Comprender cómo el proxy SWG gestiona las solicitudes HTTPS no estándar

Contenido

Introducción

Este documento describe cómo SWG Proxy procesa las solicitudes HTTPS no estándar y describe el cumplimiento de cliente requerido.

Overview

Umbrella se basa en la extensión SNI de TLS para detectar el dominio de destino y determinar si una solicitud HTTPS requiere descifrado o omisión del descifrado mediante listas de descifrado selectivo. El cliente debe cumplir con los estándares de TLS definidos en las RFC relevantes. La mayoría de los navegadores conocidos cumplen con estos estándares y Umbrella los soporta.

Preguntas comunes

¿Puede el proxy SWG procesar solicitudes web HTTPS no estándar?

No. La solicitud HTTPS falla si el cliente no realiza un intercambio de señales TLS básico. Por ejemplo, si falta el intercambio Hello del cliente o Hello del servidor, la solicitud no puede completarse.

¿Puede ser útil deshabilitar la inspección de HTTPS o agregar el dominio en cuestión a la lista de descifrado selectivo?

No, estas acciones no resuelven el problema.

Solución

Debe omitir el proxy SWG completamente para el sitio HTTPS no estándar en cuestión.

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).