

Accès aux sites Web géolimités bloqués par le pare-feu d'application Web lors de l'utilisation des adresses IP de sortie NATaaS SSE

Table des matières

Problème

Les tentatives d'accès à un site Web spécifique via Cisco Secure Access (SSE) entraînent l'affichage d'un message de blocage indiquant « désolé d'avoir été bloqué ».

Le site est accessible lorsque vous utilisez une connexion Wi-Fi domestique normale. La cause suspectée est que le site Web distant autorise uniquement l'accès à partir de plages d'adresses IP spécifiques, tandis que l'adresse IP de sortie SSE semble être en dehors de la plage autorisée.

L'enquête technique montre que le pare-feu d'application Web du site Web (Cloudflare) bloque l'ensemble de la plage d'adresses IP de sortie NATaaS d'accès sécurisé, quel que soit le pays. Le problème est reproductible et se produit de manière constante lors de l'utilisation d'adresses IP de sortie SSE.

Environnement

- Technologie : Cisco Secure Access (SSE) avec politique unifiée (politiques Internet, politiques privées, politiques DLP, RBI, profils de sécurité)
- Chemin d'accès : tout data center de SSE
- Sites Web géographiquement limités
- Contrôle de sécurité : pare-feu d'application Web (Cloudflare) sur le site Web de destination
- Accès Internet à partir d'un réseau distant (IP de sortie SSE) par rapport à un réseau local (Wi-Fi domestique)
- Aucune modification apportée au déploiement de l'accès sécurisé au moment du problème
- Message d'erreur observé : "désolé, vous avez été bloqué"

Résolution

Pour résoudre les problèmes d'accès causés par le blocage des adresses IP de sortie Cisco Secure Access NATaaS par les sites distants, ce workflow est recommandé. Ces étapes garantissent une approche méthodique pour identifier la nature du blocage et explorer les solutions de contournement ou de résolution potentielles.

Étape 1 : Confirmer le message d'erreur et bloquer le comportement

Observez ce message lors de l'accès au site via SSE :

sorry you have been blocked

Étape 2 : Valider l'accessibilité du site Web à partir de différents réseaux

Accédez au site Web à partir de :

- Tout data center SSE (bloqué)
- Une connexion Wi-Fi à domicile (accessible)

Étape 3 : Identifiez le contrôle de sécurité responsable du blocage

Observation technique : le pare-feu d'application Web (WAF) Cloudflare bloque l'ensemble de la plage IP de sortie NATaaS d'accès sécurisé.

Étape 4 : Confirmez le chemin d'accès utilisé par les utilisateurs finaux

Déterminez la méthode utilisée pour envoyer le trafic vers l'accès sécurisé :

- module de sécurité en itinérance
- Tunnel RAVPN
- Tunnel VPN de site à site
- déploiement PAC

Étape 5 : Explorez les options de contournement ou d'autorisation de référencement

Vérifiez si l'une de ces options est possible :

- Relation commerciale ou contact avec les administrateurs du site Web de destination pour demander l'autorisation de listage des adresses IP de sortie SSE.
- Les adresses IP de sortie SSE sont répertoriées dans le document :
- D'autres chemins d'accès qui peuvent utiliser différentes adresses IP de sortie non bloquées par le WAF.
- Contourner le site Web problématique du proxy SSE (les étapes exactes dépendent de la méthode utilisée pour envoyer le trafic vers Secure Access)

Étape 6 : Documentation des observations et des étapes suivantes

Documentez ces observations :

Le message d'erreur

Le chemin d'accès et les résultats correspondants

Communications avec l'administrateur du site distant si la liste est autorisée.

Motif

La cause principale de ce problème est que le pare-feu d'application Web (Cloudflare) du site de destination bloque activement la plage d'adresses IP de sortie NATaaS de Cisco Secure Access (SSE). Ce blocage n'est pas limité aux adresses IP non israéliennes ou au filtrage de géolocalisation. Il cible plutôt l'ensemble de la plage d'adresses IP de sortie connue associée à Cisco Secure Access, probablement en raison d'une stratégie ou d'une configuration de sécurité sur le site Web distant. Par conséquent, tout trafic provenant de ces adresses IP est refusé, quel que soit son pays source réel ou l'emplacement de l'utilisateur final.

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.