

HTTP 429-snelheidslimiet en verbindingfouten bij toegang tot toepassingen via Secure Access SWG

Inhoud

uitgifte

Gebruikers krijgen te maken met HTTP 429-snelheidsbegrenzingsfouten wanneer ze proberen toegang te krijgen tot de toepassing, bijvoorbeeld <https://xxxx.com> via Cisco Secure Access SWG (Secure Web Gateway). Het probleem treft door bedrijven beheerde laptops en begon ongeveer twee weken voor de opening van de zaak. Gebruikers ervaren deze fouten tijdens inlogpogingen of bij het openen van bepaalde toepassingsfuncties na succesvolle verificatie.

Wanneer het domein wordt toegevoegd aan de bypass-lijst voor beveiligde toegang, ondervinden gebruikers bovendien HTTP 500-serverfouten tijdens het invoeren van een OTP (eenmalig wachtwoord) of algemene verbindingfouten wanneer het verkeer niet langer via de SWG IP-bereiken (151.186.x.x) verloopt.

De eigenaar van de toepassing bevestigde dat er onlangs geen tarieflimieten zijn gewijzigd aan de serverzijde en het probleem lijkt verband te houden met verkeer afkomstig van Cisco Secure Access SWG Egress IP-adressen.

milieu

- Cisco Secure Access (voorheen Cisco Umbrella) met SWG ingeschakeld
- Zakelijk beheerde laptops met Cisco SSE (Security Service Edge)-client
- SWG egress IP-bereiken: 151.186.x.x
- Datacenters: AWS Singapore (Asia Pacific 1) en AWS US West (Oregon)
- Toepassing: <https://sbstransit.aereacommercial.com>

resolutie

De oplossing omvat het implementeren van een bypass-configuratie en het coördineren met de eigenaar van de toepassing om specifieke IP-adressen te kunnen opsommen.

Volg de volgende stappen.

Stap 1: Huidig SWG-gedrag verifiëren

Controleer het huidige beleid en voer de IP-gegevens in door deze URL te openen vanaf een getroffen apparaat:

`https://policy.test.sse.cisco.com/?host=https://sbstransit.aereacommercial.com`

Hierin wordt het huidige SWG-IP-adres weergegeven dat wordt gebruikt (doorgaans bereik 151.186.x.x) en wordt bevestigd dat het verkeer wordt verwerkt via Secure Access SWG.

Stap 2: Domein toevoegen aan de bypass-lijst voor beveiligde toegang

Navigeer naar Internet Settings > Bypass Secure Access in het Cisco Secure Access-dashboard en voeg het problematische domein toe om zowel DNS- als SWG-inspectie te omzeilen:

`sbstransit.aereacommercial.com`

Stap 3: Test de toegang van een niet-bedrijfsnetwerk

Toepassingstoegang testen vanaf een netwerk waar het verkeer niet doorstroomt via Secure Access SWG (151.186.x.x bereik). Dit kan worden gedaan vanaf een persoonlijk apparaat of door de SSE-client tijdelijk uit te schakelen.

Identificeer het openbare ISP-IP-adres door te gaan naar:

<https://whatismyip.com>

Stap 4: Coördineer IP-autorisatie met de eigenaar van de toepassing

Geef het geïdentificeerde openbare ISP-IP-adres aan de eigenaar van de toepassing en vraag of dit IP aan de toepassingszijde mag worden vermeld. Hiermee kunt u controleren of de toepassing IP-gebaseerde beperkingen implementeert die van invloed zijn op IP-adressen van SWG Secure Access.

Stap 5: Resolutie controleren

Nadat de eigenaar van de toepassing de IP-vermelding heeft geïmplementeerd, test u het toegangsgedrag om te bevestigen dat gebruikers met succes toegang tot de toepassing kunnen krijgen zonder HTTP 429 of verbindingfouten te ondervinden.

Oorzaak

De applicatie lijkt tariefbeperkingen of toegangsbeperkingen te implementeren op basis van bron-IP-adressen. Wanneer meerdere gebruikers toegang krijgen tot de toepassing via Cisco Secure Access SWG, lijkt al het verkeer afkomstig te zijn van gedeelde SWG Egress IP-bereiken (151.186.x.x). Dit zorgt ervoor dat het snelheidsbeperkende mechanisme van de applicatie wordt geactiveerd, omdat het buitensporige verzoeken opmerkt die afkomstig zijn van een enkel IP-adres of IP-bereik.

Het probleem wordt nog verergerd door het feit dat door bedrijven beheerde apparaten het verkeer door de SSE-client blijven leiden, zelfs wanneer deze is aangesloten op persoonlijke netwerken, waarbij hetzelfde IP-gedrag wordt gehandhaafd dat de beperkingen van de toepassing veroorzaakt.

Gerelateerde inhoud

- [Cisco Technical Support en downloads](#)

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.