

HTTP 429-Durchsatzbegrenzung und Verbindungsfehler beim Zugriff auf Anwendungen über SWG für sicheren Zugriff

Inhalt

Problem

Beim Zugriff auf die Anwendung treten Fehler mit HTTP-429-Ratenbegrenzungen auf, z. B. <https://xxxx.com> über Cisco Secure Access SWG (Secure Web Gateway). Das Problem betrifft vom Unternehmen verwaltete Laptops und begann etwa zwei Wochen vor der Eröffnung des Gehäuses. Diese Fehler treten bei Anmeldeversuchen oder beim Zugriff auf bestimmte Anwendungsfunktionen nach erfolgreicher Authentifizierung auf.

Wenn die Domäne zur Umgehungsliste für sicheren Zugriff hinzugefügt wird, treten bei der OTP-Eingabe (einmaliges Kennwort) zusätzlich HTTP 500-Serverfehler auf, oder es treten allgemeine Verbindungsfehler auf, wenn der Datenverkehr nicht mehr über die SWG-IP-Bereiche (151.186.x.x) eingeht.

Der Anwendungseigentümer bestätigte, dass kürzlich auf der Serverseite keine Ratenbeschränkungen geändert wurden. Das Problem scheint mit dem Datenverkehr in Zusammenhang zu stehen, der von den Ausgangs-IP-Adressen der Cisco Secure Access SWG stammt.

Umwelt

- Cisco Secure Access (ehemals Cisco Umbrella) mit aktivierter SWG-Funktion
- Vom Unternehmen verwaltete Laptops mit Cisco SSE-Client (Security Service Edge)
- SWG-Ausgangs-IP-Bereiche: 151.186.x.x
- Rechenzentren: AWS Singapur (Asien-Pazifik-Raum 1) und AWS USA West (Oregon)

- Anwendung: <https://sbstransit.aereacommercial.com>

Auflösung

Die Lösung umfasst die Implementierung einer Bypass-Konfiguration und die Koordination mit dem Anwendungseigentümer, um spezifische IP-Adressen aufzulisten.

Führen Sie die nächsten Schritte aus.

Schritt 1: Aktuelles SWG-Verhalten überprüfen

Überprüfen Sie die aktuelle Richtlinie, und geben Sie IP-Informationen aus, indem Sie von einem betroffenen Gerät auf diese URL zugreifen:

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

Hier sehen Sie die aktuell verwendete SWG-Ausgangs-IP (i. d. R. 151.186.x.x) und die Bestätigung, dass der Datenverkehr über die Secure Access-SWG verarbeitet wird.

Phase 2: Domäne zu sicherer Zugriffsumgehungsliste hinzufügen

Navigieren Sie zu Internet Settings > Bypass Secure Access (Interneteinstellungen > Sicheren Zugriff umgehen) im Cisco Secure Access Dashboard, und fügen Sie die problematische Domäne hinzu, um sowohl DNS- als auch SWG-Prüfungen zu umgehen:

`sbstransit.aereacommercial.com`

Schritt 3: Testen des Zugriffs über ein nicht unternehmenseigenes Netzwerk

Testen des Anwendungszugriffs aus einem Netzwerk, in dem der Datenverkehr nicht über die Secure Access SWG eingeht (Bereiche 151.186.x.x) Dies kann über ein privates Gerät erfolgen oder indem der SSE-Client vorübergehend deaktiviert wird.

Geben Sie die öffentliche IP-Adresse des Internet Service Providers an. Diese finden Sie unter:

<https://whatismyip.com>

Schritt 4: Koordination der IP-Zulassungslisten mit dem Anwendungsbesitzer

Geben Sie die identifizierte öffentliche ISP-IP-Adresse an den Anwendungseigentümer weiter, und fordern Sie an, dass diese IP auf der Anwendungsseite aufgeführt werden darf. So können Sie überprüfen, ob die Anwendung IP-basierte Einschränkungen implementiert, die sich auf die Ausgangs-IPs der SWG für sicheren Zugriff auswirken.

Schritt 5: Auflösung überprüfen

Nachdem der Anwendungseigentümer die IP-Zulassungsliste implementiert hat, testen Sie das Zugriffsverhalten, um sicherzustellen, dass Benutzer erfolgreich auf die Anwendung zugreifen können, ohne dass HTTP 429- oder Verbindungsfehler auftreten.

Ursache

Die Anwendung scheint eine Durchsatzratenbegrenzung oder Zugriffsbeschränkungen basierend auf Quell-IP-Adressen zu implementieren. Wenn mehrere Benutzer über die Cisco Secure Access SWG auf die Anwendung zugreifen, scheint der gesamte Datenverkehr aus gemeinsam genutzten SWG-Ausgangs-IP-Bereichen (151.186.x.x) zu stammen. Dadurch wird der Mechanismus zur Ratenbegrenzung der Anwendung ausgelöst, da übermäßige Anforderungen von einer einzelnen IP-Adresse oder einem IP-Bereich erkannt werden.

Das Problem wird noch dadurch verschärft, dass vom Unternehmen verwaltete Geräte den Datenverkehr auch dann über den SSE-Client weiterleiten, wenn sie mit persönlichen Netzwerken verbunden sind. Dabei wird dasselbe IP-Ausgangsverhalten beibehalten, das die

Einschränkungen der Anwendung auslöst.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.