Comprensión del Descifrado de Tráfico SWG con Descifrado HTTPS Activado

Contenido

Introducción

Este documento describe cómo Cisco Secure Web Gateway (SWG) maneja el descifrado del tráfico cuando el descifrado HTTPS está habilitado.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Secure Web Gateway.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

En una regla de política web establecida con el descifrado HTTPS habilitado, el tráfico se descifra sólo si hay un indicador de nombre de servidor (SNI) presente en el intercambio de señales TLS.

Solución

Las políticas de seguridad y de uso aceptable se pueden seguir aplicando en función de los servidores de destino a los que se envía la solicitud. Se pueden crear listas de destino para estos

servidores de destino y se pueden aplicar las reglas correspondientes.

Todavía se puede aplicar cualquier bloque para las políticas DNS para túneles y AnyConnect.

Causa

Este comportamiento es por diseño.

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).