使用服务日志来提高网络钓鱼检测效率

本章包含以下部分：

概述

服务日志用于根据思科邮件安全设备产品手册准则来收集个人数据。

服务日志会被发送到思科 Talos 云服务，以改进网络钓鱼检测。

注释 从 AsyncOS 13.5 开始，服务日志将 senderbase 替换为发送到思科 Talos 云服务的遥测数据。

邮件网关仅从客户邮件中收集有限的个人数据，并提供大量有用的威胁检测功能，这些功能可与专用分析系统结合使用，来收集观察到的威胁活动，然后分析其趋势并建立关联。思科会将这些个人数据用于改进思科安全邮件云网关的功能，以分析威胁形势、提供对恶意邮件的威胁分类解决方案，以及保护邮件网关免受新威胁（例如垃圾邮件、病毒和目录搜集攻击）的攻击。

在邮件网关上启用服务日志

过程

步骤 1 转到**安全服务 (Security Services) > 服务日志 (Service Logs)**。

步骤 2 单击**编辑全局设置 (Edit Global Settings)**。

步骤 3 选中**与服务日志信息服务共享受限制数据（推荐）**复选框。

选中此复选框，将以全局方式为邮件网关启用该功能。启用后，使用情景自适应扫描引擎 (CASE) 收集和报告数据（无论是否启用思科反垃圾邮件扫描）。在 CLI 中，使用 **servicelogsconfig** 命令可以配置相同的设置

步骤 4 单击**提交 (Submit)** 并确认更改。

在邮件网关上禁用服务日志

过程

步骤 1 转到**安全服务 (Security Services)** > **服务日志 (Service Logs)**。

步骤 2 单击**禁用 (Disable)** 并确认更改。

常见问题解答

思科了解您的隐私至关重要，因此我们在设计和运行服务时，时刻谨记要保护您的隐私。如果您注册思科 Talos 云服务，思科将收集有关您组织邮件流量的汇总统计数据，但不会收集或使用任何个人身份信息。思科收集的任何可识别您的用户或组织的信息，都将被视为机密信息。

我需要共享哪些数据？

数据是有关邮件属性及邮件网关处理不同类型邮件的方式的汇总信息。我们不收集邮件的完整正文。同样，提供给思科的可识别您的用户或组织的信息将被视为机密信息。（请参阅以下思科采取哪些措施来确保我共享的数据安全？ ，第 3 页）。

下表介绍了“人性化”格式的日志条目示例。

表 *1:* 按邮件信息共享的统计

项目	示例数据
入站 SMTP 连接的 GUID	0FyIkNX8ThST1 /IdfyNshg==
邮件的 GUID	1Hss77LIS6u7y5 GDn0QFEQ==
思科安全邮件网关邮件 ID	5191655
收件人数量及其有效性	1

项目	示例数据
来自非思科 Talos 引擎的扫描程序判定（例如，防病毒或高级恶意软件保护）	4
邮件布置	MSG_DISP_DROPPED
邮件布置原因	MSG_DISP_FILTER
邮件是否为出站传送？	true
消息大小	35100
传入邮件中继	true
邮件流方向	IP_DIR_OUT
AMP 判定信息	file_sha2_256： "\217\263\037\004\374`N \3264\265\016\314\227\005E\337\373q \177A\245 \017\004\204\340\231\260!^
丢弃邮件的采样	true

表 *2:* 按周期配置信息共享的统计

项目	示例数据
已启用病毒爆发过滤器功能	true
发件人域信誉 (SDR) 已禁用标记	true
情景自适应扫描引擎 (CASE) 版本	3.8.5-036
Talos 引擎	1.95.0.220
已启用功能的通用列表	Sophos_enabled

思科采取哪些措施来确保我共享的数据安全？

如果您同意注册思科 Talos 云服务：

- 从邮件网关发送的数据将使用安全 gRPC/HTTP2 协议发送到思科 Talos 云服务。
- 所有客户数据均在思科谨慎处理。这些数据存储在安全的位置，只有需要访问它们来改善公司邮件安全产品与服务或提供客户支持的思科员工和承包商才能访问这些数据。
- 在根据这些数据生成报告或统计数据时，不会在思科系统之外共享可识别邮件收件人或客户公司的任何信息。

共享数据是否会影响我的思科邮件网关的性能？

思科认为，这对大多数用户的性能影响非常之小。我们在邮件传送过程中记录已存在的数据。然后，客户数据会在邮件网关上汇聚并发送到思科 Talos 云服务。预计通过 HTTPS 传输的数据总大小不足典型公司邮件流量带宽的 1%。

启用后，使用情景自适应扫描引擎(CASE)收集和报告数据（无论是否启用思科反垃圾邮件扫描）。

如果您还有其他问题，请与思科客户支持部门联系。请参阅思科支持社区。

我是否可通过其他方式共享数据？

如果客户希望采取更多操作来帮助思科提供优质安全服务，可使用命令来共享其他数据。这种更高级别的数据共享还将在邮件中提供纯文本形式的附件文件名，以及URL的主机名。如果您有兴趣了解此功能，请告诉您的系统工程师或联系思科客户支持部门。