使用安全ICAP將安全訪問與本地DLP整合

目錄

簡介

本文檔介紹如何使用安全ICAP將安全訪問與本地資料丟失防護(DLP)伺服器整合。

概觀

您可以將Umbrella與您的本地DLP解決方案整合，以實現集中式事件管理和補救工作流程。此整合使用安全ICAP（Internet內容自適應協定）將違反DLP策略的HTTP/S流量轉發到您的本地DLP伺服器，以便進一步分析。

將安全訪問與本地DLP伺服器整合

- 整合使用安全ICAP，後者將違反DLP策略的HTTP/S流量安全地傳輸到您的本地DLP伺服器，以進行其他檢查。
- 安全ICAP使用TLS加密流量，並使用在Umbrella控制面板中上載的證書對DLP伺服器進行身份驗證。
- 限制入站防火牆規則，以便僅允許從Umbrella IP地址到DLP伺服器的ICAP埠的流量，以增強安全性。

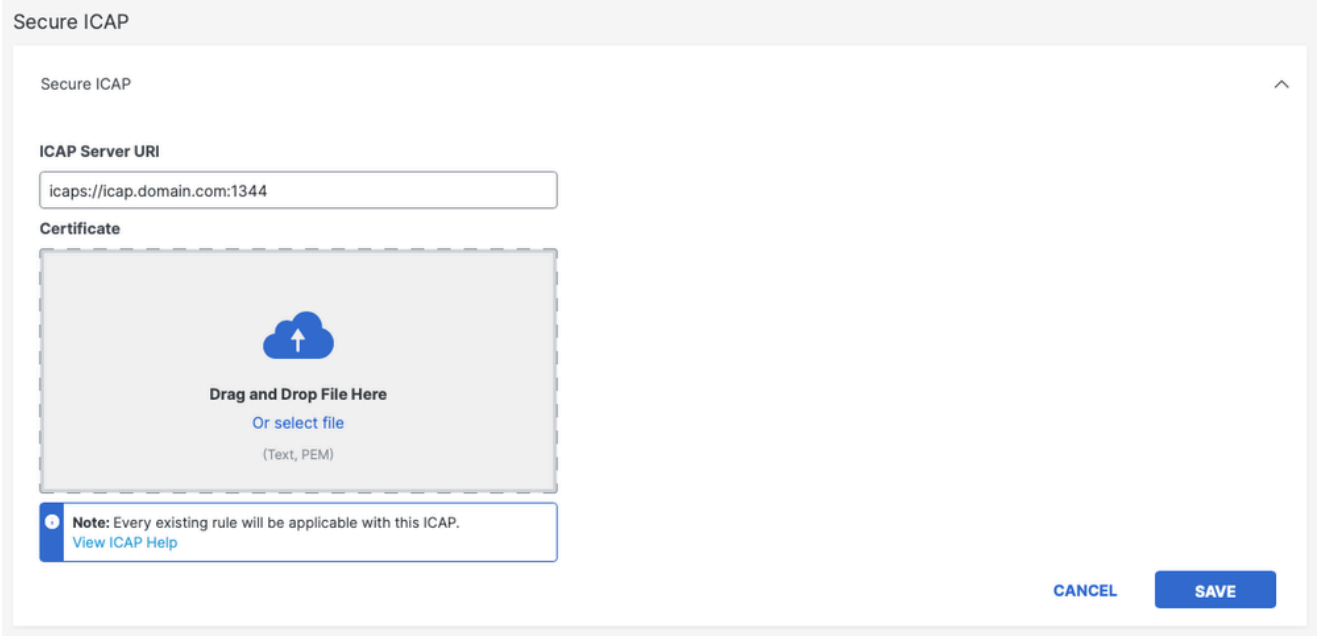
要允許的必需IP地址

向防火牆新增以下Umbrella IP地址以允許安全ICAP流量：

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

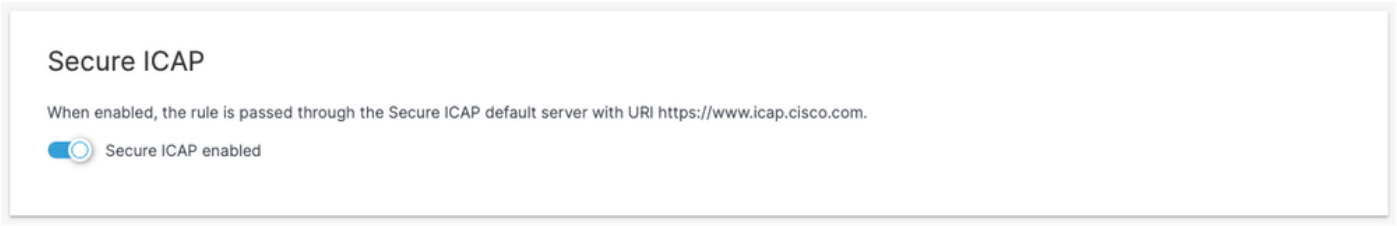
啟用安全ICAP整合

1. 載入您的本地DLP伺服器：
    - 在Umbrella控制面板中，轉至Admin > Authentication > ICAP。
    - 上傳DLP伺服器證書以啟用安全ICAP。



2. 配置即時DLP規則以將流量轉發到本地DLP伺服器：

    - 在規則配置中，使用ICAP部分啟用轉發。
    - 預設情況下啟用所有即時DLP活動規則。



傳送到本地DLP伺服器的資料

- Umbrella將整個HTTP/S消息（正文和標頭）傳送到本地DLP伺服器。
- 包含自定義標頭：
    - X-Authenticated-User：用戶身份
    - X-Authenticated-Groups：用戶組標識
    - X-Client-IP：客戶端IP地址

支援的違規事件

受監控和阻止的即時DLP違規事件均通過安全ICAP傳送。

在DLP伺服器上啟用ICAP

請參考DLP解決方案文檔和支援，以啟用嵌入式ICAP伺服器。如果僅支援ICAP（非安全ICAP），請在本地DLP伺服器之前部署TLS終端元件（如Stunnel）以啟用安全ICAP。

相關資源

請參閱Umbrella文檔以獲取其他指導：管理安全ICAP

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。