Integrazione di Secure Access con DLP locale tramite Secure ICAP

Sommario

Introduzione

In questo documento viene descritto come integrare Secure Access con i server DLP (Data Loss Prevention) locali utilizzando Secure ICAP.

Panoramica

È possibile integrare Umbrella con la soluzione DLP locale per la gestione centralizzata degli eventi e i flussi di lavoro di correzione. Questa integrazione utilizza Secure ICAP (Internet Content Adaptation Protocol) per inoltrare il traffico HTTP/S che viola i criteri di prevenzione della perdita dei dati al server di prevenzione della perdita dei dati locale per un'ulteriore analisi.

Integrazione dell'accesso sicuro con i server DLP locali

- L'integrazione utilizza Secure ICAP, che trasferisce in modo sicuro il traffico HTTP/S che viola i criteri di prevenzione della perdita dei dati al server di prevenzione della perdita dei dati locale per un'ulteriore ispezione.
- Secure ICAP crittografa il traffico utilizzando TLS e autentica il server DLP con un certificato caricato nel dashboard Umbrella.
- Limita le regole del firewall in entrata per consentire solo il traffico dagli indirizzi IP Umbrella alla porta ICAP del server DLP per una maggiore sicurezza.

Indirizzi IP richiesti da consentire

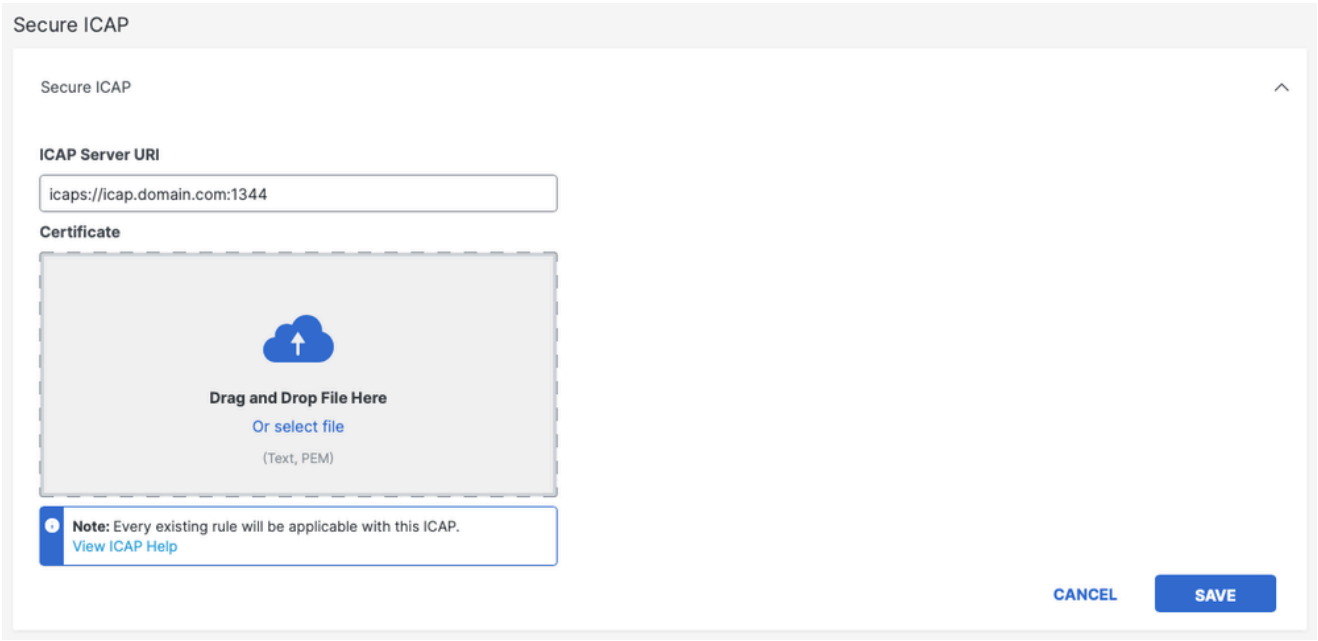
Aggiungere questi indirizzi IP Umbrella al firewall per consentire il traffico ICAP sicuro:

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Abilita integrazione ICAP sicura

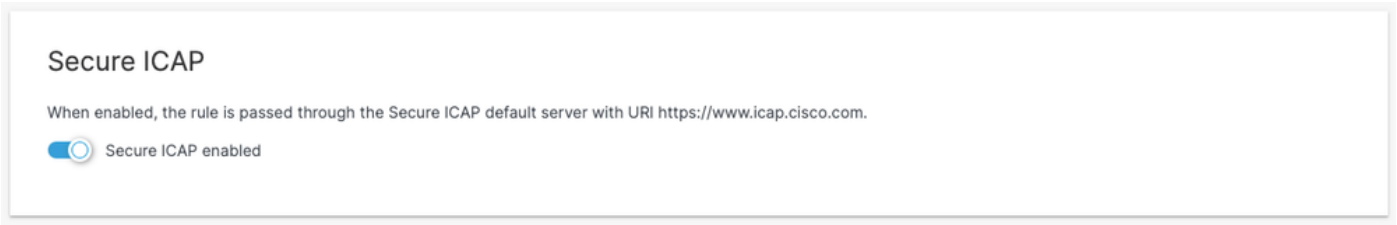
1. Server DLP locale integrato:
    - Nel dashboard Umbrella, andare aAmministrazione > Autenticazione > ICAP.

- Caricare il certificato del server DLP per abilitare Secure ICAP.



2. Configurare le regole di prevenzione della perdita dei dati in tempo reale per inoltrare il traffico al server di prevenzione della perdita dei dati locale:

    - Nella configurazione della regola, utilizzare la sezione ICAP per abilitare l'inoltro.
    - Tutte le regole attive di prevenzione della perdita dei dati in tempo reale sono abilitate per impostazione predefinita.



Dati inviati al server DLP locale

- Umbrella invia l'intero messaggio HTTP/S (corpo e intestazioni) al server DLP locale.
- Intestazioni personalizzate incluse:
    - X-Authenticated-User:Identità utente
    - X-Authenticated-Groups:Identità gruppo utenti
    - X-Client-IP:Indirizzo IP client

Eventi di violazione supportati

Gli eventi di violazione dei criteri di prevenzione della perdita dei dati in tempo reale, sia monitorati che bloccati, vengono inviati tramite Secure ICAP.

Abilita ICAP sul server DLP

Per abilitare il server ICAP incorporato, consultare la documentazione e il supporto della soluzione DLP. Se è supportato solo ICAP (non Secure ICAP), distribuire un componente di terminazione TLS (ad esempio Stunnel) davanti al server DLP locale per abilitare Secure ICAP.

Risorse correlate

Per ulteriori informazioni, fare riferimento alla documentazione di Umbrella: Gestione sicura di ICAP

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).