Resolución de problemas de validación reCAPTCHA al acceder a Google mediante SWG

Contenido

Introducción

Este documento describe cómo resolver problemas al ver la validación de Google reCAPTCHA al acceder a Google.com a través de Umbrella Secure Web Gateway (SWG).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

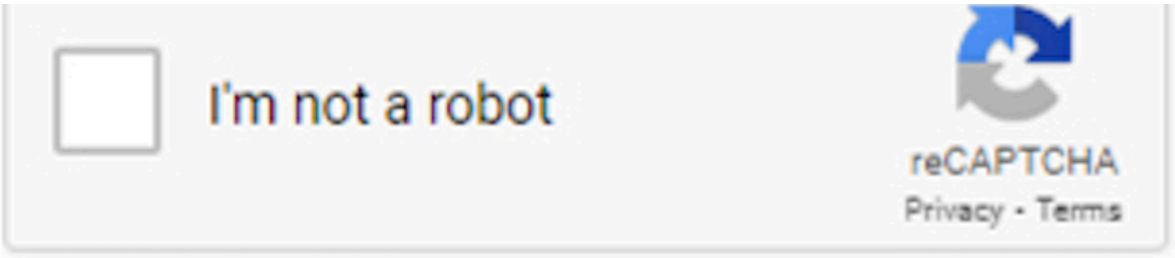
La información de este documento se basa en Cisco Umbrella SWG.

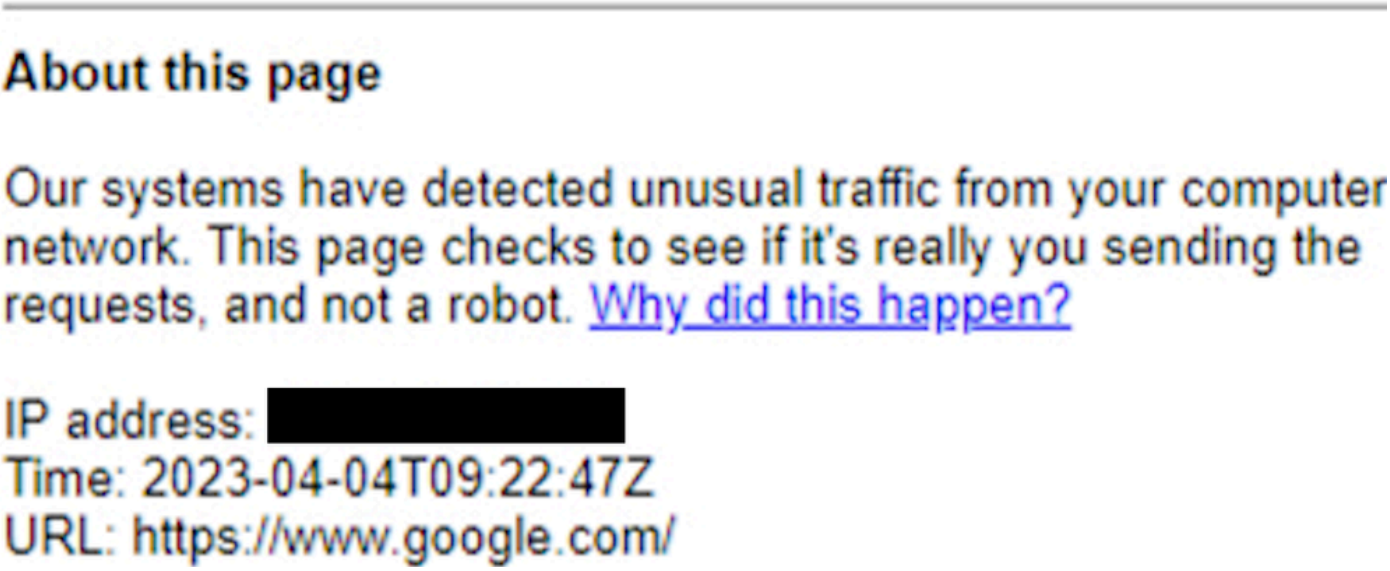
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Problema

Cuando intenta acceder a Google.com a través de Umbrella Secure Web Gateway (SWG), recibe un mensaje de error que indica "tráfico inusual de su red informática" y necesita realizar el

proceso reCAPTCHA de Google seleccionando la casilla "No soy un robot" para validar que el usuario es un ser humano en lugar de un programa (un "bot").





Solución

Google utiliza mecanismos propios para detectar y bloquear el tráfico automatizado. Este tipo de tráfico también infringe las condiciones de uso de Cisco Umbrella. Cisco colabora con Google y otros servicios para supervisar, bloquear y/o aislar a los usuarios infractores.

Ocasionalmente, Google marca como sospechosa una dirección IP o un rango de direcciones IP que utiliza el SWG de Umbrella para el tráfico de salida, y se presenta reCAPTCHA.

La mayoría de los clientes de Cisco Umbrella utilizan rangos de IP de salida que se solapan con los de otros clientes, lo que se denomina "NAT compartida". Para obtener más información sobre los intervalos de IP de salida de Umbrella SIG, consulte el artículo mencionado aquí. Si la acción de un cliente activa el reCAPTCHA, otros clientes utilizan esa dirección IP de salida que también puede ser necesaria para realizar el proceso reCAPTCHA.

Pruebe estas soluciones temporales para resolver este problema:

Opción 1

Habilite la inspección HTTPS para Google.com, de modo que Umbrella pueda insertar un encabezado Reenviado (XFF). Este encabezado reduce la ocurrencia de ReCAPTCHA y también mejora la geolocalización.

Opción 2

Actualice su servicio Umbrella para utilizar una "IP reservada", en lugar de una NAT compartida. Una IP reservada está dedicada a su tráfico, por lo que el reCAPTCHA no puede ser activado por el comportamiento de otros clientes.

Opción 3

Excluya el tráfico de Google de pasar por Umbrella SWG. Para implementaciones de archivos Secure Client, Anyconnect o PAC, utilice External Domains para gestionar las exclusiones. Para los túneles IPSec, las exclusiones se pueden configurar en el dispositivo que proporciona el túnel IPSec o en un dispositivo que enruta el tráfico al túnel IPSec.

Opción 4

Utilice un motor de búsqueda alternativo.

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).