 客户端超时的错误，请在命令行界面使用 **websecurityadvancedconfig** 命令和 websecurityadvancedconfig 命令调查并进行更改：
  - 如果诊断表示：响应时间大于或等于所配置的 URL 查找超时，请相应地增加 URL 查找超时值。
- 检查URL 过滤日志中与URL 扫描仪、思科网络安全服务或Talos 客户端 通信时的非超时错误。日志中的“Talos 客户端”表示Talos 情报服务。如果看到这种日志消息，请联系 TAC。

警报：无法连接到思科聚合服务器

问题

您将会收到以下警告风险通告：无法连接到思科聚合服务器。

解决方案

执行以下操作：

1. 通过从邮件网关 ping 服务器的主机名，检查邮件网关和思科聚合服务器之间的连接。在 CLI 中使用 aggregatorconfig 命令，查看思科聚合服务器的主机名。
2. 如果要通过“安全服务”(Security Services) >“服务更新”(Service Updates) 指定的代理连接，请确认已配置代理并且代理工作正常。
3. 检查可能会阻止连接的其他网络问题。
4. 检查 DNS 服务是否正在运行。
5. 如果问题仍然存在，请联系 Cisco TAC。

警报：无法从思科聚合服务器检索网络交互跟踪信息

问题

您将会收到以下警告风险通告：无法从思科聚合服务器检索网络交互跟踪信息。

解决方案

执行以下操作：

1. 如果要通过**安全服务 (Security Services) > 服务更新 (Service Updates)**指定的代理连接，请确认已配置代理并且代理工作正常。
2. 检查可能会阻止连接的其他网络问题。
3. 检查 DNS 服务是否正在运行。
4. 如果问题仍然存在，请联系 Cisco TAC。

警报：邮件云扫描程序 (ECS)：证书无效

问题

您将收到有关无效 ECS 连接器证书的严重风险通告。

解决方案

邮件云扫描程序客户端的追溯服务器证书验证失败。需要此证书才能连接到客户端以获取URL追溯更新。要修复此错误，请联系思科支持部门。

警报：邮件云扫描程序 (ECS)：网络无法访问

问题

当您的邮件网关无法访问 URL 追溯云扫描程序服务时，您会收到严重警报。

解决方案

验证防火墙设置。请与您的网络管理员联系以获得帮助。

使用 websecurityadvancedconfig 命令

除本文档明确描述的更改之外，未经 TAC 指导，请勿使用 websecurityadvancedconfig 命令进行任何其他更改。

邮件跟踪搜索未找到指定类别的邮件

问题

按某个类别搜索时，未找到包含该特定类别的 URL 的邮件。

解决方案

请参阅搜索结果中缺少预期邮件。

反垃圾邮件或病毒爆发过滤器不会捕获恶意 URL 和营销邮件

问题

反垃圾邮件或爆发过滤器不会捕获恶意 URL 和包含营销链接的邮件。

解决方案

- 出现这种情况，可能是因为网站信誉和类别仅是反垃圾邮件和病毒爆发过滤器用于确定其判定的众多条件中的两个。您可以通过降低重写URL、用文本替换URL、隔离或丢弃邮件等操作所需的阈值，提高这些过滤器的敏感度。有关详细信息，请参阅爆发过滤器功能和邮件策略和定义反垃圾邮件策略。或者，根据 URL 信誉得分创建内容或邮件过滤器。
- 如果邮件网关无法连接到Talos 智能服务，也可能会出现这种情况。请参阅无法连接Talos 情报服务, on page 20。

过滤类别中的 URL 未得到正确处理

问题

未应用内容或邮件过滤器中根据 URL 类别定义的操作。

解决方案

- 使用跟踪功能（“故障排除”一章中介绍）跟进邮件处理路径。
- 如果邮件网关无法连接到Talos 智能服务，则可能会出现这种情况。请参阅无法连接Talos 情报服务, on page 20。
- 如果没有任何连接问题，URL仍可能不会分类或分类错误。请参阅报告未分类和误分类的URL , on page 35。您可以使用此站点确定 URL 的类别。

最终用户通过重写的 URL 访问恶意站点

问题

恶意 URL 将被重定向到思科 Web 安全代理，但最终用户仍无法访问站点。

解决方案

如果满足以下条件，就可能出现这种情况：

- 该站点未被识别为恶意站点。
- 连接思科网络安全代理超时，这种情况应该很少见。确保网络问题不会妨碍连接。

手动配置与Talos 情报服务通信的证书

如果邮件网关无法自动获取与Talos 情报服务通信的证书，请使用此过程。

Procedure

步骤 1 获取所需的证书。

步骤 2 使用**网络 (Web) > 证书 (Certificates)** 上传证书，或在命令行界面中使用 certconfig 命令。

步骤 3 在命令行界面，输入 **`websecurityconfig`** 命令。

步骤 4 按照提示设置 Talos 情报服务身份验证的客户端证书。

关于 URL 类别

相关主题

- URL 类别说明 , on page 24
- 确定 URL 的类别 , on page 35
- 报告未分类和误分类的 URL , on page 35
- 将来的 URL 类别集变更 , on page 35

URL 类别说明

这些 URL 类别与 AsyncOS for Web Security 设备最新版本中所用的类别相同。

URL 类别	缩写	代码	说明	示例 URL
成人	adlt	1006	主要面向成年人，但不一定包含色情内容。内容可能涉及成人俱乐部（脱衣舞俱乐部、换妻俱乐部、三陪服务、脱衣舞表演等）；有关性的一般信息（非色情性质）；生殖器穿刺；成人用品或成人贺卡；不涉及性暗示的有关健康或疾病的内容。	www.adultentertainmentexpo.com www.adultnetline.com
广告	adv	1027	通常会伴随网页显示横幅广告和弹窗广告的网站；其他提供通告内容的广告网站。与广告服务和销售相关的网站属于“商业和工业网站”类别。	www.adforce.com www.doubleclick.com
酒类	alc	1077	涉及以下内容的网站：以酒类为主题的快乐活动；啤酒和葡萄酒酿造、鸡尾酒调制方法；酒商、酒庄、葡萄园、酿酒厂、酒类经销商。与酒瘾相关的网站属于“健康和营养网站”类别。与酒吧和餐厅相关的网站属于“餐饮”网站类别。	www.samueladams.com www.whisky.com

URL 类别	缩写	代码	说明	示例 URL
艺术	art	1002	涉及以下内容的网站：图库和画展；艺术家和艺术；摄影；文献和著作；表演艺术和剧场；音乐；芭蕾；博物馆；设计；建筑。与电影院和电视相关的网站属于“娱乐网站”类别。	www.moma.org www.nga.gov
占星	astr	1074	涉及以下内容的网站：占星术；星座占卜；算命；数字占卜；通灵；塔罗牌占卜。	www.astro.com www.astrology.com
拍卖	auct	1088	涉及以下内容的网站：网络和线下竞拍、拍卖行和分类广告。	www.craigslist.com www.ebay.com
商业和工业	busi	1019	涉及以下内容的网站：市场营销、商务、公司、业务实践、员工、人力资源、交通运输、薪酬、安全和风险投资；办公用品；工业设备（工艺设备）、机器和机械系统；加热设备、冷却设备；材料搬运设备；包装设备；制造业相关的固体物质运输、金属加工、建筑和建造；乘客运输；商业活动；工业设计；建设施工、建筑材料；运输和货运（货运服务、卡车运输、货运代理、卡车运输公司、货运和运输代理、快递服务、空车配运、运输跟踪、铁路运输、海运、货运专线服务、搬运和储存）。	www.freightcenter.com www.staples.com
聊天和即时消息	chat	1040	提供基于 Web 的即时消息和聊天室服务的网站。	www.icq.com www.meebo.com
欺诈和剽窃	plag	1051	助长抄袭，并出于剽窃目的销售书面著作（例如学期论文）的网站。	www.bestessays.com www.superiorpapers.com
虐童内容	cprn	1064	涉及全球违法儿童性侵内容的网站。	—

URL 类别	缩写	代码	说明	示例 URL
计算机安全	csec	1065	为公司和家庭用户提供安全产品和服务的网站。	www.computersecurity.com www.symantec.com
计算机和互联网	comp	1003	有关计算机和软件的信息，例如硬件、软件、软件支持；软件工程师、编程和网络信息；网站设计；常用 Web 和互联网；计算机科学；计算机图形和剪贴画。“免费软件和共享软件网站”单独分为一类。	www.xml.com www.w3.org
约会	date	1055	提供约会、网上交友、婚介服务的网站。	www.eharmony.com www.match.com
数字明信片	card	1082	支持发送数字明信片和电子贺卡的网站。	www.all-yours.net www.delivr.net
餐饮	food	1061	涉及以下内容的网站：餐饮设施；餐厅、酒吧、酒馆和休闲吧；酒店指南和评价。	www.hideawaybrewpub.com www.restaurantrow.com
动态和住宅	dyn	1091	通常表明用户尝试访问其家庭网络的宽带连接 IP 地址（例如远程访问家用计算机）。	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
教育	edu	1001	与教育相关的网站，内容可能涉及学校、学院、大学、教材和教学资源；技术和职业培训；在线培训；教育难题和教育政策；助学金；学校基金；标准和测试。	www.education.com www.greatschools.org
娱乐	ent	1093	涉及以下内容的网站：电影情节或讨论；音乐和乐队；电视；名人和粉丝网站；娱乐新闻；明星八卦；娱乐场所。独立于“艺术网站”类别。	www.eonline.com www.ew.com

URL 类别	缩写	代码	说明	示例 URL
极端	extr	1075	涉及以下内容的网站：具有性暴力或性犯罪性质的材料；暴力和暴力行为；品味低下的材料（通常是血腥暴力的图片，例如尸体解剖照片）；犯罪现场、犯罪和事故受害者的照片；极度淫秽的材料；冲击性网站。	www.car-accidents.com www.crime-scene-photos.com
时尚	fash	1076	涉及以下内容的网站：服装和时尚；发廊；化妆品；饰物；珠宝；香水；与人体改造相关的图片和文字；纹身和穿刺；模特经纪公司。与护肤产品相关的网站属于“健康和营养网站”类别。	www.fashion.net www.findabeautysalon.com
文件传输服务	fts	1071	以提供下载服务和托管文件共享服务为主要目的的文件传输服务网站。	www.rapidshare.com www.yousendit.com
规避过滤网站	filt	1025	推动并帮助实现无法检测的网络使用和匿名网络使用（包括 cgi、php 和 glype 匿名代理服务）的网站。	www.bypassschoolfilter.com www.filterbypass.com
金融	fnnc	1015	在性质上以金融为主的网站，内容可能涉及会计实务和会计人员、税务、税收、银行、保险、投资、国家经济、个人理财（包括所有类型的保险）、信用卡、退休规划和房地产规划、贷款、抵押等。与股票和股份相关的网站属于“在线交易网站”类别。	finance.yahoo.com www.bankofamerica.com
免费软件和共享软件	可用	1068	提供免费软件和共享软件下载服务的网站。	www.freewarehome.com www.shareware.com

URL 类别	缩写	代码	说明	示例 URL
赌博	gamb	1049	涉及以下内容的网站：赌场和网上赌博；庄家和赔率；赌博建议；具有赌博性质的竞速比赛；体育博彩；体育赌博；股票和股份点差交易服务。与戒赌相关的网站属于“健康和营养”网站类别。与政府经营的彩票相关的网站属于“彩票”网站类别。	www.888.com www.gambling.com
游戏	game	1007	涉及以下内容的网站：各种卡片游戏、桌上游戏、文字游戏和视频游戏；对战游戏；体育游戏；可下载的游戏；游戏评论；作弊码；计算机游戏和互联网游戏（例如角色扮演游戏）。	www.games.com www.shockwave.com
政府和法律	gov	1011	涉及以下内容的网站：政府网站；对外关系；与政府和选举相关的新闻和信息；与法律领域相关的信息（例如律师、律师事务所、法律著作、法律参考资料、法院、备审案件目录和法律协会）；立法及判决；民权问题；移民；专利和版权；与执法和执法系统相关的信息；犯罪报告、执法和犯罪统计；军事（例如军队、军事基地、军事组织）；反恐怖主义。	www.usa.gov www.law.com
黑客攻击	hack	1050	讨论如何绕过网站、软件和计算机安全保护的网站。	www.hackthissite.org www.gohacking.com
仇恨言论	hate	1016	煽动以下内容的网站：基于社会团体、肤色、宗教信仰、性取向、残疾、阶级、种族、民族、年龄、性别和性身份的仇恨、蔑视和歧视；种族主义；性别歧视；种族神学；厌世音乐；新纳粹组织；种族优越主义；否认大屠杀。	www.kkk.com www.nazi.org

URL 类别	缩写	代码	说明	示例 URL
健康和营养	hlth	1009	涉及以下内容的网站：卫生保健；疾病和残疾；医疗；医院；医生；医用药物；心理健康；精神病学；药物学；锻炼和健身；身体残疾；维生素和营养品；与性相关的健康知识（疾病和医疗）；与吸烟、饮酒、吸毒和赌博相关的健康知识（疾病和医疗）；与食物相关的一般知识；食物和饮料；烹饪和菜谱；食物与营养、健康、节食；烹饪方法（包括菜谱和烹饪网站）；替代疗法。	www.health.com www.webmd.com
幽默	lol	1079	与笑话、涂鸦、漫画和其他幽默内容相关的网站。与可能具有冒犯性的成人幽默相关的网站属于“成人网站”类别。	www.humor.com www.jokes.com
非法活动	ilac	1022	煽动犯罪的网站，内容可能涉及：盗窃、欺诈、非法接入电话网络；计算机病毒；恐怖主义、炸弹和无政府主义。也包括描述谋杀和自杀以及介绍谋杀和自杀方法的网站。	www.ekran.no www.thedisease.net
非法下载	ildl	1084	提供以下下载内容的网站：软件或其他材料、序列号、密钥生成器，以及违反版权协议绕过软件保护的工具。与 Torrent 下载相关的网站属于“对等文件传输网站”类别。	www.keygenguru.com www.zcrack.com
违禁药物	drug	1047	此类网站提供有关娱乐性毒品、吸毒工具，以及毒品购买和制造的信息。	www.cocaine.org www.hightimes.com
基础设施和内容交付网络网站	infr	1018	内容交付基础设施和涉及动态生成内容的网站；由于安全原因而无法更具体分类的网站，或者难以分类的网站。	www.akamai.net www.webstat.net
互联网电话服务	voip	1067	提供基于互联网的电话服务的网站。	www.evaphone.com www.skype.com

URL 类别	缩写	代码	说明	示例 URL
求职	作业	1004	涉及以下内容的网站：职业建议；编写简历和应对面试的技巧；就业服务；职位数据库；固定职业和临时职业介绍所；招聘网站。	www.careerbuilder.com www.monster.com
女用内衣和泳装	ling	1031	贴身衣服和泳装，特别是做模特时。	www.swimsuits.com www.victoriassecret.com
彩票	lotr	1034	与奖券、竞赛和国家赞助的彩票相关的网站。	www.calottery.com www.flalottery.com
手机	cell	1070	短消息服务 (SMS)、铃声和手机下载。移动运营商网站属于“商业和工业网站”类别。	www.cbfsms.com www.zedge.net
自然	natr	1013	涉及以下内容的网站：自然资源；生态学和环境保护；森林；原野；植物；花；森林保护；森林、原野和林业实践；森林管理（重新造林、森林保护、保持、砍伐、森林健康状况、抚育间伐和计划烧除）；农业实践（农学、园艺、园林、景观、绿化、除草、灌溉、修剪和收割）；污染问题（空气质量、危险废弃物、污染防治、回收利用、废弃物管理、水质和环境清理行业）；动物、宠物、家畜和动物学；生物学；植物学。	www.enature.com www.nature.org
新闻	新闻	1058	涉及以下内容的网站：新闻；头条新闻；报纸；电视台；杂志；天气；滑雪条件。	www.cnn.com news.bbc.co.uk
非政府组织	ngo	1087	非政府组织（如俱乐部、游说团、社区、非营利组织和工会）的网站。	www.panda.org www.unions.org
非色情裸体	nsn	1060	涉及以下内容的网站：裸体主义和裸体行为；自然崇拜；裸体主义者联盟；裸体艺术。	www.artenuda.com www.naturistsociety.com

URL 类别	缩写	代码	说明	示例 URL
在线社区	comm	1024	涉及以下内容的网站：有亲密关系的群体；有特殊爱好的群体；网络新闻组；网络论坛。不包括“职业社交网站”类别或“社交网络”类别的网站。	www.igda.org www.ieee.org
在线存储和备份	osb	1066	出于备份、共享和托管目的提供离线和对等存储的网站。	www.adrive.com www.dropbox.com
在线交易	trad	1028	涉及以下内容的网站：网上证券交易；与股市、股票、债券、共同资金、经纪人、股票分析和股评、股市行情、股票走势、IPO 和股票分割相关的信息。也包括支持用户在线交易股票的网站。股票和股份点差交易服务属于“赌博”类别。其他金融服务属于“财务”类别。	www.tdameritrade.com www.scottrade.com
组织电子邮件	pem	1085	用于访问企业邮件的网站（通常通过 Outlook Web Access 访问）。	—
寄放域	park	1092	通过使用广告网络付费列表的域，对流量进行收费的网站；或者由希望出售域名以谋取利润的“投机者”拥有的网站。此类网站也包括含有付费广告链接的虚假搜索网站。	www.domainzaar.com www.parked.com
对等文件传输	p2p	1056	对等文件请求网站。此类网站不会对文件传输进行跟踪。	www.bittorrent.com www.limewire.com
个人网站	pers	1081	与个人相关或由个人运营的网站；个人主页服务器；含有个人内容的网站；没有特定主题的个人博客。	www.karymullis.com www.stallman.org
照片搜索和图像	img	1090	为存储和搜索图片、照片和剪贴画提供便利的网站。	www.flickr.com www.photobucket.com
政治	pol	1083	涉及以下内容的网站：政治家；政党；与政治、选举，民主和投票相关的新闻和信息。	www.politics.com www.thisnation.com

URL 类别	缩写	代码	说明	示例 URL
色情	porn	1054	含有露骨的色情文字或内容的网站。内容可能涉及露骨的动画和卡通；一般的露骨内容；其他色情材料；毫无隐晦的聊天室；情爱模拟器；脱衣扑克游戏；成人电影；猥亵的艺术；基于 Web 的露骨邮件。	www.redtube.com www.youporn.com
职业社交网络	pnet	1089	以事业或职业发展为目的的社交网络。另请参阅“社交网络”。	www.linkedin.com www.europeanpwn.net
房地产	rest	1045	为帮助搜索以下内容提供信息的网站：房地产；办公室和商业场所；房地产列表（如出租房屋、公寓和住宅）；住宅建筑。	www.realtor.com www.zillow.com
参考	ref	1017	涉及以下内容的网站：城市和州指南；地图、时间；参考源；词典；资料库。	www.wikipedia.org www.yellowpages.com
宗教	版本	1086	涉及宗教内容和宗教信息的网站；宗教社区。	www.religionfacts.com www.religioustolerance.org
SaaS 和 B2B	saas	1080	提供在线业务服务以及支持在线会议的网络门户。	www.netsuite.com www.salesforce.com
儿童安全	kids	1057	专门面向少年儿童（尤其是经过批准）的网站。	kids.discovery.com www.nickjr.com
科技	sci	1012	与科学技术相关的网站，内容可能涉及航空航天、电子、工程、数学和其他类似学科；太空探索；气象学；地理；环境；能源（化石能源、核能、可再生能源）；通信（电话、电信）。	www.physorg.com www.science.gov
搜索引擎和门户	srch	1020	搜索引擎以及其他访问互联网信息的入口点。	www.bing.com www.google.com
性教育	sxed	1052	如实介绍性、性健康、避孕和怀孕知识的网站。	www.avert.org www.scarleteen.com

URL 类别	缩写	代码	说明	示例 URL
购物	shop	1005	涉及以下内容的网站：以物换物；网络购物；优惠券和赠品；常规办公用品；在线目录；在线商城。	www.amazon.com www.shopping.com
社交网络	snet	1069	社交网络. 另请参阅“专业网络网站”。	www.facebook.com www.twitter.com
社会科学	socs	1014	涉及以下内容的网站：与社会相关的科学和历史；考古学；人类学；文化研究；历史；语言学；地理学；哲学；心理学；女性研究。	www.archaeology.org www.anthropology.net
社会文化	scty	1010	涉及以下内容的网站：家族和关系；种族；社会组织；家谱；敬老；儿童看护。	www.childcare.gov www.familysearch.org
软件更新	swup	1053	托管软件包更新的网站。	www.softwarepatch.com www.versiontracker.com
体育和娱乐网站	sprt	1008	涉及以下内容的网站：各种体育运动（职业和业余）；娱乐活动；钓鱼；梦幻竞技；公园；游乐园；水上公园；主题公园；动物园和水族馆；SPA。	www.espn.com www.recreation.gov
流式音频	aud	1073	提供实时音频流内容（包括互联网电台和音频源）的网站。	www.live-radio.net www.shoutcast.com
视频流	vid	1072	提供实时流式视频（包括互联网电视、网播和共享视频）的网站。	www.hulu.com www.youtube.com
烟草	tob	1078	烟草宣传网站；烟草制造商网站；有关烟斗和吸烟产品（不是用于非法吸毒目的）的网站。与烟瘾相关的网站属于“健康和营养网站”类别。	www.bat.com www.tobacco.org

URL 类别	缩写	代码	说明	示例 URL
交通运输业	trns	1044	涉及以下内容的网站：个人交通；有关汽车和摩托车的信息；全新和二手汽车与摩托车的商店；汽车俱乐部；船只、飞机、房车 (RV) 和其他类似物品。说明：汽车和摩托车比赛属于“体育和娱乐网站”类别。	www.cars.com www.motorcycles.com
差旅费	trvl	1046	涉及以下内容的网站：商务和个人旅行；旅游信息；旅游资源；旅行社；度假套装；游轮航线；住宿和宿泊；旅行交通；航班预订；机票；租车；度假屋。	www.expedia.com www.lonelyplanet.com
未分类	-	-	未包含在思科数据库中的网站将被分类为“未分类网站”，以便于报告。此类网站可能包括输入错误的 URL。	—
武器	weap	1036	此类网站提供有关常规武器购买或使用的信息，例如枪支贩卖商、枪支拍卖、枪支分类广告、枪支配件、枪展和枪支培训；有关枪的一般信息。此类网站也可能包括其他武器和图片搜索网站。政府军事网站属于“政府和法律网站”类别。	www.coldsteel.com www.gunbroker.com
Web 托管	whst	1037	提供 Web 托管和带宽服务的网站。	www.bluehost.com www.godaddy.com
网页翻译网站	tran	1063	在不同语言之间翻译网页的网站。	babelfish.yahoo.com translate.google.com
基于网络的邮件	mail	1038	提供基于 Web 的公共邮件服务的网站。为个人访问其公司或组织的邮件服务提供支持的网站属于“组织邮件网站”类别。	mail.yahoo.com www.hotmail.com

确定 URL 的类别

要查找特定 URL 的类别，请访问报告未分类和误分类的 URL , on page 35中显示的站点。

报告未分类和误分类的 URL

要报告归类错误的 URL 及未归类而应归类的 URL，请访问：

https://talosintelligence.com/reputation_center/support

要检查已提交的URL 的状态，请点击此页面上的**有关已提交 URL 的状态 (Status on Submitted URLs)** 选项卡。

将来的 URL 类别集变更

难得，URL 类别集会随着新兴趋势和技术的发展而变化。例如，可能会添加、删除、重命名某个类别，也可能会将其与其他类别合并或拆分为两个类别。这些变化可能会影响现有过滤器的结果，因此如果发生变化，邮件网关将发送警报（“系统”类型，“警告”严重性）。如果您收到此类警报，可以评估和更新处理更新类别的内容和邮件过滤器。现有过滤器不会自动更改。要确保收到这些警报，请参阅添加警报收件人。

以下更改不需要更改类别集，并且不会生成警报：

- 例行归类新分类的站点。
- 将分类错误的站点重新归类。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。