

HTTP 429 Limite de débit et erreurs de connexion lors de l'accès aux applications via Secure Access SWG

Table des matières

Problème

Les utilisateurs rencontrent des erreurs de limite de débit HTTP 429 lorsqu'ils tentent d'accéder à l'application, par exemple <https://xxxx.com> via Cisco Secure Access SWG (Secure Web Gateway). Le problème concerne les ordinateurs portables gérés par l'entreprise et a commencé environ deux semaines avant l'ouverture du dossier. Les utilisateurs rencontrent ces erreurs lors des tentatives de connexion ou lors de l'accès à certaines fonctions de l'application après une authentification réussie.

En outre, lorsque le domaine est ajouté à la liste de contournement d'accès sécurisé, les utilisateurs rencontrent des erreurs de serveur HTTP 500 lors de l'entrée OTP (One-Time Password) ou des erreurs de connexion générales lorsque le trafic ne sort plus des plages IP SWG (151.186.x.x).

Le propriétaire de l'application a confirmé qu'aucune limite de débit n'a été modifiée récemment du côté du serveur, et le problème semble être lié au trafic provenant des adresses IP de sortie SWG d'accès sécurisé Cisco.

Environnement

- Cisco Secure Access (anciennement Cisco Umbrella) avec SWG activé
- Ordinateurs portables gérés par l'entreprise avec client Cisco SSE (Security Service Edge)
- Plages IP de sortie SWG : 151.186.x.x
- Centres de données : AWS Singapour (Asie Pacifique 1) et AWS US West (Oregon)

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

Résolution

La résolution implique la mise en oeuvre d'une configuration de contournement et la coordination avec le propriétaire de l'application pour autoriser la liste des adresses IP spécifiques.

Suivez les étapes suivantes.

Étape 1: Vérification du comportement SWG actuel

Vérifiez la stratégie actuelle et les informations IP de sortie en accédant à cette URL à partir d'un périphérique affecté :

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

Affiche l'adresse IP de sortie SWG en cours d'utilisation (généralement la plage 151.186.x.x) et confirme que le trafic est traité via Secure Access SWG.

Étape 2: Ajouter un domaine à la liste de contournement d'accès sécurisé

Accédez à Internet Settings > Bypass Secure Access dans le tableau de bord Cisco Secure Access et ajoutez le domaine problématique pour contourner l'inspection DNS et SWG :

`sbstransit.aereacommercial.com`

Étape 3: Tester l'accès à partir d'un réseau externe

Testez l'accès aux applications à partir d'un réseau où le trafic ne sort pas via Secure Access SWG (plages 151.186.x.x). Vous pouvez le faire à partir d'un périphérique personnel ou en désactivant temporairement le client SSE.

Identifiez l'adresse IP publique du FAI en visitant :

<https://whatismyip.com>

Étape 4: Coordonner la liste IP autorisée avec le propriétaire de l'application

Fournissez l'adresse IP publique du FAI identifiée au propriétaire de l'application et demandez que cette adresse IP soit autorisée du côté de l'application. Cela permet de vérifier si l'application met en oeuvre des restrictions IP qui affectent les adresses IP de sortie SWG d'accès sécurisé.

Étape 5: Vérifier la résolution

Une fois que le propriétaire de l'application a implémenté la liste d'autorisation IP, testez le comportement d'accès pour confirmer que les utilisateurs peuvent accéder à l'application sans rencontrer d'erreurs HTTP 429 ou de connexion.

Motif

L'application semble mettre en oeuvre une limitation de débit ou des restrictions d'accès en fonction des adresses IP source. Lorsque plusieurs utilisateurs accèdent à l'application via Cisco Secure Access SWG, tout le trafic semble provenir des plages IP de sortie partagées SWG (151.186.x.x). Le mécanisme de limitation du débit de l'application se déclenche, car il perçoit des requêtes excessives provenant d'une adresse IP ou d'une plage IP unique.

Le problème est aggravé par le fait que les périphériques gérés par l'entreprise continuent à acheminer le trafic via le client SSE même lorsqu'ils sont connectés à des réseaux personnels, conservant le même comportement IP de sortie qui déclenche les restrictions de l'application.

Autres informations utiles

- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.