解决思科安全访问的实时DLP问题

目录

介绍

- 必备条件和警告

概述

一般故障排除核对表

排除漏报故障

- 分类器、文件和字符串
- 文件标签
- 网站和目标

排除误报故障

- 桌面应用支持
- DLP分类器陷阱
- 精确数据匹配(EDM)

介绍

本文档介绍在安全Web网关(SWG)环境中内联或实时数据丢失防护(DLP)问题的故障排除步骤。

必备条件和警告

- HTTPS检测：确保已启用HTTPS检查。DLP无法扫描加密流量。确保使用思科安全访问根CA或自定义CA解密网站。
- QUIC协议：在所有浏览器中禁用QUIC协议。QUIC使用UDP，它绕过SWG并防止DLP扫描。
- IPv6:如果流量未达到SWG，则禁用IPv6，因为双堆栈功能必须导致绕过。
- 安全策略:确保访问规则未启用“允许 — 覆盖安全”或“隔离”。

概述

内联DLP是SWG的扩展扫描功能。监控或阻止上传通过SWG代理上传的文件中的敏感、机密或个人可识别数据。客户使用思科定义的标识符（例如信用卡或社会保险号）或自定义关键字创建数据分类。这些分类适用于分配给特定身份和目标的DLP策略。DLP引擎仅扫描HTTP POST、PUT和PATCH方法。

一般故障排除核对表

如果未进行DLP检测，请验证所概述的步骤：

- 连接性:通过访问http://policy.test.sse.cisco.com确认客户端正在使用SWG。验证应用了正确的SWG数据中心，测试结果显示为“受安全访问保护”。
- 解密：确保已在安全配置文件中启用SSL解密。验证没有选择性解密或“不解密”列表排除。
- 流量控制：确保没有在“Internet设置”中配置外部域绕行。
- 身份：如果DLP策略依赖于Active Directory组，请确认用户是正确组的成员。
- Application Settings:如果将Microsoft域用于DLP，请确保禁用Office 365旁路或M365兼容性设置。
- 活动搜索：使用Reporting > Activity Search确保完整URL可见（已解密），并且预期身份与流量关联。选中Reporting > Data Loss Prevention以确认是否记录了监控或阻止活动。
- 策略配置：验证DLP策略是否针对正确的身份和目标应用进行了配置。
- 测试：使用确认完好的目的地(例如，pastebin.com或dlptest.com)和来自Cisco文档的确认完好的测试示例字符串。
- 支持数据：从用户处收集HAR文件，以验证通过SWG路由的流量并检查SWG报头。

排除漏报故障

如果DLP处于活动状态，但特定分类器无法触发，请调查以下区域：

分类器、文件和字符串

- 文件状态：确保文件未加密或不可扫描。使用简单文本文件测试。
- 阈值：检查Policy > Data Classification中的Threshold和Proximity设置。分类器可能需要较高的命中数或接近自定义字符串。
- 正则表达式模式：使用在线工具(例如regexr.com)可视化模式。简化模式，以捕获更小的字符串部分并逐渐扩展。

文件标签

- 兼容性：文件标签检测不适用于Confluence或JIRA。
- 元数据：在Microsoft应用程序中打开文档属性。该值必须与Umbrella File标签完全匹配；区分大小写。
- 加密 :标签检测不适用于受密码保护或加密的文件。

网站和目标

- 支持的应用：查看支持的应用程序列表。对于不受支持的应用或“所有目标”，仅扫描特定的mime类型。
- 经过审核的应用：对经过审核的应用程序(例如dlptest.com)进行更全面的扫描。只能扫描任意网站是否存在文件违规。
- 文件名：系统仅为某些经过审核的应用程序搜索文件名。

排除误报故障

如果DLP意外匹配内容，请在报告>防数据丢失中检查分类器名称和DLP规则。如果检测合法但不需要检测，请调整Thresholds或Proximity设置以优化策略。

桌面应用支持

对基于桌面的应用程序（例如Outlook、Teams或Google Workspace）的支持是以尽力而为的。效率取决于文件上传过程中使用的消息格式，基于Web的版本与桌面版本可能不同。对于未经审核的应用，不能保证支持文件上传。

DLP分类器陷阱

- 信用卡号：使用Luhn算法进行验证。仅使用有效的信用卡号进行测试。
- 人员姓名：需要2-3个单词，并且每个单词都必须大写。
- 名称组合：名称和其他数据之间需要分隔符字符串（例如，“Viagra - John Smith”匹配，但“Viagra John Smith”不匹配）。
- 出生日期：必须靠近关键字或标题，例如“dob”或“birth date”。
- 不良内容：如果文本类似于书籍或报告，则某些例外字符串会阻止此分类器触发。
- 邮政编码：必须接近特定位置相关的关键字。

精确数据匹配(EDM)

在研究EDM之前，请确认常规DLP扫描功能是否正常。对于EDM特定问题，请检查“上次编辑”(Last Edit)字段是否在控制面板中是当前字段，并验证索引工具输出。

命令用法：

使用-d选项运行索引工具以生成一个布鲁姆过滤器文件(.blm)。 此命令用于验证EDM索引和排除必须跳过记录的原因。-d标志指示工具输出诊断布卢姆过滤器文件，该文件应与支持人员共享，同时提供示例文件或HAR/Web开发人员工具数据。

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）。