

排除DNS活动日志条目中的决策受阻故障

目录

问题

报告以下一个或多个症状：

- Activity Search (Monitor > Activity Search , 已过滤为DNS事件) 显示域的Decision/Action = Blocked , 但是查看Internet Access规则不会显示明显阻止该域的规则。
- 该域不存在于管理员维护的任何Block目标列表中。

环境

- 本文档中的信息基于：
 - 思科安全接入(SSE)云平台
 - 具有漫游安全模块的思科安全客户端5.x已部署并注册到安全访问组织

分辨率

步骤1.检验已评估的身份

- 确认决策针对的是哪个身份。如果事件显示网络、站点或隧道身份而不是预期的漫游计算机或用户，则查询匹配与所检查的规则集不同的规则集。
- 对于漫游用户，验证设备已注册且报告为受保护

身份不匹配：更正部署，以便应用预期身份（注册漫游设备、修复AD/用户组映射或调整网络身份规则集），而不是松开错误匹配的规则。

第2步：检查安全类别是否匹配

- 如果事件包含安全类别（Malware、C2、Phishing、Newseen Domains、DNS Tunneling等），则阻止来自匹配规则集的安全设置 — 不需要目标列表或内容规则引用该域。
- 在思科Talos情报门户上查找域的当前信誉和分类，网址为<https://talosintelligence.com/>（信誉中心查找）。
- 如果Talos中显示的分类或信誉不正确，请直接通过<https://talosintelligence.com/>向Talos提交争议/重新分类请求（提交案例），以便重新评估域。Talos更新分类后，更改会传播到安全访问实施。

第3步：检查CNAME链

- 从未过滤的有利点解析域并检查完整的应答链（例如，`dig +noall +answer <domain>`或`nslookup -debug <domain>`）。
- 根据目标列表和Talos分类检查链中的每个CNAME目标；受阻的CNAME目标解释对明显干净的查询域所做的受阻决策

第4步：从上到下重新评估策略的实际身份

- 从第1步按照身份顺序浏览Internet访问规则，检查每个规则的身份范围、计划、启用状态以及安全/内容/应用设置，向下检查并包括默认规则。
- 使用具有确切标识和目标的策略测试程序（例如 — policy.test.sse.cisco.com/?=cisco.com）查看安全访问报告为匹配的规则，并将其与事件上命名的规则进行比较。

特殊情况：新发现的域

如果事件的安全类别是Newly Seen Domains(NSD)

补救选项，按优先顺序：

如果域是业务关键型域，请将其添加到适用规则引用的允许目标列表；对于该目标，allow条目优先于NSD安全块。

禁用加密DNS(DoH)和QUIC

加密DNS和QUIC会导致DNS层可视性差距，从而导致活动搜索结果混乱：通过浏览器DoH解析的查询不会到达安全访问解析器（因此它们完全不在日志中），而DoH提供程序域本身可能显示为Blocked事件。

在受管终端上禁用这些传输可确保所有DNS保持可检查状态，活动日志反映实际终端行为。

每个浏览器的HTTPS上的DNS(DoH)

Google Chrome

- 手动：导航至chrome://settings/security，然后关闭使用安全DNS。

Microsoft Edge

- 手动：导航至edge://settings/privacy，然后关闭使用安全DNS。

Mozilla Firefox

- 手动：Menu > Settings > Privacy & Security > DNS over HTTPS（或较旧版本中的网络设置），然后选择Off/取消选择Enable DNS over HTTPS。
- 注意：Umbrella/Secure Access解析器对Mozilla canary域(use-application-dns.net)的应答方式是，以指示Firefox在默认情况下保持DoH关闭；仍建议使用显式GPO设置，因为用户设置DoH配置会覆盖金丝雀检查。警告：请勿将Mozilla kill-switch/canary域添加到阻止目标列表——阻止页面A记录响应被视为有效，并且可能导致Firefox保留或升级其DoH使用情况。

QUIC(HTTP/3)

QUIC在UDP/443上运行，可以传输常规网络流量和DoH3(DNS over HTTP/3)，从而绕过预期TCP的检查路径。

禁用QUIC会强制浏览器回退到基于TCP的HTTP/2或HTTP/1.1，从而恢复完全可视性：

- Chrome/Edge:手动（非持久性，用户可更改）：将chrome://flags/#enable-quic / edge://flags/#enable-quic设置为Disabled。
- Firefox:设置首选项network.http.http3.enable = false(about:config or policy/AutoConfig)。

如果在这些步骤后，事件上报告的匹配规则仍然无法与配置协调，请向思科TAC提交案例并提供活动搜索事件导出（时区、身份、匹配规则、类别、记录类型和域的时间戳）以及相关规则和目标列表的屏幕截图。

原因

安全类别匹配（Talos情报）— 域被安全设置（例如，恶意软件、命令和控制、网络钓鱼、加密挖掘、DNS隧道或新发现的域）阻止，这些安全设置基于Cisco Talos信誉和分类，而不是管理员明确配置的任何目标列表或内容规则。这是“无明显匹配”块的最常见原因。

身份属性不匹配 — 查询归因于与预期不同的身份（网络/站点身份而不是漫游计算机、不同的AD用户/组，或者未注册设备回退到网络级策略），因此匹配了不同的规则（通常更严格或默认）。

规则顺序和默认规则 — 策略中更高级的规则（或底部的默认/全部捕获规则）在预期的Allow规则之前匹配；还可以禁用、计划目标规则，或者将目标规则限定于不包括受影响源的身份。

目标列表继承 — 阻止目标列表包含父域(example.com)，该父域隐式覆盖所有子域(app.example.com)，或包含域解析到的IP/CIDR。仅搜索列表以查找精确的FQDN不会显示这一点。

CNAME链阻塞 — 允许查询的域，但其解析链包含阻止的域（通常是CDN、跟踪器或停留/阻止的主机）的CNAME;该决策将应用于链，并且日志将原始查询的域显示为Blocked。

应用程序或内容类别匹配 — 域属于被阻止的应用程序（应用程序控制）或内容类别，管理员未将其关联；分类可能与直觉不同（例如，分类为文件共享或代理/匿名器的业务工具）。

最近的策略或分类更改 — 策略或Talos分类最近更改；查看中的事件早于（或迟于）更改，或者策略传播/客户端同步在查询时尚未完成。

相关内容

- [为Umbrella配置内部DNS服务器](#)
- [使用Umbrella配置HTTPS上的DNS\(DoH\)](#)
- [在安全访问中添加域控制器](#)
- [思科安全访问阻止页面信息](#)
- [思科技术支持和下载](#)

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）。