

Solucione problemas de validação do reCAPTCHA ao acessar o Google via SWG

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

[Opção 1](#)

[Opção 2](#)

[Opção 3](#)

[Opção 4](#)

Introdução

Este documento descreve como solucionar problemas relacionados à validação do Google reCAPTCHA ao acessar Google.com via Umbrella Secure Web Gateway (SWG).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

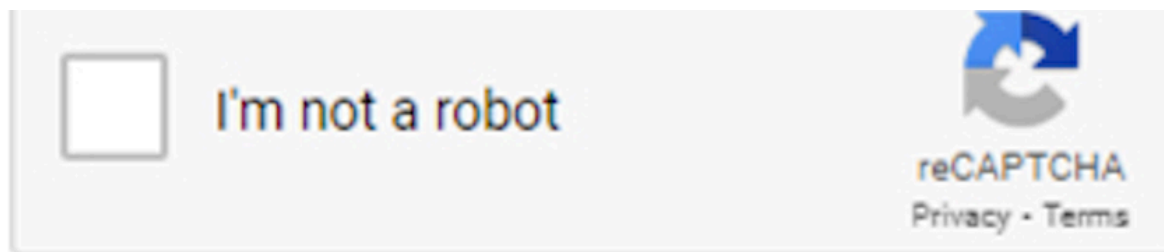
Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella SWG.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Quando você tenta acessar Google.com através do Umbrella Secure Web Gateway (SWG), você recebe uma mensagem de erro indicando "tráfego incomum de sua rede de computadores" e precisa executar o processo reCAPTCHA do Google marcando a caixa de seleção "Eu não sou um robô" para validar que o usuário é um humano em vez de um programa (um "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/>

Solução

O Google usa mecanismos proprietários para detectar e bloquear o tráfego automatizado. Esse tipo de tráfego também viola os termos de uso do Cisco Umbrella. A Cisco trabalha com o Google e outros serviços para monitorar, bloquear e/ou isolar usuários ofensivos.

Ocasionalmente, um endereço IP ou intervalo de endereços IP usado pelo SWG da Umbrella para tráfego de saída é sinalizado como suspeito pelo Google, e reCAPTCHA é apresentado.

A maioria dos clientes do Cisco Umbrella usa intervalos de IP de saída que se sobrepõem aos de outros clientes, que são chamados de "NAT compartilhado". Para obter mais detalhes sobre os intervalos de IP de saída do Umbrella SIG, consulte o artigo mencionado aqui. Se a ação de um cliente acionar o reCAPTCHA, outros clientes usarão esse endereço IP de saída também para executar o processo reCAPTCHA.

Tente estas soluções alternativas para resolver este problema:

Opção 1

Habilite a Inspeção HTTPS para Google.com, para que o Umbrella possa inserir um cabeçalho Encaminhado (XFF). Esse cabeçalho reduz a ocorrência de ReCAPTCHA e também melhora a localização geográfica.

Opção 2

Atualize seu serviço Umbrella para usar um ["IP Reservado"](#), em vez de um NAT compartilhado. Um IP reservado é dedicado ao seu tráfego, portanto o reCAPTCHA não pode ser acionado pelo comportamento de outros clientes.

Opção 3

Exclua o tráfego do Google de passar pelo Umbrella SWG. Para implantações de cliente seguro, Anyconnect ou arquivo PAC, use [Domínios externos](#) para lidar com exclusões. Para túneis IPsec, as exclusões podem ser configuradas no dispositivo que fornece o túnel IPsec, ou em um dispositivo que roteia o tráfego para o túnel IPsec.

Opção 4

Use um mecanismo de pesquisa alternativo.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.