使用安全ICAP将安全访问与本地DLP集成

目录

简介

本文档介绍如何使用安全ICAP将安全访问与本地防数据丢失(DLP)服务器集成。

概述

您可以将Umbrella与本地DLP解决方案集成，实现集中式事件管理和补救工作流程。此集成使用安全ICAP（Internet内容自适应协议）将违反DLP策略的HTTP/S流量转发到您的本地DLP服务器，以便进一步分析。

将安全访问与本地DLP服务器集成

- 集成使用安全ICAP，可将违反DLP策略的HTTP/S流量安全地传输到您的本地DLP服务器，以进行其他检查。
- 安全ICAP使用TLS加密流量并使用在Umbrella控制面板中上传的证书对DLP服务器进行身份验证。
- 限制入站防火墙规则，仅允许从Umbrella IP地址到DLP服务器的ICAP端口的流量，以增强安全性。

要允许的必需IP地址

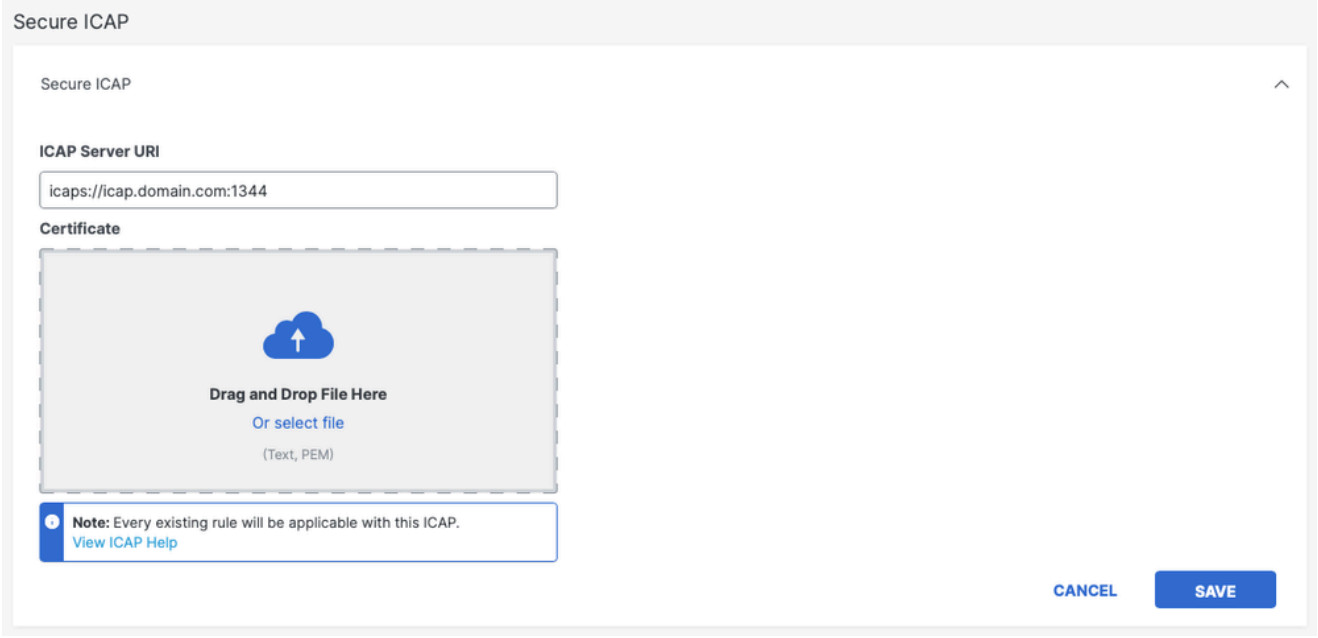
将以下Umbrella IP地址添加到防火墙以允许安全ICAP流量：

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

启用安全ICAP集成

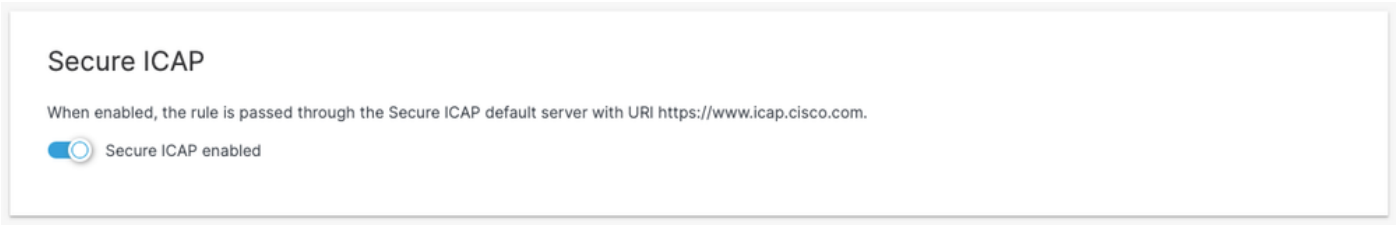
1. 加入本地DLP服务器：

    - 在Umbrella控制面板中，转至Admin > Authentication > ICAP。
    - 上传DLP服务器证书以启用安全ICAP。



2. 配置实时DLP规则以将流量转发到本地DLP服务器：

    - 在规则配置中，使用ICAP部分启用转发。
    - 默认情况下，所有实时DLP活动规则均处于启用状态。



发送到本地DLP服务器的数据

- Umbrella将整个HTTP/S消息（正文和报头）发送到本地DLP服务器。
- 包含自定义信头：
    - X-Authenticated-User：用户身份
    - X-Authenticated-Groups：用户组身份
    - X-Client-IP：客户端IP地址

支持的违规事件

监控和阻止的实时DLP违规事件都通过安全ICAP发送。

在DLP服务器上启用ICAP

请参阅您的DLP解决方案文档和支持，以启用嵌入式ICAP服务器。如果仅支持ICAP（非安全ICAP），请在您的本地DLP服务器之前部署TLS终端组件（如Stunnel）以启用安全ICAP。

相关资源

请参阅Umbrella文档以获取其他指导：管理安全ICAP

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）。