Troubleshoot reCAPTCHA Validation When Accessing Google via SWG

Contents

Introduction

This document describes how to troubleshoot seeing Google reCAPTCHA Validation when accessing Google.com via Umbrella Secure Web Gateway (SWG).

Prerequisites

Requirements

There are no specific requirements for this document.

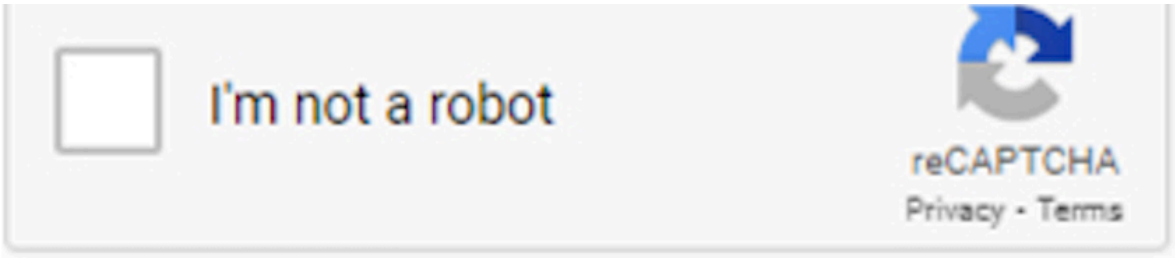
Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

Problem

When you try to access Google.com via Umbrella Secure Web Gateway (SWG), you receive an error message indicating "unusual traffic from your computer network" and need to perform Google's reCAPTCHA process by selecting the "I'm not a robot" checkbox to validate that the user is a human rather than a program (a "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 uses proprietary mechanisms to detect and block automated traffic. This type of traffic also violates Cisco Umbrella's terms of use. Cisco works with Google and other services to monitor, block, and/or isolate offending users.

Occasionally an IP address or range of IP addresses used by Umbrella's SWG for egress traffic is flagged as suspicious by Google, and reCAPTCHA is presented.

Most Cisco Umbrella customers use egress IP ranges that overlap with that of other customers, which is referred as "shared NAT". For more details on Umbrella SIG Egress IP ranges, please refer to the article mentioned here. If one customer's action triggers the reCAPTCHA, other customers use that egress IP address can also be required to perform the reCAPTCHA process.

Try these workarounds to resolve this issue:

Option 1

Enable HTTPS Inspection for Google.com, so that Umbrella can insert a Forwarded (XFF) header. This header reduces ReCAPTCHA occurrence, and also improves geo-location.

Option 2

Upgrade your Umbrella service to use a "Reserved IP", rather than a shared NAT. A reserved IP is dedicated to your traffic, so the reCAPTCHA cannot be triggered by the behavior of other customers.

Option 3

Exclude Google traffic from going through Umbrella SWG. For Secure Client, Anyconnect or PAC file deployments, use External Domains to handle exclusions. For IPSec tunnels, exclusions can be configured on the device which provides the IPSec tunnel, or on a device that routes traffic to the IPSec tunnel.

Option 4

Use an alternate search engine.