

Límite de velocidad HTTP 429 y errores de conexión al acceder a las aplicaciones a través de SWG de acceso seguro

Contenido

Problema

Los usuarios se enfrentan a errores de límite de velocidad HTTP 429 al intentar acceder a la aplicación, por ejemplo, <https://xxxx.com> a través de Cisco Secure Access SWG (Secure Web Gateway). El problema afecta a los portátiles gestionados por la empresa y comenzó aproximadamente dos semanas antes de la apertura del caso. Los usuarios experimentan estos errores durante los intentos de inicio de sesión o cuando acceden a determinadas funciones de la aplicación después de una autenticación correcta.

Además, cuando el dominio se agrega a la lista de desvío de acceso seguro, los usuarios se encuentran con errores de servidor HTTP 500 durante la entrada OTP (contraseña de un solo uso) o errores de conexión generales cuando el tráfico ya no egresa a través de los rangos de IP SWG (151.186.x.x).

El propietario de la aplicación confirmó que no se han cambiado límites de velocidad recientemente en el lado del servidor, y el problema parece estar relacionado con el tráfico que se origina en las direcciones IP de salida de Cisco Secure Access SWG.

Entorno

- Cisco Secure Access (anteriormente Cisco Umbrella) con SWG activado
- Portátiles gestionados por la empresa con el cliente Cisco SSE (Security Service Edge)
- Intervalos IP de salida SWG: 151.186.x.x
- Data Centers: AWS Singapur (Asia Pacífico 1) y AWS US West (Oregón)

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

Resolución

La resolución implica la implementación de una configuración de omisión y la coordinación con el propietario de la aplicación para permitir la lista de direcciones IP específicas.

Siga los pasos siguientes.

Paso 1: Verificar el Comportamiento Actual de SWG

Verifique la política actual y la información de IP de salida accediendo a esta URL desde un dispositivo afectado:

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

Muestra la IP de salida de SWG actual que se está utilizando (normalmente, un intervalo de 151.186.x.x) y confirma que el tráfico se está procesando a través de SWG de acceso seguro.

Paso 2: Agregar dominio a lista de omisión de acceso seguro

Navegue hasta Internet Settings > Bypass Secure Access en el panel de Cisco Secure Access y agregue el dominio problemático para saltar la inspección de DNS y SWG:

`sbstransit.aereacommercial.com`

Paso 3: Probar el acceso desde una red no corporativa

Pruebe el acceso a las aplicaciones desde una red en la que el tráfico no egresa a través de SWG de acceso seguro (intervalos de 151.186.x.x). Esto se puede hacer desde un dispositivo personal o inhabilitando temporalmente el cliente SSE.

Identifique la dirección IP del ISP público visitando:

<https://whatismyip.com>

Paso 4: Coordine la lista de permisos de IP con el propietario de aplicación

Proporcione la dirección IP del ISP público identificada al propietario de la aplicación y solicite que se permita esta IP en la lista del lado de la aplicación. Esto ayuda a verificar si la aplicación está implementando restricciones basadas en IP que afectan a las IP de salida del SWG de acceso seguro.

Paso 5: Verificar resolución

Después de que el propietario de la aplicación implemente la lista de IP permitidos, pruebe el comportamiento de acceso para confirmar que los usuarios pueden acceder correctamente a la aplicación sin encontrar errores de conexión o HTTP 429.

Causa

La aplicación parece implementar límites de velocidad o restricciones de acceso basadas en direcciones IP de origen. Cuando varios usuarios acceden a la aplicación a través de Cisco Secure Access SWG, parece que todo el tráfico se origina a partir de intervalos de IP de salida SWG compartidos (151.186.x.x). Esto hace que se active el mecanismo de limitación de velocidad de la aplicación, ya que percibe solicitudes excesivas que provienen de una sola dirección IP o intervalo IP.

El problema se agrava por el hecho de que los dispositivos administrados por la empresa continúan enrutando el tráfico a través del cliente SSE incluso cuando están conectados a redes personales, manteniendo el mismo comportamiento IP de salida que activa las restricciones de la

aplicación.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).