Integration von sicherem Zugriff mit Vor-Ort-DLP über sicheres ICAP

Inhalt

Einleitung

In diesem Dokument wird die Integration von sicherem Zugriff mit lokalen DLP-Servern (Data Loss Prevention) unter Verwendung von sicherem ICAP beschrieben.

Überblick

Sie können Umbrella in Ihre DLP-Lösung vor Ort integrieren und so ein zentrales Management von Sicherheitsvorfällen und Workflows zur Problembehebung ermöglichen. Bei dieser Integration wird Secure ICAP (Internet Content Adaptation Protocol) verwendet, um HTTP/S-Datenverkehr, der gegen DLP-Richtlinien verstößt, zur weiteren Analyse an den lokalen DLP-Server weiterzuleiten.

Integration von sicherem Zugriff mit lokalen DLP-Servern

- Für die Integration wird Secure ICAP verwendet, das einen gegen die DLP-Richtlinien verstoßenden HTTP/S-Verkehr sicher an den lokalen DLP-Server überträgt, um eine zusätzliche Überprüfung zu ermöglichen.
- Secure ICAP verschlüsselt den Datenverkehr mithilfe von TLS und authentifiziert Ihren DLP-Server mit einem im Umbrella Dashboard hochgeladenen Zertifikat.
- Beschränken Sie eingehende Firewall-Regeln, um nur den Datenverkehr von Umbrella IP-Adressen zum ICAP-Port Ihres DLP-Servers zu erlauben, um die Sicherheit zu erhöhen.

Zulässige erforderliche IP-Adressen

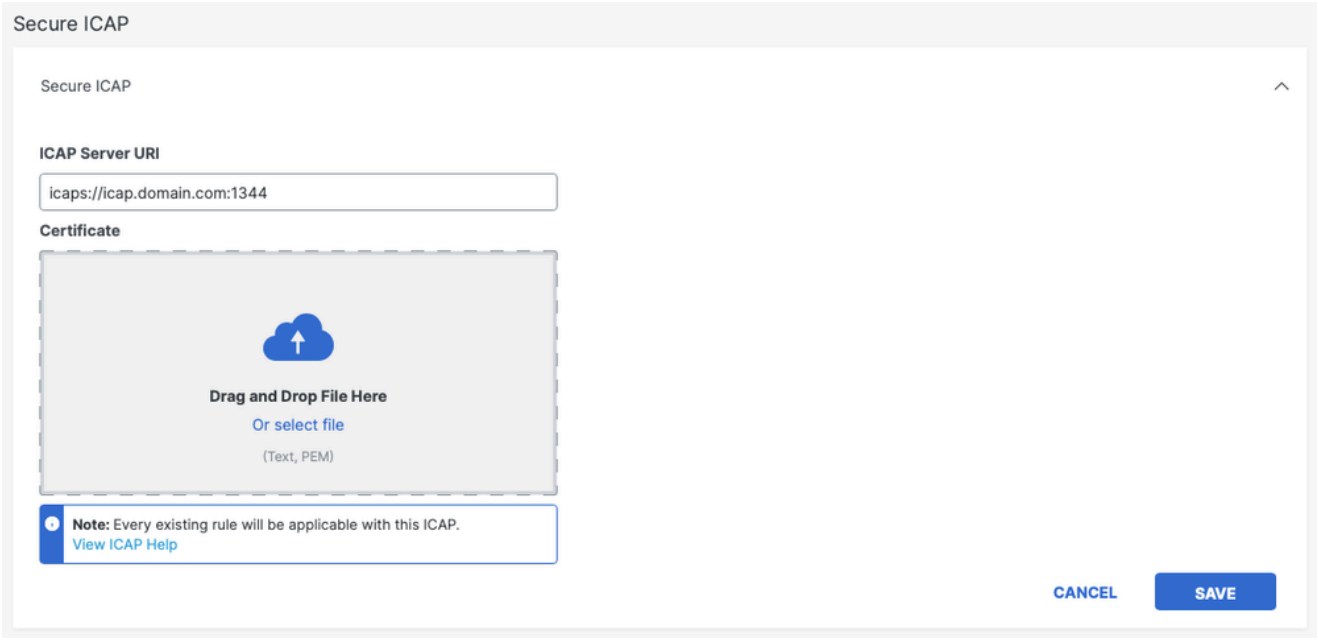
Fügen Sie Ihrer Firewall die folgenden Umbrella IP-Adressen hinzu, um sicheren ICAP-Datenverkehr zuzulassen:

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Sichere ICAP-Integration aktivieren

1. Integrieren Sie den lokalen DLP-Server:

    - Gehen Sie im Umbrella Dashboard zuAdmin > Authentication > ICAP.
    - Laden Sie das SvD-Serverzertifikat hoch, um Secure ICAP zu aktivieren.



2. Konfigurieren Sie Echtzeit-SvD-Regeln, um Datenverkehr an den lokalen SvD-Server weiterzuleiten:

    - Verwenden Sie in der Regelkonfiguration den ICAP-Abschnitt, um die Weiterleitung zu aktivieren.
    - Alle aktiven Echtzeit-SvD-Regeln sind standardmäßig aktiviert.

An lokalen SvD-Server gesendete Daten

- Umbrella sendet die gesamte HTTP/S-Nachricht (Text und Header) an den lokalen DLP-Server.
- Benutzerdefinierte Header sind enthalten:
    - X-Authenticated-User:Benutzeridentität
    - X-Authenticated-Groups: Benutzergruppenidentität
    - X-Client-IP:Client-IP-Adresse

Unterstützte Verletzungsereignisse

Sowohl überwachte als auch blockierte DLP-Verletzungsereignisse in Echtzeit werden über

Secure ICAP gesendet.

Aktivieren Sie ICAP auf Ihrem SvD-Server

Informationen zur Aktivierung des integrierten ICAP-Servers finden Sie in der DLP-Lösungsdokumentation und im Support. Wenn nur ICAP (nicht Secure ICAP) unterstützt wird, stellen Sie eine TLS-Terminierungskomponente (wie z. B. Stunnel) vor Ihrem lokalen DLP-Server bereit, um Secure ICAP zu aktivieren.

Zugehörige Ressourcen

Weitere Informationen finden Sie in der Umbrella-Dokumentation: Sicheres ICAP verwalten

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.