Secure ICAPを使用したセキュアなアクセスとオンプレミスのDLPの統合

内容

はじめに

このドキュメントでは、Secure ICAPを使用して、セキュアアクセス(PAC)をオンプレミスのデータ損失防止(DLP)サーバと統合する方法について説明します。

概要

UmbrellaをオンプレミスのDLPソリューションと統合して、イベントの一元管理と修復ワークフローを実現できます。この統合では、Secure ICAP(Internet Content Adaptation Protocol)を使用して、DLPポリシーに違反するHTTP/Sトラフィックをオンプレミスの DLPサーバに転送し、さらなる分析を行います。

セキュアなアクセスとオンプレミスのDLPサーバの統合

- 統合では、Secure ICAPを使用します。これは、DLPポリシーに違反するHTTP/Sトラフィックをオンプレミスの DLPサーバに安全に転送し、追加のインスペクションを実行します。
- Secure ICAPは、TLSを使用してトラフィックを暗号化し、Umbrellaダッシュボードにアップロードされた証明書を使用してDLPサーバを認証します。
- セキュリティを強化するため、Umbrella IPアドレスからDLPサーバのICAPポートへのトラフィックのみを許可するように着信ファイアウォール規則を制限します。

許可に必要なIPアドレス

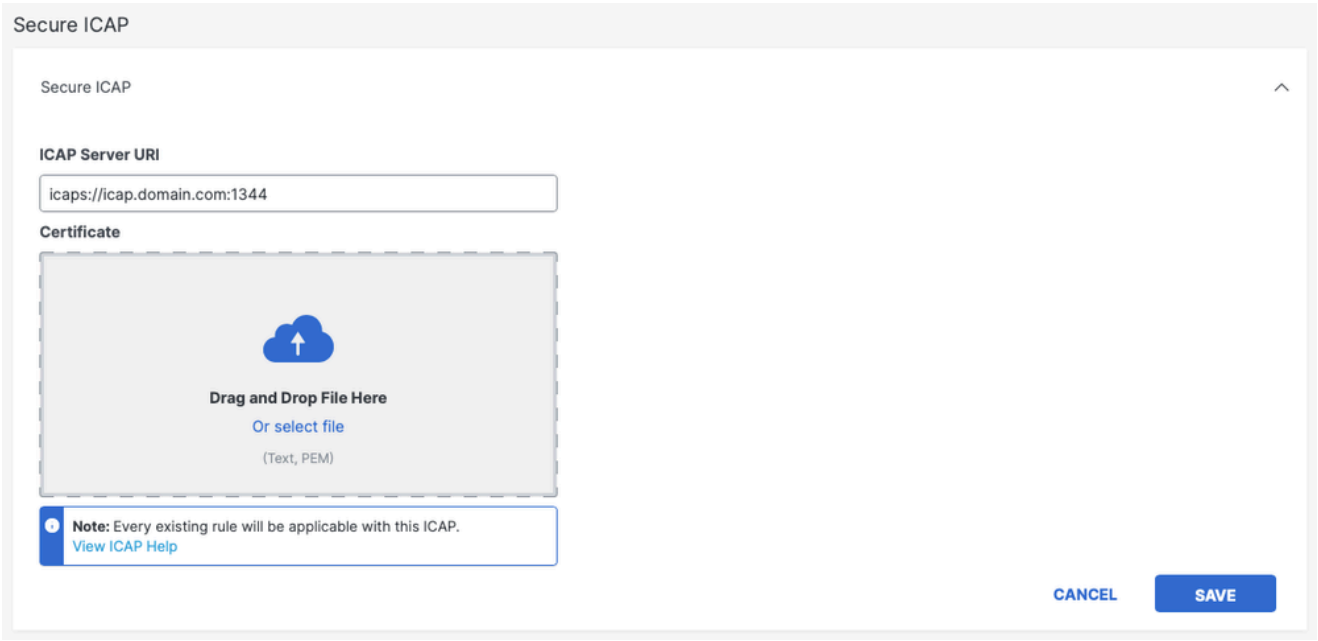
次のUmbrella IPアドレスをファイアウォールに追加して、セキュアICAPトラフィックを許可します。

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

セキュアなICAP統合の有効化

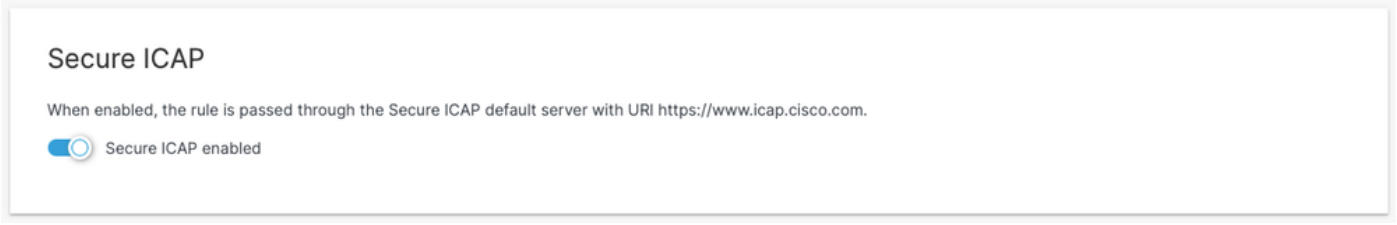
1. オンプレミスDLPサーバのオンボード：
    - Umbrellaダッシュボードで、Admin > Authentication > ICAPの順に選択します。

- DLPサーバ証明書をアップロードして、Secure ICAPを有効にします。



2. オンプレミスDLPサーバにトラフィックを転送するためのリアルタイムDLPルールを設定します。

    - ルール設定では、ICAPsectionを使用して転送を有効にします。
    - リアルタイムDLPのアクティブなルールはすべてデフォルトで有効になっています。



オンプレミスDLPサーバに送信されるデータ

- Umbrellaは、HTTP/Sメッセージ全体（本文とヘッダー）をオンプレミスのDLPサーバに送信します。
- カスタムヘッダーが含まれます。
    - X-Authenticated-User:ユーザID
    - X-Authenticated-Groups:ユーザグループID
    - X-Client-IP:クライアントIPアドレス

サポートされる違反イベント

監視されるリアルタイムDLP違反イベントとブロックされるリアルタイムDLP違反イベントの両方がSecure ICAP経由で送信されます。

DLPサーバでのICAPの有効化

組み込みICAPサーバを有効にするには、DLPソリューションのマニュアルとサポートを参照してください。ICAP（Secure ICAPではない）のみがサポートされている場合、オンプレミスのDLPサーバの前にTLSターミネーションコンポーネント（Stunnelなど）を展開して、Secure ICAPを有効にします。

関連するリソース

詳細については、Umbrellaのドキュメント「Manage Secure ICAP」を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。