Dépannage de la validation reCAPTCHA lors de l'accès à Google via SWG

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Problème
- Solution
  - Option 1
  - Option 2
  - Option 3
  - Option 4

Introduction

Ce document décrit comment dépanner la validation de Google reCAPTCHA lors de l'accès à Google.com via Umbrella Secure Web Gateway (SWG).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

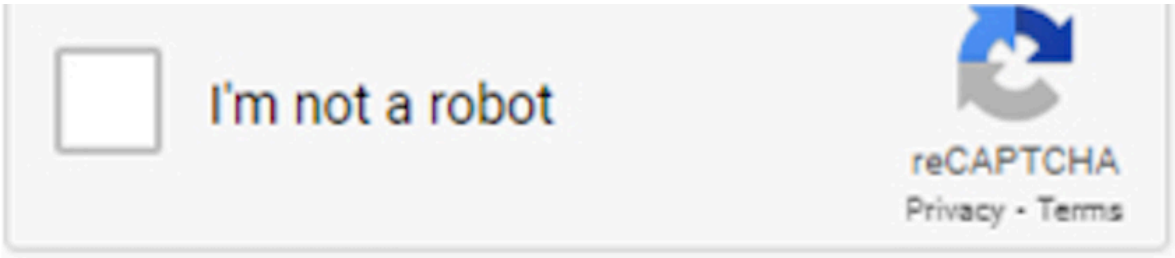
Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella SWG.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Lorsque vous essayez d'accéder à Google.com via Umbrella Secure Web Gateway (SWG), vous recevez un message d'erreur indiquant « trafic inhabituel en provenance de votre réseau informatique » et vous devez exécuter le processus reCAPTCHA de Google en cochant la case « Je ne suis pas un robot » pour valider que l'utilisateur est un humain plutôt qu'un programme (un « bot »).



About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: [redacted]
Time: 2023-04-04T09:22:47Z
URL: https://www.google.com/

Solution

Google utilise des mécanismes propriétaires pour détecter et bloquer le trafic automatisé. Ce type de trafic enfreint également les conditions d'utilisation de Cisco Umbrella. Cisco travaille avec Google et d'autres services pour surveiller, bloquer et/ou isoler les utilisateurs contrevenants.

Occasionnellement, une adresse IP ou une plage d'adresses IP utilisée par le SWG d'Umbrella pour le trafic de sortie est signalée comme suspecte par Google, et reCAPTCHA est présenté.

La plupart des clients Cisco Umbrella utilisent des plages d'adresses IP de sortie qui chevauchent celles des autres clients, ce que l'on appelle la « NAT partagée ». Pour plus d'informations sur les plages IP de sortie Umbrella SIG, veuillez vous reporter à l'article mentionné ici. Si l'action d'un client déclenche le processus reCAPTCHA, d'autres clients utilisent cette adresse IP de sortie qui peut également être requise pour exécuter le processus reCAPTCHA.

Essayez ces solutions de contournement pour résoudre ce problème :

Option 1

Activez l'inspection HTTPS pour Google.com, afin qu'Umbrella puisse insérer un en-tête XFF (Forwarded). Cet en-tête réduit les occurrences ReCAPTCHA et améliore également la géolocalisation.

Option 2

Mettez à niveau votre service Umbrella pour utiliser une "adresse IP réservée", plutôt qu'une NAT partagée. Une adresse IP réservée est dédiée à votre trafic, de sorte que le reCAPTCHA ne peut pas être déclenché par le comportement d'autres clients.

Option 3

Exclure le trafic Google du trafic via Umbrella SWG. Pour les déploiements de fichiers Secure Client, Anyconnect ou PAC, utilisez External Domains pour gérer les exclusions. Pour les tunnels IPSec, des exclusions peuvent être configurées sur le périphérique qui fournit le tunnel IPSec ou sur un périphérique qui achemine le trafic vers le tunnel IPSec.

Option 4

Utiliser un autre moteur de recherche.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.