Intégrer un accès sécurisé avec DLP sur site à l'aide de Secure ICAP

Table des matières

Introduction

Ce document décrit comment intégrer l'accès sécurisé aux serveurs DLP (Data Loss Prevention) sur site à l'aide de Secure ICAP.

Aperçu

Vous pouvez intégrer Umbrella à votre solution DLP sur site pour centraliser la gestion des événements et les workflows de résolution. Cette intégration utilise le protocole Secure ICAP (Internet Content Adaptation Protocol) pour transférer le trafic HTTP/S qui enfreint les stratégies DLP vers votre serveur DLP sur site pour une analyse plus approfondie.

Intégrer un accès sécurisé aux serveurs DLP sur site

- L'intégration utilise Secure ICAP, qui transfère en toute sécurité le trafic HTTP/S qui viole les stratégies DLP vers votre serveur DLP sur site pour une inspection supplémentaire.
- Secure ICAP chiffre le trafic à l'aide de TLS et authentifie votre serveur DLP avec un certificat téléchargé dans le tableau de bord Umbrella.
- Limitez les règles de pare-feu entrantes pour autoriser uniquement le trafic des adresses IP Umbrella vers le port ICAP de votre serveur DLP pour une sécurité améliorée.

Adresses IP requises à autoriser

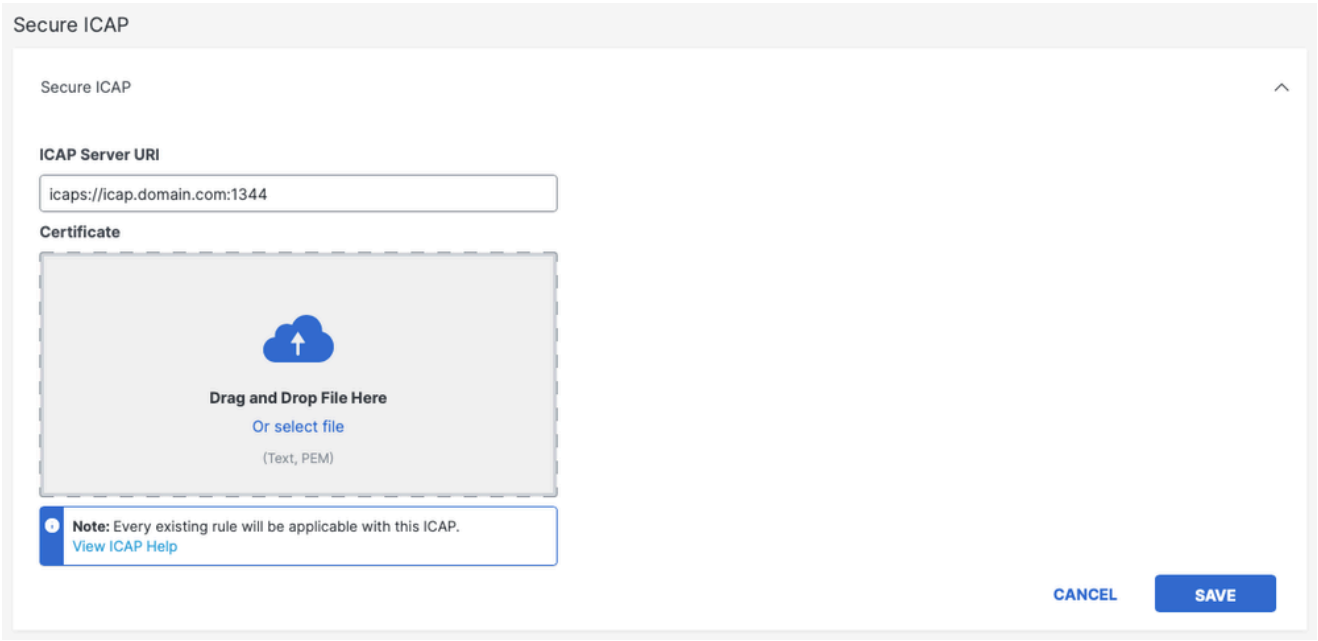
Ajoutez les adresses IP Umbrella suivantes à votre pare-feu pour permettre le trafic ICAP sécurisé :

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Activer l'intégration ICAP sécurisée

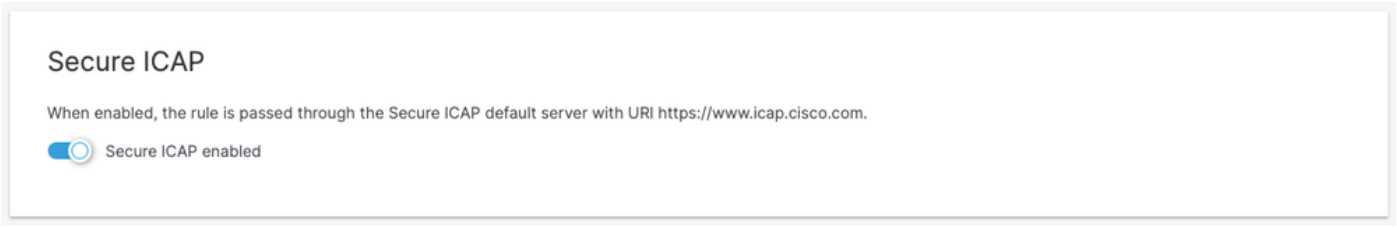
1. Intégrez votre serveur DLP sur site :
    - Dans le tableau de bord Umbrella, accédez à Admin > Authentication > ICAP.

- Téléchargez le certificat du serveur DLP pour activer Secure ICAP.



2. Configurez les règles DLP en temps réel pour transférer le trafic vers le serveur DLP sur site :

   - Dans la configuration de la règle, utilisez la section ICAP pour activer le transfert.
   - Toutes les règles DLP actives en temps réel sont activées par défaut.



Données envoyées au serveur DLP sur site

- Umbrella envoie l'intégralité du message HTTP/S (corps et en-têtes) au serveur DLP sur site.
- Les en-têtes personnalisés sont inclus :
  - X-Authenticated-User:identité de l'utilisateur
  - X-Authenticated-Groups:identité du groupe d'utilisateurs
  - X-Client-IP:adresse IP du client

Événements de violation pris en charge

Les événements de violation DLP en temps réel surveillés et bloqués sont envoyés via Secure ICAP.

Activer ICAP sur votre serveur DLP

Consultez la documentation et l'assistance de votre solution DLP pour activer le serveur ICAP intégré. Si seul ICAP (et non Secure ICAP) est pris en charge, déployez un composant de terminaison TLS (tel que Stunnel) devant votre serveur DLP sur site pour activer Secure ICAP.

Ressources connexes

Reportez-vous à la documentation Umbrella pour obtenir des conseils supplémentaires : Manage Secure ICAP

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.