内容限制

以下主题介绍如何将访问控制策略配置为使用内容限制功能：

关于内容限制

主要搜索引擎和内容传递服务提供允许您限制搜索结果和网站内容的功能。例如，学校使用内容限制功能来遵守儿童互联网保护法案 (CIPA)。

当由搜索引擎和内容传递服务实施时，您可以仅针对个别浏览器或用户执行内容限制功能。系统允许您将这些功能扩展到您的整个网络。

该系统允许您执行以下服务：

- 安全搜索 - 许多主要搜索引擎支持此服务，此服务过滤掉被企业、政府和教育环境分类为不允许的限制级成人内容。系统不限制用户访问所支持搜索引擎主页的能力。

您可以使用两种方法配置系统执行这些功能：

方法：访问控制规则
内容限制功能通过请求 URI 中的元素、相关 Cookie 或自定义 HTTP 标头报头元素传达搜索或内容查询的限制状态。您可以将访问控制规则配置为在系统处理流量时修改这些元素。

方法：DNS Sinkhole
对于 Google 搜索，您可以将系统配置为将流量重定向到 Google SafeSearch 虚拟 IP 地址 (VIP)，对安全搜索实施过滤。

下表描述这些执行方法之间的差异。

表 *1:* 内容限制方法的比较

属性	方法：访问控制规则	方法：**DNS Sinkhole**
支持的设备	任意	Cisco Secure Firewall Threat Defense 仅
支持的搜索引擎	规则编辑器的**应用 (Applications)** 选项卡中任何标记 `safesearch supported` 的项目	仅限 Google
支持 YouTube 受限模式	是	是
需要 SSL 策略	是	否
主机必须使用 IPv4	否	是
连接事件日志记录	是	是

在确定要使用哪种方法时，请考虑以下限制：

- 访问控制规则方法需要一种 SSL 策略，该策略会影响性能。
- Google SafeSearch VIP 仅支持 IPv4 流量。如果您配置 DNS Sinkhole 来管理 Google 搜索，则受影响的网络上的所有主机必须使用 IPv4。

根据使用的方法，系统会记录连接事件中**原因 (Reason)** 字段的不同值：

- 访问控制规则 - 内容限制 `(Content Restriction)`
- DNS Sinkhole - `DNS 阻止 (DNS Block)`

内容限制的要求和前提条件

型号支持

任意，或如程序中所示。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

内容限制的准则和限制

- 仅 Snort 2 支持安全搜索。
- YouTube 和 Google 不支持在访问控制规则中实施的 YouTubeEDU 功能。请删除所有配置 YouTubeEDU 的访问控制规则，因为它们实际上不起作用。您还可以删除关联的解密规则。

使用访问控制规则执行内容限制

以下步骤程序介绍了如何配置限制内容的访问控制规则。

注释 在访问控制规则中启用安全搜索或 时，内联规范化会被自动启用。

过程

步骤 1 创建 解密策略。

步骤 2 添加用于处理安全搜索 流量的规则：

- 选择**解密 - 重新签名 (Decrypt - Resign)** 作为规则的**操作 (Action)**。
- 在**应用 (Applications)** 中，将所选操作添加到**所选应用和过滤器 (Selected Applications and Filters)** 列表中：
  - 安全搜索 - 添加类别：搜索引擎 (Category: search engine) 过滤器。

步骤 3 为您添加的规则设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

步骤 4 创建或编辑访问控制策略，并将解密策略与访问控制策略相关联。

有关详细信息，请参阅将其他策略与访问控制相关联。

步骤 5 在访问控制策略中，添加用于处理安全搜索和 流量的规则：

- 选择**允许 (Allow)** 作为规则的**操作 (Action)**。
- 在 **应用** 中，点击 **安全搜索**（） 的图标，然后设置相关选项。
  - 访问控制规则的安全搜索选项 ， 第 4 页
- 在**应用 (Applications)** 中，优化**所选应用和过滤器 (Selected Applications and Filters)** 列表中的所选应用。

在大多数情况下，启用安全搜索 会在 **所选应用和过滤器** 列表中填入适当的值。如果在您启用此功能时，安全搜索 应用已经存在于列表中，则系统不会自动填充列表。如果应用没有按预期填充，请按照以下方式手动添加：

- 安全搜索 - 添加类别：搜索引擎 (`Category: search engine`) 过滤器。

有关详细信息，请参阅配置应用条件和过滤器。

步骤 6 为您添加的访问控制规则设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

步骤 7 配置系统在阻止受限内容时显示的 HTTP 响应页面；请参阅选择 HTTP 响应页面。

步骤 8 部署配置更改；请参阅 部署配置更改。

访问控制规则的安全搜索选项

Firepower 系统仅支持特定搜索引擎的安全搜索过滤。有关受支持的搜索引擎的列表，请参阅访问控制规则编辑器的**应用 (Applications)** 选项卡中标记支持安全搜索 (`safesearch supported`) 的应用。有关不受支持的搜索引擎的列表，请参阅标记不支持安全搜索 (`safesearch unsupported`) 的应用。

为访问控制规则启用安全搜索时，请设置以下参数：

启用安全搜索
为匹配此规则的流量启用安全搜索过滤。

不受支持的搜索流量
指定在处理来自不受支持的搜索引擎的流量时您希望系统执行的操作。如果您选择**阻止 (Block)** 或**阻止并重置 (Block with Reset)**，还必须配置在系统阻止受限内容时所显示的 HTTP 响应页面；请参阅选择 HTTP 响应页面。

使用 DNS Sinkhole 执行内容限制

通常，DNS Sinkhole 会将流量定向到特定的目标。此过程描述如何将 DNS Sinkhole 配置为将流量重定向到 Google 安全搜索虚拟 IP 地址 (VIP)，这会强制对 Google 和 YouTube 搜索结果应用内容过滤器。

由于 Google 安全搜索为 VIP 使用单个 IPv4 地址，因此主机必须使用 IPv4 寻址。

注意 如果您的网络包括代理服务器，则除非您在代理服务器和互联网之间放置 威胁防御设备，否则此内容限制方法无效。

此过程描述了仅对 Google 搜索实施内容限制。要对其他搜索引擎实施内容限制，请参阅使用访问控制规则执行内容限制，第 3 页。

开始之前

此程序仅适用于 威胁防御 并需要 IPS 许可证。

过程

步骤 1 通过以下 URL 获得支持的 Google 域列表：https://www.google.com/supported_domains。

步骤 2 在本地计算机上创建自定义 DNS 列表，并添加以下条目：

- 要执行 Google 安全搜索，为每个支持的 Google 域添加一个条目。
- 要实施 YouTube 限制模式，请添加一个“youtube.com”条目。

自定义 DNS 列表必须是文本文件 (.txt) 格式。文本文件的每一行都必须指定一个单独的域名，去掉任何前导句点。例如，支持的域“.google.com”必须显示为“google.com”。

步骤 3 将自定义 DNS 列表上传到 管理中心；请参阅将新的安全智能列表上传到 Cisco Secure Firewall Management Center。

步骤 4 确定 Google 安全搜索 VIP 的 IPv4 地址。例如，在 forcesafesearch.google.com 上运行 `nslookup`。

步骤 5 为安全搜索 VIP 创建一个 Sinkhole 对象；请参阅创建 Sinkhole 对象。

为此对象使用以下值：

- IPv4 地址 - 输入安全搜索 VIP 地址。
- IPv6 地址 - 输入 IPv6 环回地址 (`::1`)。
- 记录到 Sinkhole 的连接 - 点击“记录连接” (Log Connections)。
- 类型 - 选择**无**。

步骤 6 创建基本的 DNS 策略；请参见创建基本 DNS 策略。

步骤 7 为 Sinkhole 添加 DNS 规则；请参阅创建和编辑 DNS 规则。

对于此规则：

- 选中**已启用 (Enabled)** 复选框。
- 从操作下拉列表中选择 **Sinkhole**。
- 从 **Sinkhole** 下拉列表中选择您创建的 Sinkhole 对象。
- 将您创建的自定义 DNS 列表添加到 **DNS** 上的**所选项目 (Selected Items)** 列表中。
- （可选）在**网络 (Networks)** 中选择一个网络，以将内容约束限制为特定用户。例如，如果要将内容约束限制为学生用户，请将学生分配给不同于教员的子网，并在此规则中指定该子网。

步骤 8 将 DNS 策略与访问控制策略相关联；请参阅将其他策略与访问控制相关联。

步骤 9 部署配置更改；请参阅 部署配置更改。

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。