FQDN 和 URL 过滤类别

FQDN/URL 过滤类别

多云防御 使用来自 WebRootTM BrightCloud (www.brightcloud.com) 的威胁情报，根据网站的风险评分对网站进行分类。这包括完全限定域名 (FQDN)（有时称为域名）和 URL。当来自公共云环境的流量与这些站点建立出站连接（出口）时，这会提供 84 个类别的站点：

- FQDN（域）- 超过 10 亿个分类 FQDN（域）
- URL - 45+ 十亿个分类 URL

为了提高识别和处理流量的效率，网关将预加载前 100 万个 FQDN/URL 及其类别的缓存。网关还将利用 10000 个 FQDN/URL 及其类别（不属于前 100 万个）的运行时缓存。如果流量包含任何缓存的 FQDN/URL，则将立即知道类别。如果在缓存中找不到 FQDN/URL，网关将查询控制器以通过 BrightCloud 解析类别。此操作预计在 200 毫秒内完成。如果它在预期时间内完成，则将根据获知的类别处理流量，并且配置文件将根据为该类别定义的策略对流量进行操作。如果操作未在预期时间内完成，则流量将被处理为未分类，并且配置文件将根据为未分类定义的策略对流量进行操作。一旦解析返回，获知的类别将被添加到缓存中以供后续解析，即使解析发生在预期的时间内并且流量已被处理。如果运行时缓存已用尽，网关将清除最早访问的 FQDN/URL 及其类别（每 10 个条目），以确保有更多空间可用于最近访问的 FQDN/URL 及其类别。

Note 使用类别进行 FQDN 过滤的对象包括：

1. TLS 客户端 Hello 中的 SNI
2. 用于 FQDN 查找的 DNS 查询
3. HTTP 主机名报头（用于明文 HTTP 流量）

恶意类别

多云防御 认为以下类别特别恶意：

Table 1: 恶意类别 多云防御 将以下类别视为特别恶意

类别名称 (Category Name)	类别说明
恶意软件网站	托管恶意内容的站点，包括可执行文件、偷渡式感染站点、恶意脚本、病毒、木马和代码。
网络钓鱼和其他欺诈	网络钓鱼、域名欺诈和其他伪装成信誉良好的站点，通常是为了收集用户的个人信息。这些站点通常是短暂的，因此它们在正常运行时间方面不会持续很长时间。
代理规避和匿名程序	以绕过 URL 过滤或监控的任何方式获取 URL 访问权限的代理服务器和其他方法。绕过过滤的基于 Web 的翻译网站。
按键记录器和监控	跟踪用户击键或监控其网上冲浪习惯的软件代理。通常用于收集敏感数据，例如用户名和密码。
垃圾邮件 URL	已知分发未经请求的邮件（垃圾邮件）的站点。
间谍软件和广告软件	提供或促进最终用户或组织未知或未经其明确同意的信息收集或跟踪的间谍软件或广告软件网站，以及可能安装在用户计算机上的未经请求的广告弹出窗口和程序。
僵尸网络	这些 URL（通常是 IP 地址）被确定为僵尸网络的一部分，从中发起网络攻击。攻击可能包括垃圾邮件、DOS、SQL 注入、代理劫持和其他未经请求的联系。

多云防御 在通过 **发现** > **流量** > **DNS** 和 **调查** > **流分析** > **流量摘要**查看流量时提供流量分析，其中可以选择预定义的 恶意类别 过滤器来显示与这些恶意类别 FQDN 和 URL 通信的实例和 VPC。

完整的类别列表如下所示。

类别的完整列表

类别名称 (Category Name)	类别名称 (Category Name)	类别名称 (Category Name)	类别名称 (Category Name)
堕胎	游戏	机动车	性教育
滥用药物	政府	音乐	共享软件和免费软件
成人和色情	毛额	新闻与媒体	购物
酒精和烟草	黑客攻击	裸体	社交网络
拍卖	仇恨和种族主义	在线贺卡	社会
僵尸网络	健康和医疗	打开 HTTP 代理	垃圾邮件 URL
商业与经济	家居和园艺	寄放域	体育
作弊程序	狩猎和钓鱼	付费冲浪	间谍软件和广告软件
计算机和互联网信息	违法	点对点	流媒体
计算机和互联网安全	图片和视频搜索	个人网站和博客	泳衣和内衣
已确认的垃圾邮件源	个人炒股建议和工具	个人存储	培训和工具
内容交付网络	互联网通信	哲学和政治宣传	转换
小众和神秘	互联网门户	网络钓鱼和其他欺诈	差旅费
约会	求职	私有 IP 地址	未分类
死网站	按键记录器和监控	代理规避和匿名程序	未确认的垃圾邮件源
动态生成的内容	童鞋	可疑	暴力类
教育机构	法务	房地产	武器
娱乐和艺术	本地信息	娱乐和爱好	网络广告
时尚和美容	恶意软件网站	参考和研究	Web 托管
金融服务业	大麻	宗教	基于 Web 的电子邮件
赌博	军事搜索引擎	服务	

将过滤配置文件与策略规则集规则关联

- 请参阅 FQDN 过滤 以创建/编辑 FQDN 过滤配置文件
- 请参阅 URL 过滤 以创建/编辑 URL 过滤配置文件

BrightCloud URL/IP 查找工具

BrightCloud 提供在线 URL/IP 查找工具 (https://www.brightcloud.com/tools/url-ip-lookup.php)，可用于了解特定 FQDN/URL 的类别及其 Web 信誉。

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。