Integre el acceso seguro con DLP en las instalaciones mediante ICAP seguro

Contenido

Introducción

Este documento describe cómo integrar Secure Access con servidores de prevención de pérdida de datos (DLP) in situ mediante Secure ICAP.

Overview

Puede integrar Umbrella con su solución de DLP in situ para gestionar eventos centralizados y flujos de trabajo de remediación. Esta integración utiliza Secure ICAP (Internet Content Adaptation Protocol) para reenviar el tráfico HTTP/S que infringe las políticas de DLP a su servidor DLP en las instalaciones para su posterior análisis.

Integre el acceso seguro con servidores DLP en las instalaciones

- La integración utiliza ICAP seguro, que transfiere de forma segura el tráfico HTTP/S que infringe las políticas de DLP a su servidor DLP en las instalaciones para una inspección adicional.
- Secure ICAP cifra el tráfico mediante TLS y autentica el servidor DLP con un certificado cargado en el panel de Umbrella.
- Restrinja las reglas de firewall de entrada para permitir solo el tráfico de las direcciones IP de Umbrella al puerto ICAP del servidor DLP para mejorar la seguridad.

Direcciones IP necesarias para permitir

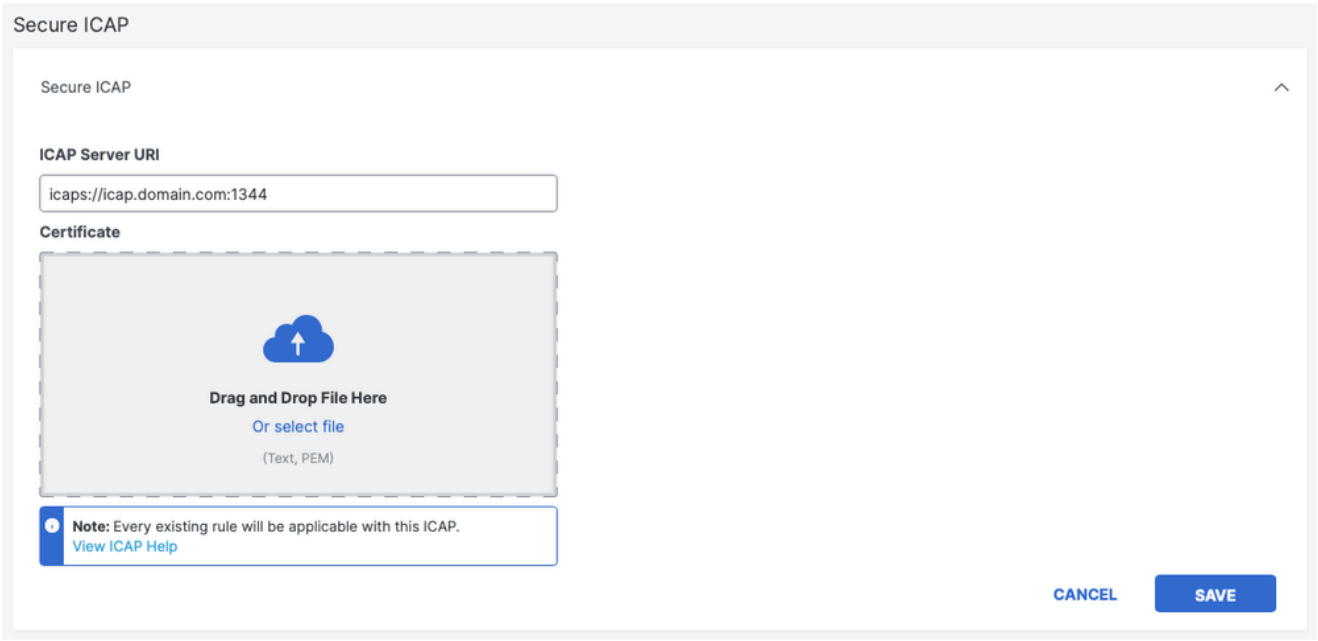
Agregue estas direcciones IP de Umbrella al firewall para permitir el tráfico ICAP seguro:

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Habilitar integración segura de ICAP

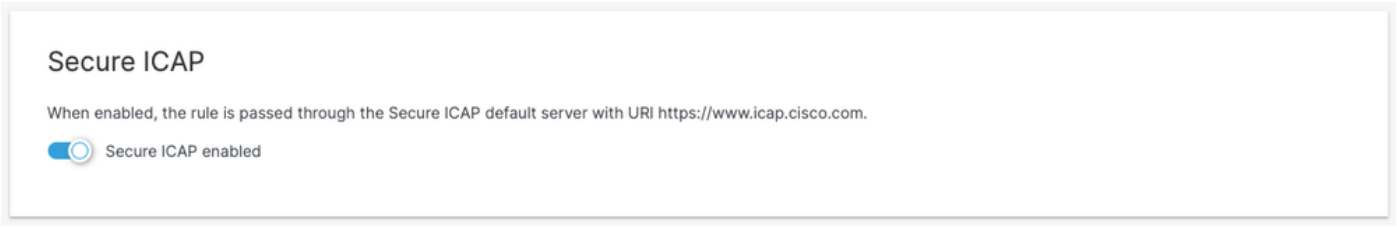
1. Incorpore su servidor DLP en las instalaciones:
    - En el panel de Umbrella, vaya aAdmin > Authentication > ICAP.

- Cargue el certificado del servidor DLP para activar el ICAP seguro.



2. Configuración de reglas de DLP en tiempo real para reenviar el tráfico al servidor DLP local:

   - En la configuración de la regla, utilice la secciónICAPpara habilitar el reenvío.
   - Todas las reglas activas de DLP en tiempo real están activadas de forma predeterminada.



Datos enviados al servidor DLP local

- Umbrella envía el mensaje HTTP/S completo (cuerpo y encabezados) al servidor DLP local.
- Se incluyen encabezados personalizados:
  - X-Authenticated-User:Identidad de usuario
  - X-Authenticated-Groups:identidad de grupo de usuarios
  - X-Client-IP:Dirección IP del cliente

Eventos de violación admitidos

Los eventos de violación de DLP en tiempo real supervisados y bloqueados se envían a través de ICAP seguro.

Activar ICAP en el servidor DLP

Consulte la documentación y la asistencia de la solución DLP para habilitar el servidor ICAP integrado. Si sólo se admite ICAP (no ICAP seguro), implemente un componente de terminación de TLS (como Stunnel) delante del servidor DLP en las instalaciones para habilitar ICAP seguro.

Recursos relacionados

Consulte la documentación de Umbrella para obtener orientación adicional: Administración de Secure ICAP

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).