URL 过滤

您可以使用访问控制规则实施 URL 过滤。

URL 过滤概述

使用 URL 过滤功能控制网络上的用户可以访问的网站：

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。这是建议选项。
- 手动 URL 过滤 - 通过任意许可证，可以手动指定单个 URL、URL 组以及 URL 列表和源，以实现对网络流量的精细、自定义控制。有关详细信息，请参阅手动 URL 过滤， 第 15 页。

另请参阅安全情报，用于阻止恶意 URL、域和 IP 地址的类似但不同的功能。

关于使用类别和信誉进行 URL 过滤

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，ebay.com 属于“拍卖”类别，而 monster.com 属于“职位搜索”类别。

  URL 可以属于多个类别。

- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。信誉的范围从 未知风险（第 0 级）或 不可信（第 1 级）到 信任（第 5 级）。

基于类别和信誉的 URL 过滤的优势

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问控制来阻止黑客攻击 类别中的 不可信 的 URL。 或者，您可以使用 QoS 对来自视频流类别中站点的流量进行速率限制。也存在基于威胁类型的类别，例如间谍软件和广告软件类别。

使用类别和信誉数据可简化策略创建和管理。此方法可保证系统按预期控制网络流量。由于思科会不断更新有关新 URL 的威胁情报以及现有 URL 的新类别和新风险的信息，因此系统会使用最新信息来过滤所请求的 URL。代表安全威胁的站点或提供不良内容的站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下是一些系统如何适应的示例：

- 如果某个访问控制规则阻止所有游戏网站，在新域注册并分类为“游戏”时，系统则可以自动阻止这些站点。 同样，如果 QoS 规则对所有 视频流 站点进行速率限制，则系统可自动限制流向新 视频流 站点的流量。
- 如果某个访问控制规则阻止所有恶意软件站点，而某个购物页面受到恶意软件感染，系统可以将来自该购物站点的 URL 重新分类为恶意软件站点，并阻止该站点。
- 如果访问控制规则阻止不可信社交网站，但有人在其个人资料页面发布的链接中提供有指向恶意负载的链接，则系统便可以将该页面的信誉从 可靠更改为 不可信，并阻止该网站。

解密策略 “不解密”规则中基于类别的过滤的限制

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 情报组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。

注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践。

有关详细信息，请参阅 在 URL 过滤中使用类别 ，第 7 页。

URL 类别和信誉说明

类别说明

可从https://www.talosintelligence.com/categories中获取每个 URL 类别的说明。

要查看那些类别，请确保点击 **威胁类别** 。

信誉级别说明

转至 https://talosintelligence.com/reputation_center/support 并查看“常见问题”部分。

来自思科云的 URL 过滤数据

添加 URL 过滤许可证将自动启用启用 URL 过滤。允许根据网站的一般分类或 类别和风险级别或 信誉来进行流量过渡。

默认情况下，当用户浏览的URL的类别和信誉不在以前访问过的网站的本地缓存中时，系统会将其提交到云进行威胁情报评估，并将结果添加到缓存中。

或者，您可以使用类别和信誉的本地 URL 数据集，这可以加快 Web 浏览速度。当您启用（或重新启用）URL 过滤时， 管理中心 会自动向思科查询 URL 数据并将数据集推送到受管设备。然后，当用户浏览到某个URL时，系统会在将其提交到云进行威胁情报评估之前，检查本地数据集和缓存中的类别和信誉信息。要查看使用本地数据集的选项，包括如何完全禁用单个云查找，请参阅URL过滤选项，第 10 页。

默认情况下，启用 URL 数据的自动更新；我们强烈建议您不要禁用这些更新。

URL 类别集可能会定期更改。当您收到更改通知时，请检查您的 URL 过滤配置，以确保按预期处理流量。有关详细信息，请参阅如果 URL 类别集发生更改，请执行操作，第 21 页。

URL 过滤的最佳实践

请记住以下的 URL 过滤的准则和限制：

按照类别和信誉过滤

请按照如何使用类别和信誉配置 URL 过滤，第 9 页 中的相关说明来操作。

配置策略以检查在可以识别 URL 之前必须通过的数据包

在满足以下情况之前，系统无法过滤 URL：

- 客户端与服务器之间建立受监控连接。
- 系统识别会话中的 DNS，HTTP 或 HTTPS 应用。
- 系统识别所请求的 域或URL（对于加密会话，从 一个非加密的域名、ClientHello 消息或服务器证书中获取）。

此识别应在 3 到 5 个数据包内发生，或者在 TLS/SSL 握手中的服务器证书交换（如果流量已加密）后发生。

重要提示！要确保您的系统检查否则会通过的这些初始数据包，请参阅在识别流量之前检查通过的数据包和子主题。

如果早期流量与所有其他规则条件都匹配，但是识别未完成，则系统允许数据包通过并建立连接（或完成 TLS/SSL 握手）。在系统完成其识别后，系统会将相应的规则操作应用于剩余会话流量。

阻止威胁类别

请确保您的策略专门处理威胁类别，以识别已知的恶意站点。除了阻止信誉不佳的站点之外，请执行此操作。

例如，要保护网络免受恶意站点的攻击，必须阻止所有威胁类别。此外，Talos 建议您仅阻止类别为“差”的站点。如果您具有积极的安全状态，可以阻止可疑的信誉，但这可能会导致更多的误报。

有关详细信息，请参阅 URL 类别和信誉说明，第 2 页中的 URL中的 **威胁类别** 。

URL 条件和规则顺序

- 将 URL 规则置于 必须 命中的所有其他规则之后。
- URL 可以属于多个类别。可以允许一个类别的网站并阻止另一个类别的网站，无论是明确地还是依赖于默认操作。在这种情况下，请确保创建 URL 规则并对其进行排序，从而获得预期效果，具体取决于允许还是阻止应优先。

有关规则的其他指南，请参阅以下主题：访问控制规则的最佳实践。

未分类或无信誉的 URL

在构建 URL 规则时，首先应选择要匹配的类别。如果您明确选择 **未分类** URL，但不能通过信誉进一步限制。

具有“不受信任”信誉的未分类URL由 **恶意站点** 类别处理。如果要阻止具有任何其他信誉级别的未分类站点（例如“可疑”），则必须阻止所有未分类的站点。

选择类别和信誉级别后，可以选择 **应用到未知信誉**。例如，您可以创建应用于信誉不受信任，可疑和未知的站点的规则。

不能为 URL 手动分配类别和信誉，但在访问控制和 QoS 策略中，可以手动阻止特定 URL。请参阅手动 URL 过滤，第 15 页。另请参阅争议 URL 类别和信誉，第 20 页。

针对已加密 Web 网络流量的 URL 过滤

在对加密的 Web 网络流量执行 URL 过滤时，系统将：

- （如果已启用DNS过滤）检查系统之前是否已发现源域或该域在本地信誉数据库中，如果是，则根据域的信誉和类别执行操作。否则，即使已在访问控制策略的高级设置中启用 **重试URL缓存缺失查找** ，系统也会根据您的加密流量配置处理流量。
- 不考虑加密协议；如果规则包含URL条件，但不包含指定协议的应用条件，该规则将同时匹配 HTTPS 和 HTTP 流量。
- 不使用 URL 列表。您必须改用 URL 对象和组。
- 根据用于加密流量的公钥证书中的使用者公用名匹配HTTPS流量，并评估事务期间随时提供的任何其他 URL（包括解密后的 HTTP URL）的信誉。

- 不考虑对象公用名内的子域。
- 不显示被访问控制规则（或任何其他配置）阻止的已加密连接的 HTTP 响应页面；请参阅对 HTTP 响应页面的限制，第 17 页。

URL 过滤和 TLS 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

访问控制策略高级设置为 TLS 服务器身份发现提供 **早期应用检测和 URL 分类** 选项。

我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。解密策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

注释

- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Cisco Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由 Cisco Secure Firewall Management Center管理的此类受管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。
- TLS 服务器身份发现也可在 TLS 1.2 会话上运行。

有关详细信息，请参阅访问控制策略高级设置。

HTPP/2

系统可从 TLS 证书提取 HTTP/2 URL，但无法从负载进行提取。

手动 URL 过滤

- 使用自定义安全情报列表或源对象指定 URL。请勿使用 URL 对象或直接在规则中输入 URL。有关详细信息，请参阅手动 URL 过滤选项，第 15 页。
- 如果使用 URL 对象手动过滤特定 URL 或通过直接在规则中输入 URL，请仔细考虑可能会受到影响的其他流量。要确定网络流量是否与URL条件相匹配，系统执行简单的子字符串匹配。如果请求的 URL 与字符串的任何部分匹配，则认为该 URL 匹配。
- 如果使用手动URL过滤创建其他规则的例外情况，请将具有例外情况的特定规则置于本应适用的一般规则之上。

在 URL 中搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，系统不会阻止使用网络搜索来搜索 amazon.com，但会阻止浏览至 amazon.com。

高可用性部署中的 URL 过滤

有关使用高可用性中的 Firepower 管理中心进行 URL 过滤的指南，请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的 *URL* 过滤和安全情报。

所选设备型号的内存限制

- 内存较少的设备型号在本地存储较少的URL数据，因此系统可能会更频繁地检查云，以确定不在本地数据库中的站点的类别和信誉。

  内存较低的设备包括：

  - Firepower 1010
  - Threat Defense Virtual 配备 8 GB RAM

威胁防御中恢复 TLS 会话的 URL 匹配

在以下条件下使用与 Snort 2 的 URL 匹配：

- 如果没有 TLS 会话恢复且已启用 SSL 策略，或者客户端 Hello 消息包含服务器名称指示 (SNI) 扩展名。
- 如果存在 TLS 会话恢复且未启用 SSL 策略，或者客户端 Hello 消息不包含 SNI 扩展。

过滤 HTTPS 流量

要过滤加密流量，系统将根据 TLS/SSL 握手期间传递的信息确定请求的URL：用于加密流量的公钥证书中的使用者公用名。

HTTPS 过滤与 HTTP 过滤不同，它不考虑使用者公用名称内的子域。在访问控制或 QoS 策略中手动过滤 HTTPS URL 时，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

提示 在 解密策略中，可以通过定义可分辨名称 解密策略 规则条件来处理和解密发送到特定 URL 的流量。证书的使用者可分辨名称中的公用名属性包含站点的 URL。通过解密 HTTPS 流量，访问控制规则可以评估解密的会话，从而改进 URL 过滤。

按加密协议控制流量

系统在访问控制或 QoS 策略中执行 URL 过滤时，不考虑加密协议（HTTP 与 HTTPS）。对于手动 URL 条件和基于信誉的 URL 条件均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- http://example.com/
- https://example.com/

要配置仅与 HTTP 或 HTTPS 流量匹配的规则，请向该规则添加应用条件。例如，可以通过构造两个访问控制规则（每个规则具有应用和 URL 条件）来允许对某个站点进行 HTTP 访问，同时禁止 HTTP 访问。

第一个规则允许 HTTPS 流量到达网站：

操作：允许
应用：HTTPS
URL：example.com

第二个规则阻止对同一网站进行 HTTP 访问：

操作：阻止
应用：HTTP
URL：example.com

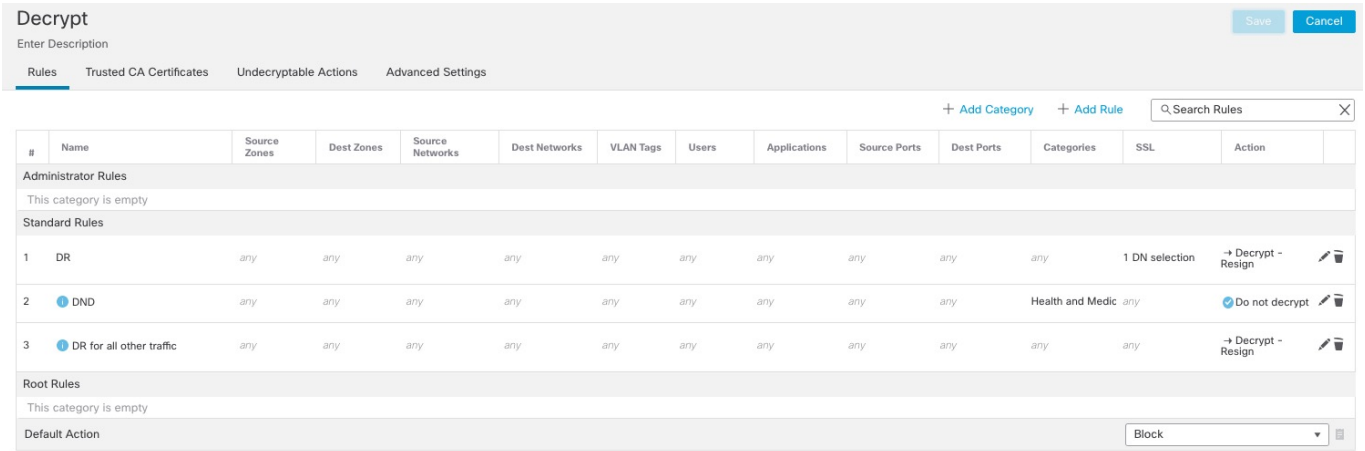
在 URL 过滤中使用类别

“不解密”规则中的类别限制

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 情报组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进 URL 过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅 使用 TLS/SSL 解密的准则。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践。

URL 过滤的许可证要求

威胁防御 许可证

- 类别和信誉过滤 - URL 过滤
- 手动过滤 - 无其他许可证。

经典许可证

- 类别和信誉过滤 - URL 过滤
- 手动过滤 - 无其他许可证。

威胁防御设备的 URL 过滤许可证

请参阅 思科安全防火墙管理中心管理指南的 许可证 一章中的 *URL* 许可证 。

URL 过滤的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

如何使用类别和信誉配置 URL 过滤

	相应操作	更多信息
第 1 步	确保拥有正确的许可证。	将 URL 过滤许可证分配给将过滤 URL 的每个托管设备。
第 2 步	确保 管理中心 可以与云通信以获取 URL 过滤数据。	《Cisco Secure Firewall Management Center 管理指南》中的互联网接入要求 和 通信端口要求 。
第 3 步	了解限制和准则并采取任何必要的措施。	URL 过滤的最佳实践， 第 3 页
第 4 步	启用 URL 过滤功能。	使用类别和信誉启用 URL 过滤， 第 10 页
第 5 步	配置规则以按类别和信誉过滤 URL。	配置 URL 条件， 第 11 页 为了最好地防御恶意站点，您必须按信誉阻止站点，并阻止所有威胁类别中的 URL。 （选件）补充或选择性覆盖基于类别和信誉的 URL 过滤， 第 16 页
第 6 步	（可选）允许用户能够通过点击忽略警告页面来绕过对网站的阻止。	配置 HTTP 响应页面， 第 16 页
步骤 7	对规则进行排序，使流量首先命中关键规则。	URL 规则顺序
第 8 步	（可选）修改与URL过滤相关的高级选项。	通常，除非您有特定的原因需要更改默认值，否则请使用默认值。 有关高级选项的信息，包括以下内容，请参阅访问控制策略高级设置。 • **要在连接事件中存储的最大 URL 字符数** • **允许交互式阻止绕过阻止的时长（秒）** • **重试 URL 缓存缺失查询** • **对 DNS 流量启用信誉实施**
步骤 9	部署更改。	部署配置更改
步骤 10	确保系统按预期接收未来的URL数据更新	配置 URL 过滤运行状况监控器， 第 20 页
步骤 11	确保您已启用其他功能来保护网络免受恶意站点的攻击	请参阅安全情报。

使用类别和信誉启用 URL 过滤

您必须是管理员用户才能执行此任务。

开始之前

按照 如何使用类别和信誉配置 URL 过滤，第 9 页中所述，完成所有前提条件。

过程

步骤 1 选择**集成** > **其他集成**。

步骤 2 请点击 **云服务**。

步骤 3 配置 URL 过滤选项，第 10 页。

步骤 4 点击**保存 (Save)**。

URL 过滤选项

添加 URL 过滤许可证将自动启用启用 URL 过滤。允许根据网站的一般分类或 类别和风险级别或 信誉来进行流量过渡。

虽然默认情况下系统配置为将所有URL提交到云以进行威胁情报评估，但使用类别和信誉数据的本地数据集可以提高 Web 浏览速度。当您启用（或重新启用）URL 过滤时， 管理中心 会自动向思科查询 URL 数据并将数据集推送到受管设备。此过程可能需要一些时间。

如果您使用 SSL 规则处理已加密的流量，则另请参阅 解密规则 准则和限制。

启用自动更新

如果**启用自动更新**（默认），则 管理中心 每 30 分钟会检查一次云以获取更新。如果需要严格控制系统联系外部资源的时间，可以禁用自动更新，改为使用调度程序创建定期任务。请参阅在《Cisco Secure Firewall Management Center 管理指南》中 使用已安排任务自动执行 *URL* 过滤更新 。

立刻更新

点击 **立即更新** 以执行一次性的按需 URL 数据更新。如果有更新正在进行，则不能启动按需更新。虽然每日更新通常是小量更新，但如果距离上一次更新超过五天，新的 URL 数据最多可能需要 20 分钟才能下载完，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

URL 查询源

您可以选择系统如何为用户浏览的 URL 分配类别和信誉。您可以选择：

- **仅本地数据库**：仅使用本地数据集。如果您不想将未分类的 URL（类别和声誉不在本地数据集中）提交给思科，例如出于隐私原因，则可以使用此选项。但请注意，与未分类URL的连接不会与使用基于类别或信誉的URL条件的规则进行匹配。在这种情况下，您将无法手动对该URL指定类别或信誉。

- **本地数据库和思科云 (Local Database and Cisco Cloud)**：尽可能使用本地数据集，这样可以加快Web浏览速度。当用户浏览到类别和信誉不在本地数据集或之前访问过的网站缓存中的URL时，系统会将其提交到云端进行威胁智能评估，并将结果添加到缓存中。
- **仅思科云**（默认）：不使用本地数据集。当用户浏览到类别和信誉不在之前访问过的网站的本地缓存中的URL时，系统会将其提交到云端进行威胁智能评估，并将结果添加到缓存中。此选项可保证获得最新的类别和信誉信息。

  此选项需要威胁防御版本 7.3。如果启用此选项，运行较早版本的设备将使用 **本地数据库和思科云** 选项。

已缓存的 URL 到期

如果您选择 **仅本地数据库** 作为 URL 查询源，则此设置不相关。

缓存类别和信誉数据使Web浏览速度更快。默认情况下，URL 的缓存数据永不过期，以获得最快的性能。

要尽量减少与过时数据匹配的 URL 实例，可以将缓存中的 URL 设置为过期。要获得更高的威胁数据准确性和通用性，请选择较短的到期时间。经过指定的时间之后，系统将在网络上的用户第一次访问缓存的 URL 后刷新缓存的 URL。第一个用户看不到刷新的结果，但访问此 URL 的下一个用户将会看到刷新的结果。

配置 URL 条件

通过根据 URL 类别和信誉控制对站点的访问来保护您的网络。

开始之前

注意 作为前提条件，请确保在访问控制策略的顶部至少创建一个包含类别或信誉参数的监控规则。这对于查看符合特定访问控制策略的任何 URL 的任何类别或信誉数据至关重要。

如果访问控制策略中没有配置类别或信誉参数的规则，则管理中心的“**连接事件**”页面不会显示任何命中访问控制策略的 URL 流量的类别或信誉数据。

过程

步骤 1 在规则编辑器中，点击 URL 条件的以下：

- 访问控制或 QoS-点击 **URLs**。
- SSL-点击 **类别**。

步骤 2 查找并选择要控制的 URL 类别：

在访问控制 或 QoS 规则中，点击 **类别**。

要有效保护网络免受恶意站点的攻击，必须阻止所有威胁类别 URL。此外，Talos 建议您仅阻止类别为“差”的站点。如果您具有积极的安全状态，可以阻止可疑的信誉，但这可能会导致更多的误报。有关威胁类别列表，请参阅URL 类别和信誉说明，第 2 页。

请务必点击列表底部的箭头以查看所有可用类别。

步骤 3 （可选）通过选择**信誉 (Reputation)** 来限制 URL 类别。

请注意，如果您明确匹配**未分类**URL，但不能通过信誉进一步限制。选择信誉级别也会将比您选择的级别更高或更低的其他信誉包括在内，具体取决于规则操作：

- 如果规则允许或信任网络流量，则包括级别更低的信誉。例如，如果您将访问控制规则配置为允许良性（4 级），系统还会自动允许受信任（5 级）站点。
- 如果规则对网络流量进行速率限制、解密、阻止或监控，则包括级别更高的信誉。例如，如果将访问控制规则配置为阻止可疑站点（2 级），则系统还会阻止不受信任（1 级）站点。

如果更改规则操作，则系统会自动更改 URL 条件中的信誉级别。

或者，选择 **应用到未知信誉**。

步骤 4 点击 **添加 URL** 或 **添加到规则**，或进行拖放操作。

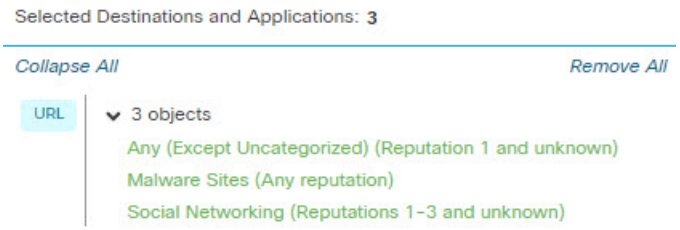
步骤 5 （可选）要在访问控制或 QoS 规则中选择预定义的 URL 对象或 URL 列表和源，请点击 **URL**，选择对象，然后将其添加到目标。

这些对象实施手动 URL 过滤，而不是基于类别的过滤。

步骤 6 保存或继续编辑规则。

示例：访问控制规则中的 URL 条件

下图显示用于阻止以下内容的访问控制规则的 URL 条件：所有具有中性或更差的信誉级别的恶意软件站点、所有不受信任站点以及所有社交站点。



下表总结如何构建该条件。

受阻 URL	类别	信誉
恶意软件站点，无论信誉如何	恶意软件网站	任意
任何不受信任的 URL（1 级）	任意	1 - 不受信任

受阻 URL	类别	信誉
具有声誉等级为中性或更差 （1 至 3 级）的社交站点	社交网络	3 - 中性

具有 URL 条件的规则

下表列出了支持 URL 条件的规则，以及每个规则类型支持的过滤类型。

规则类型	是否支持类别和信誉过滤？	支持手动过滤？
访问控制	兼容	兼容
解密策略	兼容	否；使用可分辨名称条件
QoS	兼容	兼容

要在具有 **不解密** 规则条件的 a 解密策略 中使用 URL 过滤，请参阅 在 URL 过滤中使用类别 ，第 7 页。

URL 规则顺序

为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

如果为规则配置例外，请将例外置于另一条规则之上。

DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别

默认情况下，在每个新访问控制策略的 **高级** 选项卡上启用 **启用对 DNS 流量的信誉实施** 选项。 此选项会轻微修改 URL 过滤行为，并且仅在启用和配置 URL 过滤时适用。

当此选项启用：

- 当浏览器查找域名以获取 IP 地址时，系统会在 URL 事务中尽早评估域类别和信誉
- 加密流量的类别和信誉通常无需解密即可确定

  如果 DNS 过滤无法确定加密流量的 URL，则使用您的加密流量配置处理该流量。

启用 DNS 过滤以在域查找期间识别 URL

默认情况下，在新的访问控制策略中启用DNS过滤。但是，可能需要其他配置才能使此设置生效。

开始之前

- 必须许可、启用和配置使用类别和信誉的 URL 过滤。

  （DNS 过滤不使用 URL 选项卡中的以下设置：URL 组、URL 对象、URL 列表和源，以及输入到“输入 URL”文本框中的 URL。）

- 请参阅 DNS 过滤限制，第 14 页中的限制。

过程

步骤 1 在访问控制策略的高级设置中，选择 **对 DNS 流量启用信誉实施**。

步骤 2 在同一策略中，对于配置了 URL 类别和信誉阻止的每个访问控制规则：

- 应用条件 - 如果应用条件不是**任何**（或为空），则将 **DNS** 添加到该列表。其他与 DNS 相关的选项与此目的无关。
- 端口条件 - 如果端口/协议条件不是**任何**（或为空），请添加 **DNS_over_TCP** 和 **DNS_over_UDP**。

步骤 3 保存更改。

下一步做什么

如果您已完成更改：部署配置更改

DNS 过滤限制

匹配具有**阻止并重置**、**交互式阻止**或**交互式阻止并重置**操作的规则的流量将被视为规则操作为**阻止**。

尝试访问阻止的URL的最终用户会遇到无法解释的无法连接到其页面的情况；连接将旋转，然后超时。

DNS 过滤和事件

由 DNS 过滤生成的连接事件使用以下特别需要关注的字段记录：DNS 查询、URL 类别、URL 信誉和目标端口。DNS 查询字段包含域名；对于 DNS 过滤匹配，URL 字段将为空。目的端口将是 53。

另外：

- 当访问控制规则操作为**允许**或**信任**时，将为同一流量生成两个连接事件，一个用于 DNS 过滤（填充 **DNS 查询 (DNS Query)** 字段），另一个用于 URL 过滤（填充 **URL** 字段）。
- 系统第一次遇到特定 URL 时，您将看到该单个会话的两个事件：一个事件显示 DNS 查询未分类/无信誉，一个事件显示 URL 的实际类别和信誉，这些是在 DNS 期间检索到的使用标准 URL 过滤进行处理时，将查询 和 应用于会话。

手动 URL 过滤

在访问控制和 QoS 规则中，您可以通过手动过滤单个 URL、URL 组 或 URL 列表和源，补充或选择性地覆盖基于类别和信誉的 URL 过滤。

例如，您可使用访问控制阻止不适合您的组织的网站类别。但是，如果该类别包含合适的网站，并且您要为其提供访问权限，则您可以为该站点创建手动的“允许”(Allow) 规则，然后将其置于该类别的“阻止”(Block) 规则之前。

您可以在没有特殊许可证的情况下执行此类 URL 过滤。

SSL 规则不支持手动 URL 过滤；相反，使用可分辨名称条件。

⚠

注意 根据您实施手动 URL 过滤的方式，URL 匹配可能不是您想要的。请参阅手动 URL 过滤选项，第 15 页。

手动 URL 过滤选项

有几种方法可以指定用于手动 URL 过滤的 URL：

选项	说明
（**最佳实践**） 使用自定义安全情报 URL 列表或源对象。	这是推荐的手动 URL 过滤方法。 您可以创建新列表或源，也可以在访问控制或 QoS 规则中选择现有列表或源。 有关信息，请参阅 自定义安全情报列表和源 和子主题。
单独或作为组使用 URL 对象。有关 URL 对象的说明，请参阅 URL。 或 将 URL 直接输入到访问控制规则中。（Web 界面中规则页面上的 **输入URL** 选项。）	如果不包含路径（即URL 中无/字符），则匹配仅基于服务器主机名。如果包含一个或多个/字符，则整个URL 字符串将用于子字符串匹配。然后，如果满足以下任一条件，则 URL 被视为匹配项： • 字符串位于 URL 的开头。 • 字符串后面有一个点。 • 字符串开头包含一个点。 • 字符串后面跟有 :// 字符。 例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。 **注释** 我们建议您不要使用手动URL 过滤阻止或允许个别网页或部分网站（即，带有 / 字符的 URL），因为这样可能会重组服务器并将页面移至新路径。 **输入 URL** 选项不支持通配符。

补充或选择性覆盖基于类别和信誉的 URL 过滤

在访问控制或 QoS 规则中，可以使用安全情报 URL 列表和源来补充或指定基于类别和信誉的 URL 过滤规则的例外情况。

重要提示！如果您在此过程中配置的列表或源包含基于类别或信誉的规则的例外情况，请按规则顺序将此规则置于这些规则之上。

在 SSL 规则中，使用可分辨名称条件配置并行行为。

开始之前

- 使用类别和信誉配置 URL 过滤请参阅配置 URL 条件，第 11 页。
- 了解手动 URL 过滤的重要最佳实践。请参阅URL 过滤的最佳实践，第 3 页和手动 URL 过滤选项，第 15 页。
- 配置一个或多个包含要用于手动过滤的URL的安全情报对象（列表或源）。请参阅自定义安全情报列表和源。

过程

步骤 1 导航至您将在其中定义规则的访问控制或 QoS 策略。

步骤 2 创建或编辑要在其中添加新条件的规则：

- 如果要补充基于类别或信誉的 URL 过滤规则，请编辑现有规则。
- 如果要覆盖或创建基于类别或信誉的 URL 过滤规则的例外，请创建新规则。

步骤 3 选择您创建的列表或源作为目标 URL 条件。

步骤 4 保存规则。

配置 HTTP 响应页面

作为访问控制的一部分，您可以使用访问控制规则或访问控制策略默认操作配置在系统阻止 Web 请求时要显示的 *HTTP* 响应页面。

所显示的响应页面取决于阻止会话的方式：

- **阻止响应页面**：覆盖用于说明拒绝已被连接的默认浏览器或服务器页面。
- **交互式阻止响应页面**：警告用户，并且还允许其点击按钮（或刷新页面）以加载最初请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

如果未选择响应页面，则系统将在没有交互或说明的情况下阻止会话。

对 HTTP 响应页面的限制

- 系统仅为被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的未加密连接或解密 HTTP/HTTPS 连接显示响应页面。对于被任何其他策略或机制阻止的连接，系统不会显示响应页面。
- 如果重置连接（发送 RST 数据包），系统将无法显示响应页面。如果启用响应页面，系统将优先处理此配置。即使选择**阻止并重置**或**交互式阻止并重置**作为规则操作，系统也会显示响应页面，但不会重置匹配的 Web 连接。要确保重置已阻止的 Web 连接，必须禁用响应页面。

  请注意，所有与此规则匹配的非 Web 流量都会被阻止并重置。
- 对于被访问控制规则（或其他任何配置）阻止的加密连接，系统不会显示响应页面。如果未配置 SSL 策略，或者 SSL 策略允许已加密流量通过，则访问控制规则会评估已加密连接。

  例如，系统无法解密 HTTP/2 或 SPDY 会话。如果使用以上协议之一加密的网络流量通过访问控制规则评估，则会话被阻止时系统不会显示响应页面。

  However, the system does display a response page for connections that are decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. 在这些情况下，系统会加密响应页面并在重新加密的 SSL 数据流最后发送该页面。
- 如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。
- 如果在未指定 “http” 或 “https” 的情况下输入 URL，并且浏览器在端口 80 上发起连接，并且用户点击响应页面，并且该连接随后重定向到端口 443，则用户不会看到第二个交互式响应页面，因为对此 URL 的响应已被缓存。
- 如果网络流量在系统识别请求的 URL 之前被阻止，则系统不会显示响应页面；请参阅URL 过滤的最佳实践，第 3 页。
- 如果在允许应用规则之后配置了阻止 URL 访问控制规则，则系统不会显示响应页面。

HTTP 响应页面的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

选择 HTTP 响应页面

HTTP 响应页面能否稳定显示取决于页面的网络配置、流量负载和大小。较小的页面更有可能成功显示。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **HTTP 响应**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 选择**阻止响应页面 (Block Response Page)** 和**交互式阻止响应页面 (Interactive Block Response Page)**：

- “系统提供”(System-provided) - 显示常规响应。点击 **视图**（  ） 可查看此页面的代码。
- “自定义”(Custom) - 创建自定义响应页面。屏幕上将显示一个弹出窗口，其中预先填充有系统提供的代码，您可以通过点击 **编辑**（  ）来替换或修改此代码。计数器显示已使用的字符数量。
- “无”(None) - 在没有交互或说明的情况下禁用响应页面并阻止会话。要对整个访问控制策略快速禁用交互式阻止，请选择此选项。

步骤 3 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

配置对 HTTP 响应页面的交互式阻止

配置交互式阻止时，用户可在看到警告后加载原先请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

提示 要对整个访问控制策略快速禁用交互式阻止，既不要显示系统提供的页面，也不要显示自定义页面。然后，系统会阻止所有连接而不交互。

如果用户不绕过交互式阻止，则会拒绝匹配流量而不进行进一步检查。如果用户绕过交互式阻止，则访问控制规则会允许流量，不过，流量仍然可能受到深度检查和阻止。

默认情况下，用户绕行的有效时间为 10 分钟（600 秒），而在在后续访问时不显示警告页面。可以将持续时间设置为长达一年，也可以强制用户每次都绕过阻止。此设置适用于策略中的每条“交互式阻止”规则。不能对每条规则都设置限制。

以交互方式阻止的流量的日志记录选项与允许的流量中的日志记录选项相同，但如果用户不绕过交互式阻止，则系统只能记录连接开始事件。在系统最初警告用户时，它会使用 `Interactive Block`

或 Interactive Block with reset 操作标记任何已记录的连接开始事件。如果用户绕过阻止，则为会话记录的其他连接事件具有操作 Allow。

配置交互式阻止

以下程序介绍了如何允许用户绕过 URL 过滤规则。

过程

步骤 1 作为访问控制的一部分，请配置与网络流量匹配的访问控制规则；请参阅创建和编辑访问控制规则：

- 操作 - 将规则操作设置为**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**；请参阅访问控制规则交互式阻止操作。
- 条件 - 使用 URL 条件指定要进行交互式阻止的网络流量；请参阅URL 条件（URL 过滤）。
- 日志记录 - 假设用户将绕过阻止并相应地选择日志记录选项；请参阅《Cisco Secure Firewall Management Center 管理指南》中的允许连接的日志记录 。
- 检测 - 假设用户将绕过阻止并相应地选择深度检查选项；请参阅访问控制概述。

步骤 2 （可选）在访问控制策略 **HTTP 响应 (HTTP Responses)** 上，选择自定义交互式阻止 HTTP 响应页面；请参阅选择 HTTP 响应页面 ，第 18 页。

步骤 3 （可选）在访问控制策略**高级 (Advanced)** 设置中，更改用户绕行超时；请参阅为受阻网站设置用户绕过超时 ，第 19 页。

在用户绕过阻止后，系统允许用户浏览到该页面而不发出警告，直至经过超时期为止。

步骤 4 保存访问控制策略。

步骤 5 部署配置更改；请参阅 部署配置更改。

为受阻网站设置用户绕过超时

以下程序介绍如何设置用户绕过URL过滤阻止后允许浏览的时间。超时到期后，用户必须再次绕过阻止。

过程

步骤 1 点击 **策略** > **访问控制** 并编辑策略。

步骤 2 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 3 点击常规设置旁边的 **编辑**（ ） 。

如果显示**视图**（ ），则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 在 **Allow an Interactive Block to bypass blocking for (seconds)** 字段中，键入用户绕过到期之前必须经过的秒数。

将此值设置为 0 表示交互式阻止响应显示一次，并且用户绕行永远不会过期。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

配置 URL 过滤运行状况监控器

如果系统在获取或更新 URL 类别和信誉数据时出现问题，以下运行状况策略会发出警报。

- URL 过滤监视器
- 设备中威胁数据更新

要确保按照您希望的方式进行配置，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 运行状况模块 和 配置运行状况监控 。

争议 URL 类别和信誉

如果您不同意 Talos 指定的类别或信誉，可以提交重新评估请求。

开始之前

您将需要思科账户凭证。

过程

步骤 1 在 管理中心 Web 界面中，执行以下操作之一：

争议选项的位置	争议选项的路径
云服务配置页面	a. 导航至**集成** > **其他集成** > **云服务**页面。 b. 选择**争议 URL 类别和信誉**。
手动 URL 查找页面	a. 导航至手动 URL 查找页面：**分析** > **高级** > **URL**。 b. 查找所有争议的 URL。 c. 要查看表格行末尾的 **争议** ，请将鼠标悬停在结果列表中的相关条目上，然后点击争议。

争议选项的位置	争议选项的路径
URL 连接事件	a. 导航至**分析 > 连接**菜单下的任何页面，此页面包括一个包含 URL 的表。 b. 右键点击**URL 类别**或**URL 信誉**列（如有需要，请显示隐藏列）中的项目，然后选择一个选项。

Talos 网站将在单独的浏览器窗口中打开。

步骤 2 使用思科凭证登录 Talos 网站。

步骤 3 查看信息并遵循 Talos 页面上的说明。

步骤 4 在 Talos 网站上查找有关如何处理所提交的争议以及期望的响应（如有）的信息。

争议流程与 Firepower 产品无关。

如果 URL 类别集发生更改，请执行操作

URL 类别集可能会偶尔发生更改，以适应新的 Web 趋势和不断发展的使用模式。

这些更改会影响策略和事件。

在计划进行 URL 类别更改之前和之后不久，您将在受更改影响的任何访问控制，SSL 和 QoS 策略的规则列表中以及在您编辑。

在看到这些警报时，您应采取措施。

注释 本主题中描述的对 URL 类别集的更新与简单地在现有类别中添加新的 URL 或对错误分类的 URL 进行重新分类的变化不同。此主题不适用于单个 URL 的类别更改。

过程

步骤 1 如果您在访问控制策略中的规则旁边看到警报，请将鼠标悬停在警报上以查看详细信息。

步骤 2 如果警报提到 URL 类别更改，请编辑规则以查看更多详细信息。

步骤 3 将鼠标悬停在规则对话框中的 URL 或类别上，可查看有关更改类型的一般信息。

步骤 4 如果您在类别旁边看到警报，请点击警报以查看详细信息。

步骤 5 如果您在更改说明中看到“更多信息”链接，请点击该链接以在 Talos 网站上查看有关类别的信息。

或者，查看 URL 类别和信誉说明，第 2 页 链接中的所有类别的列表和说明。

步骤 6 根据更改类型，采取适当的操作：

类别更改的类型	系统将执行的操作	您应该采取的措施
现有类别即将被弃用	还没有。您有几周的时间来更改受影响的规则。 如果您在此期间不执行操作，系统最终将无法重新部署策略。	从包含此类别的所有规则中删除此类别。如果有类似的新类别，请考虑改为使用该类别。
已添加新类别	默认情况下，系统不使用新添加的类别。	考虑为新类别创建新规则。
删除现有类别	类别将以加删除线文本的形式（即，在类别名称上划一条横线）显示在规则中。	您必须先从规则中删除过时类别，然后才能进行部署。

步骤 7 检查您的 SSL 规则（类别）是否存在这些更改，并根据需要执行操作。

步骤 8 检查您的 QoS 规则（URL）是否存在这些更改，并根据需要执行操作。

下一步做什么

部署配置更改；请参阅 部署配置更改。

URL 类别和信誉变更：对事件的影响

- 当URL类别发生更改时，系统在类别更改之前处理的事件将与其原始类别名称相关联，并标记为**传统**。系统在类别更改之后处理的事件将与新类别相关联。

  随着时间的推移，较旧的传统事件将逐渐退出系统。

- 如果在处理 URL 时其没有信誉，则事件查看器中的 URL 信誉列将为空。

URL 过滤故障排除

类别列表中缺少预期的 URL 类别

URL 过滤功能使用的类别集与安全情报功能不同；您期望看到的类别可能是安全情报类别。要查看这些类别，请查看访问控制策略中 **安全情报** 选项卡上的 **URL** 选项卡。

初始数据包不经检查通过

请参阅在识别流量之前检查通过的数据包以及子主题。

另请参阅DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别 ，第 13 页。

运行状况警报：“URL 过滤注册失败”

验证您的 管理中心 和任何代理是否可以连接到思科云。您可能需要以下主题中有关 URL 过滤和 URL 类别的信息： 《Cisco Secure Firewall Management Center 管理指南》中的 互联网访问要求 和 通信端口要求 。

如何查找特定 URL 的类别和信誉？

进行手动查找。请参阅《Cisco Secure Firewall Management Center 管理指南》中的查找 *URL* 类别和信誉。

尝试手动查找时出错：“<URL> 云查找失败”

请确保已正确启用此功能。请参阅在 《Cisco Secure Firewall Management Center 管理指南》中 查找 *URL* 类别和信誉 中的前提条件。

似乎根据 URL 类别和信誉对 URL 进行了错误处理

问题：系统无法根据 URL 类别和信誉正确处理 URL。

解决方案：

- 验证与 URL 关联的 URL 类别和信誉是否如您所料。请参阅《Cisco Secure Firewall Management Center 管理指南》中的查找 *URL* 类别和信誉。
- 可以通过URL 过滤选项，第 10 页（可以使用使用类别和信誉启用 URL 过滤，第 10 页进行访问）中所述的设置来解决以下问题。
  - URL 缓存可以保存过时信息。请参阅URL 过滤选项，第 10 页中有关**已缓存的 URL 到期**的信息。
  - 可能无法使用来自云的当前信息更新本地数据集。有关**启用自动更新**设置的信息，请参阅URL 过滤选项，第 10 页。
  - 系统可以配置为不检查云以获取当前数据。请参阅URL 过滤选项，第 10 页中有关 **向思科云查询未知 URL** 设置的信息。
- 访问控制策略可以配置为将流量传递到 URL，而无需检查云。有关**重试 URL 缓存缺失查找**设置的信息，请参阅访问控制策略高级设置。
- 另请参阅URL 过滤的最佳实践，第 3 页。
- 如果使用 SSL 规则处理 URL，请参阅解密规则 准则和限制和SSL 规则顺序
- 验证是否正在使用您希望处理的访问控制规则处理 URL，并且此规则将执行您希望执行的操作。考虑规则顺序。
- 验证 管理中心上的本地 URL 类别和信誉数据库是否已从云中成功更新，且托管设备是否已从管理中心成功更新。

这些进程的状态将在运行状况监视器、**URL 过滤监视器**模块和**设备中威胁数据更新**模块中报告。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的 运行状况 /

如果要立即更新本地URL类别和信誉数据库，请转至**集成** > **其他集成**，点击**云服务**，然后点击**立即更新 (Update Now)**。有关详细信息，请参阅URL 过滤选项 ， 第 10 页。

URL 类别或信誉不正确

对于访问控制或 QoS 规则：使用手动过滤，注意规则顺序。请参阅手动 URL 过滤 ， 第 15 页和配置 URL 条件 ， 第 11 页。

对于 SSL 规则：不支持手动过滤。改为使用可分辨名称条件。

也请按月 争议 URL 类别和信誉 ， 第 20 页。

网页加载速度缓慢

可以在安全与性能之间权衡取舍。某些选项：

- 考虑修改**缓存 URL 到期**设置。点击 **集成** > **其他集成**，然后选择 **云服务**。有关信息，请参阅URL 过滤选项 ， 第 10 页。
- 考虑在访问控制策略高级设置中取消选择**重试 URL 缓存缺失查找**设置。

事件不包括 URL 类别和信誉

- 确保已在访问控制策略中包含适用的URL规则，规则处于活动状态，并且策略已部署到相关设备。
- 如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。
- 必须为 URL 类别和信誉配置处理连接的规则。
- 即使已在 SSL 规则的类别选项卡中配置 URL 类别，也必须在访问控制策略的规则中配置 URL 选项卡。

DNS 过滤不起作用

确保您已完成 启用 DNS 过滤以在域查找期间识别 URL ， 第 13 页中的所有前提条件和步骤。

最终用户尝试访问被阻止的 URL，而页面只是旋转和超时

当启用 DNS 过滤且最终用户访问被阻止的 URL 时，页面将旋转但不会加载。最终用户不会收到该页面被阻止的通知。这是当前启用 DNS 过滤时的限制。

请参阅DNS 过滤限制 ， 第 14 页。

事件包括 URL 类别和信誉，但 URL 字段为空

如果 DNS 查询字段已填充且 URL 字段为空，则在启用 DNS 过滤功能时会出现这种情况。

请参阅DNS 过滤和事件，第 14 页。

为单个事务生成多个事件

单个 Web 事务有时会生成两个连接事件，一个用于 DNS 过滤，另一个用于 URL 过滤。当启用 DNS 过滤并且符合以下条件时，会出现这种情况：

- 流量的访问控制规则操作为“允许”或“信任”。
- 系统首次遇到 URL。

请参阅DNS 过滤和事件，第 14 页。

URL 过滤历史记录

功能	最低 管理中心	最低 威胁防御	详情
新的 URL 类别	版本 7.0 的新增内容，适用于所有版本	任意	新 URL 类别：专用 IP 地址 有关详细信息，请参阅 Talosintelligence.com
DNS 过滤	7.0 6.7（测试版）	任意	每个访问控制策略的高级设置中的新选项都允许按类别和信誉提前过滤网络流量。 该功能会在新安装中默认启用。 支持的平台：任何支持版本的 管理中心 和托管设备。
能够为未知信誉的站点指定处理方式	6.7	任意	您现在可以指定对未知信誉的 URL 的处理方式。 修改后的屏幕：访问控制策略和 QoS 策略中的 URL 规则以及 SSL 策略中的类别规则在信誉选择区域下方包括一个新复选框。 支持的平台：全部

功能	最低 管理中心	最低 威胁防御	详情
新增和更改的 URL 类别 信誉级别的新名称	6.5	任意	以下更改适用于访问控制和 QoS 策略中的 URL 规则以及 SSL 策略中的类别规则： URL 类别集已更改。在您创建 URL 规则时，现在有两个类别“页面”可供选择。 与每个信誉级别关联的名称已更改。 有关新类别和信誉名称的说明，请参阅URL 类别和信誉说明，第 2 页。 有关特定于升级的完整详细信息，另请参阅版本说明和版本 6.5 的升级说明。 如果将来类别集发生更改，您的规则将显示图标以提醒您。 修改的屏幕：访问控制策略、SSL 策略和 QoS 策略中的 URL 规则；与 URL 类别相关的事件数据。 支持的平台： 管理中心 和运行版本 6.5 的设备。
对传统设备许可的细微更改	6.5	任意	对于使用经典许可证的设备，在设备注册到 管理中心 并将 URL 过滤许可证分配给设备之前不会启用 URL 过滤。 支持的平台：NGIPSv 和 ASA 与 FirePOWER 服务设备。
用于从思科云检索URL数据的地址已更改	6.5	任意	请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的互联网访问要求中的“URL 过滤”行。
有机会对指定的 URL 类别提出异议	6.5	任意	如果您不同意系统分配给 URL 的类别，您可以提交更改类别的请求。 新增/修改的屏幕： • 右键点击**分析**菜单下的连接事件表中的 URL 类别或信誉时的新菜单选项。 • “URL 查找”页面（**分析 > 高级 > URL**）上的“新建”按钮。（将鼠标指针悬停在 URL 上以显示此按钮。） • **系统 > 集成 > 云服务**页面上的新选项 支持的平台：所有
思科 CSI 选项卡已重命名为**云服务**	6.4	任意	修改的屏幕和导航：**系统 > 集成 > 思科 CSI** 现在已更改为**系统 > 集成 > 云服务** 支持的平台： 管理中心
将 URL 过滤信息从各个位置移动到新的“URL 过滤”章节	6.3	任意	将有关为 URL 过滤配置云通信的信息移动至新的“URL 过滤”章节。将某些其他 URL 过滤信息从其他位置移动至本章。在本章节中对思科 CSI 主题的结构进行了相关更改。

功能	最低 管理中心	最低 威胁防御	详情
新选项：已缓存的URL到期	6.3	任意	使用此新控件来平衡 URL 类别和信誉数据的性能与新鲜度，以便尽量减少与过时数据匹配的 URL 实例。 修改的屏幕：**系统 > 集成 > 思科 CSI**。 支持的平台：所有。
已更改菜单路径	6.3	任意	手动 URL 查找页面的路径已从**分析 > 查找 > URL** 更改为**分析 > 高级 > URL**。

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。