Conformité à l'exportation et restrictions géographiques pour Cisco Secure Access

Table des matières

Introduction

Ce document décrit comment exporter la conformité et les restrictions géographiques pour un accès sécurisé Cisco.

Informations générales

Conformément à la politique générale de conformité à l'exportation de Cisco et en réponse à la guerre contre l'Ukraine, Cisco restreint l'achat, le déploiement et l'accès à Secure Access depuis plusieurs pays et régions, y compris la Russie, la Biélorussie, la Crimée, Lougansk, Donetsk, la Syrie, Cuba, l'Iran et la Corée du Nord.

DNS (Domain Name Server)

- 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 le blocage géographique n'a pas de politiques de sécurité ou de filtrage de contenu appliquées. Les rapports sont également désactivés. 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'il est utilisé pour DNS, le module de sécurité d'itinérance Secure Client continue de résoudre le trafic DNS.

Sécurité Web

- Les serveurs de sécurité Web n'acceptent pas le trafic dont l'adresse IP d'origine provient de l'un des pays ou régions bloqués.
- La configuration par défaut du module de sécurité d'itinérance du client sécurisé le fait se

connecter directement à Internet lorsque l'accès sécurisé n'est pas disponible. Certaines configurations client spécifiques fonctionnent en mode « fail closed », ce qui peut entraîner la perte de l'accès à Internet pour les utilisateurs.
- Le fichier par défaut d'informations d'identification d'accès protégé (PAC) l'oblige à se connecter directement à Internet lorsque l'accès sécurisé 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 (Internet Key Exchange). Le comportement et l'expérience utilisateur dépendent de la configuration spécifique du client. Certaines configurations rétablissent une connexion Internet directe, d'autres rétablissent la commutation multiprotocole par étiquette (MPLS) et d'autres encore peuvent entraîner la perte de l'accès à Internet.

Accès administrateur et tableau de bord

Le tableau de bord et les API d'accès sécurisé sont bloqués pour les utilisateurs se connectant à partir de l'une des régions répertoriées.

FAQ

1. Que faire si les utilisateurs sont bloqués, mais qu'ils ne se trouvent pas dans l'une des régions affectées ?
   Contactez l'assistance et ils sont heureux de vous renseigner.

2. Dans quelle mesure vos données de blocage géographique sont-elles précises ?
   Des services de géolocalisation de pointe sont utilisés afin de déterminer le pays pour une adresse IP donnée.

3. Que faut-il faire si l’emplacement associé à l’adresse IP est incorrect ?
   Il est recommandé de soumettre une demande de correction à ces services :

- https://www.maxmind.com/en/geoip-location-correction
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/
- http://www.ipligence.com/

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.