

HTTP 429 Rate Limit and Connection Errors When Accessing Applications Through Secure Access SWG

Contents

Issue

Users encounter HTTP 429 rate limit errors when attempting to access the application for example <https://xxxx.com> through Cisco Secure Access SWG (Secure Web Gateway). The issue affects corporate-managed laptops and began approximately two weeks prior to the case opening. Users experience these errors during login attempts or when accessing certain application functions after successful authentication.

Additionally, when the domain is added to the Secure Access bypass list, users encounter HTTP 500 server errors during OTP (One-Time Password) entry, or general connection errors when traffic no longer egresses through the SWG IP ranges (151.186.x.x).

The application owner confirmed that no rate limits were changed recently on the server side, and the issue appears to be related to traffic originating from Cisco Secure Access SWG egress IP addresses.

Environment

- Cisco Secure Access (formerly Cisco Umbrella) with SWG enable
- Corporate-managed laptops with Cisco SSE (Security Service Edge) client
- SWG egress IP ranges: 151.186.x.x
- Data Centers: AWS Singapore (Asia Pacific 1) and AWS US West (Oregon)
- Application: <https://sbstransit.aereacommercial.com>

Resolution

The resolution involves implementing a bypass configuration and coordinating with the application owner to allowlist specific IP addresses.

Follow the next steps.

Step 1: Verify Current SWG Behavior

Check the current policy and egress IP information by accessing this URL from an affected device:

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

This shows the current SWG egress IP being used (typically 151.186.x.x range) and confirm the traffic is being processed through Secure Access SWG.

Step 2: Add Domain to Secure Access Bypass List

Navigate to **Internet Settings > Bypass Secure Access** in the Cisco Secure Access dashboard and add the problematic domain to bypass both DNS and SWG inspection:

`sbstransit.aereacommercial.com`

Step 3: Test Access from Non-Corporate Network

Test application access from a network where traffic does not egress via Secure Access SWG (151.186.x.x ranges). This can be done from a personal device or by temporarily disabling the SSE client.

Identify the public ISP IP address by visiting:

`https://whatismyip.com`

Step 4: Coordinate IP Allowlisting with Application Owner

Provide the identified public ISP IP address to the application owner and request that this IP be allowlisted on the application side. This helps verify whether the application is implementing IP-based restrictions that affect Secure Access SWG egress IPs.

Step 5: Verify Resolution

After the application owner implements the IP allowlisting, test access behavior to confirm that users can successfully access the application without encountering HTTP 429 or connection errors.

Cause

The application appears to implement rate limiting or access restrictions based on source IP addresses. When multiple users access the application through Cisco Secure Access SWG, all traffic appears to originate from shared SWG egress IP ranges (151.186.x.x). This causes the rate limiting mechanism of the application to trigger, as it perceives excessive requests coming from a single IP address or IP range.

The issue is compounded by the fact that corporate-managed devices continue to route traffic through the SSE client even when connected to personal networks, maintaining the same egress IP behavior that triggers the restrictions of the application.

Related Content

- [Cisco Technical Support & Downloads](#)