# Échec de la connexion du client VPN Azure avec la sécurité Web d'accès sécurisé activée

## Table des matières

## Problème

Après la migration d'Umbrella vers SSE et l'activation de Web Security avec une licence SIA nouvellement attribuée, les connexions du client VPN Azure ne parviennent pas à établir pour les utilisateurs lorsque Web Security est activé. Le problème de connectivité du client VPN Azure affecte tous les clients, les empêchant de se connecter au VPN. Lorsque le client d'accès sécurisé Cisco est désinstallé des ordinateurs clients, la connectivité VPN est restaurée, indiquant que le client d'accès sécurisé bloque la connexion aux services VPN Azure.

La désactivation de la sécurité Web ou la désinstallation de Cisco Secure Access Client restaure la connectivité VPN, mais cela a un impact sur l'accès des utilisateurs aux ressources sur le VPN Azure lorsque la protection de la sécurité Web est nécessaire.

## Environnement

- Cisco Secure Access (anciennement SIA) avec Web Security activé
- Client VPN Azure
- Migration de Umbrella vers SSE terminée
- Licence SIA nouvellement attribuée

## Résolution

La résolution implique l'ajout de l'adresse IP publique de la passerelle VPN Azure à la liste d'exceptions SSE/SWG pour empêcher l'interception du trafic qui bloque les connexions VPN.

### Étape 1: Identifier l'adresse IP de la passerelle VPN Azure

Déterminez l'adresse IP publique de la passerelle VPN Azure.

### Étape 2: Ajouter une exception basée sur IP à SSE/SWG

1.- Ajoutez l'adresse IP publique de la passerelle virtuelle Azure à la liste d'exceptions SSE/SWG dans l'environnement Cisco Secure Access.

2.- Connectez-vous à Cisco Secure Access Dashboard - Cliquez sur Connect - End user Connectivity - Internet Security - Ajouter une exception. Cela empêche la passerelle Web sécurisée d'intercepter et d'inspecter le trafic destiné à la passerelle VPN Azure.

### Étape 3: Tester la connectivité VPN

Après avoir appliqué l'exception basée sur IP, testez la connexion VPN Azure pour vérifier que les clients peuvent établir des connexions VPN avec la sécurité Web activée.

### Étape 4: Développer les tests

Étendez le test de l'exception basée sur IP à d'autres utilisateurs dans l'environnement afin de garantir une fonctionnalité cohérente avant de considérer la résolution comme terminée.

## Motif

Le problème se produit parce que le mécanisme d'exception Secure Web Gateway (SWG) nécessite une recherche DNS pour un domaine afin de créer une entrée de cache de domaine à IP. Lorsque le client VPN Azure se connecte directement à l'adresse IP sans effectuer de requête DNS pour l'URL VPN, le module SWG ne peut pas mapper le domaine à l'adresse IP. Par conséquent, le SWG continue d'inspecter et d'intercepter le trafic vers l'adresse IP, empêchant

ainsi l'établissement de la connexion VPN.

L'analyse de capture de paquets n'a montré aucune requête DNS pour l'URL VPN et aucun trafic d'interception SWG visible pour l'adresse IP de la passerelle Azure, confirmant que le SWG bloquait la connexion en raison de l'absence de mappage domaine-adresse IP correct dans son cache.

## 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.