

# Problemen met reCAPTCHA-validatie oplossen bij toegang tot Google via SWG

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

[Optie 1](#)

[Optie 2](#)

[Optie 3](#)

[Optie 4](#)

---

## Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen bij het zien van Google reCAPTCHA-validatie bij het openen van Google.com via Umbrella Secure Web Gateway (SWG).

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

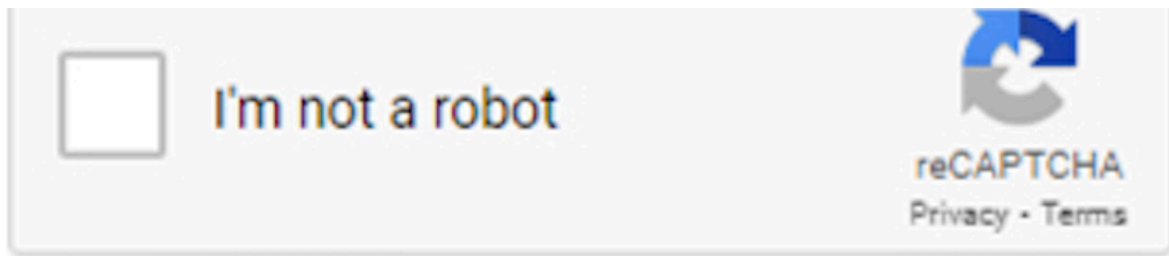
De informatie in dit document is gebaseerd op Cisco Umbrella SWG.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Probleem

Wanneer u probeert toegang te krijgen tot Google.com via Umbrella Secure Web Gateway (SWG), ontvangt u een foutmelding met de vermelding "ongebruikelijk verkeer van uw computernetwerk" en moet u het reCAPTCHA-proces van Google uitvoeren door het selectievakje "Ik ben geen robot" te selecteren om te valideren dat de gebruiker een mens is in plaats van een

programma (een "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/>

## Oplossing

Google gebruikt eigen mechanismen om geautomatiseerd verkeer te detecteren en te blokkeren. Dit soort verkeer is ook in strijd met de gebruiksvoorwaarden van Cisco Umbrella. Cisco werkt samen met Google en andere services om overtredende gebruikers te controleren, blokkeren en/of isoleren.

Af en toe wordt een IP-adres of een reeks IP-adressen die door Umbrella's SWG worden gebruikt voor uitgaand verkeer door Google als verdacht gemarkeerd en wordt reCAPTCHA weergegeven.

De meeste Cisco Umbrella-klanten gebruiken IP-segmenten die overlappen met die van andere klanten, die worden aangeduid als "gedeelde NAT". Voor meer informatie over Umbrella SIG Egress IP-reeksen, verwijzen wij u naar het hier genoemde artikel. Als de actie van een klant de reCAPTCHA activeert, kunnen andere klanten die het IP-adres voor uitgang gebruiken, ook worden gevraagd om het reCAPTCHA-proces uit te voeren.

Probeer deze tijdelijke oplossingen om dit probleem op te lossen:

### Optie 1

Schakel HTTPS-inspectie in voor Google.com, zodat Umbrella een doorgestuurde (XFF) header kan invoegen. Deze header vermindert het voorkomen van ReCAPTCHA en verbetert ook de geolocatie.

## Optie 2

Upgrade uw Umbrella-service om een ["Gereserveerd IP"](#) te gebruiken, in plaats van een gedeelde NAT. Een gereserveerd IP-adres wordt toegewezen aan uw verkeer, dus de reCAPTCHA kan niet worden geactiveerd door het gedrag van andere klanten.

## Optie 3

Sluit Google-verkeer uit van het doorlopen van Umbrella SWG. Gebruik [Externe domeinen](#) voor de implementatie van Secure Client-, Anyconnect- of PAC-bestanden om uitsluitingen af te handelen. Voor IPSec-tunnels kunnen uitsluitingen worden geconfigureerd op het apparaat dat de IPSec-tunnel levert of op een apparaat dat verkeer naar de IPSec-tunnel leidt.

## Optie 4

Gebruik een alternatieve zoekmachine.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.