FAQ Cisco Umbrella concernant le géoblocage basé sur IP

Table des matières

Introduction

Ce document décrit les changements de comportement présentés aux clients de Cisco Umbrella et d'OpenDNS en Russie et au Belarus à partir du 1er août. Ces changements de comportement s'appliquent également à d'autres régions pour lesquelles Cisco Umbrella met en oeuvre un blocage géographique basé sur IP. Dernière mise à jour du présent document : le 28 juillet 2022.

Clients DNS :

- Le service DNS pour les requêtes provenant d'adresses IP identifiées comme provenant de Russie, Biélorussie, Crimée, Lougansk, Donetsk, Syrie, Cuba, Iran, Corée du Nord et d'autres régions sanctionnées avec géoblocage ne doit pas avoir de politiques de sécurité ou de filtrage de contenu appliquées. Les requêtes DNS reçoivent toujours une réponse valide et sont traitées avec le même niveau de service que le trafic provenant du reste du monde.
- Lorsqu'ils sont utilisés pour le DNS, les modules de sécurité d'itinérance Umbrella et AnyConnect Umbrella continuent de résoudre le trafic DNS.
- La synchronisation des clients itinérants et les listes de domaines internes peuvent continuer à se synchroniser avec le tableau de bord et fournir le comportement attendu (envoi de domaines internes au serveur DNS interne). Cela peut changer à l'avenir.

Clients SIG :

- Les serveurs de passerelle Web sécurisés Umbrella n'acceptent pas le trafic dont l'adresse IP d'origine provient de Russie, Biélorussie, Crimée, Louhansk, Donetsk, Syrie, Cuba, Iran, Corée du Nord et d'autres régions sanctionnées avec blocage géographique. La façon dont cette solution est mise en oeuvre fait que les connexions provenant de ces régions voient les serveurs Cisco Umbrella comme étant hors ligne ou indisponibles. Le trafic n'est pas accepté ou traité.
- La configuration par défaut du module AnyConnect Umbrella l'amène à se connecter

directement à Internet lorsque Umbrella n'est pas disponible. Certaines configurations client spécifiques peuvent fonctionner en mode « fail closed », ce qui entraînerait la perte de l'accès à Internet pour les utilisateurs.
- La liste des domaines externes continue de se synchroniser, pour l'instant, pour obtenir des mises à jour d'Umbrella. Cela peut changer à l'avenir.
- Le fichier PAC Umbrella par défaut le connecte directement à Internet lorsque Umbrella n'est pas disponible. Certaines configurations client spécifiques (par exemple, celles sans route par défaut) peuvent être fermées en cas d'échec, ce qui entraîne la perte de l'accès à Internet pour les utilisateurs.
- Les tunnels IPsec sont déconnectés par blocage IP ou révocation des informations d'identification IKE. Le comportement et l'expérience utilisateur dépendent de la configuration spécifique du client. Certaines configurations peuvent revenir à une connexion Internet directe, d'autres peuvent revenir à MPLS et d'autres peuvent entraîner la perte de l'accès à Internet par les utilisateurs.

Tous les clients :

- Une fois le blocage géographique basé sur IP entièrement mis en oeuvre pour un pays, l'accès au tableau de bord Umbrella et à l'API est également bloqué.

Que faire si mes utilisateurs dans les régions touchées se connectent à un VPN d'entreprise en dehors des régions touchées, qui se connecte à son tour à Umbrella ?

Notre blocage géographique est basé sur IP, basé sur l'adresse IP source vue par le service Umbrella.

Pourquoi Cisco fait-il cela ?

Visitez The War in Ukraine : Soutenir nos clients, partenaires et communautés pour plus d'informations.

Que se passe-t-il si mes utilisateurs sont bloqués mais qu'ils ne se trouvent pas dans l'une des régions affectées ?

Veuillez contacter le support technique pour obtenir une enquête sur le document émis.

Dans quelle mesure vos données de blocage géographique sont-elles précises ?

Nous utilisons des services de géolocalisation de pointe pour déterminer le pays d'une adresse IP donnée.

Que dois-je faire si l'emplacement associé à mon adresse IP est incorrect ?

Nous vous recommandons de soumettre une demande de correction à ces services :

- https://www.maxmind.com/en/geoip-location-correction (service principal utilisé pour Umbrella)
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/contact/
- http://www.ipligence.com/contact/

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.