

Dépannage de la compatibilité entre Netskope et Umbrella Roaming Client

Table des matières

[Introduction](#)

[Aperçu](#)

[Incidence](#)

[Résolution : Ignorer le client d'itinérance du proxy](#)

Introduction

Ce document décrit comment dépanner les problèmes de compatibilité entre Netskope et le client d'itinérance Umbrella.

Aperçu

Ce KBA est destiné aux utilisateurs du proxy Netskope qui rencontrent un problème de synchronisation du client d'itinérance avec le tableau de bord Umbrella. Le client d'itinérance ne s'active donc pas correctement sur le réseau. Cet article explique comment exclure nos synchronisations du proxy Netskope.

Ces informations s'appliquent aux clients itinérants sur Windows et MacOS.

Incidence

Lorsque SSL est tunnalisé via le proxy Netskope, dirigeant le trafic SSL vers les serveurs Netskope, le client d'itinérance ne peut pas se synchroniser correctement avec Umbrella. Il reste donc dans un état non protégé et non chiffré. Dans certains cas, le client peut être chiffré avant la première synchronisation, ce qui entraîne un problème connu entraînant l'échec de la résolution des domaines internes (qui ne figurent pas dans la liste de suffixes de recherche DNS locale).

Plusieurs applications natives se comportent avec Netskope comme si elles étaient épinglées à des certificats, ce qui entraîne l'acceptation de certificats tiers. Cette épinglage se produit en raison de l'infrastructure de chiffrement .NET utilisée par le client d'itinérance.

Résolution : Ignorer le client d'itinérance du proxy

La solution consiste à empêcher le processus de service du client d'itinérance d'être dirigé via le proxy de Netskope via sa fonctionnalité « Applications épinglées par certificat ».

Les applications, si elles sont définies, permettent de bloquer ou de contourner une application. Si vous sélectionnez Contourner (requis pour la synchronisation des clients en itinérance), le client

Netskope n'oriente pas le trafic du point d'extrémité vers le proxy Netskope dans le cloud et les applications continuent à fonctionner. Si vous sélectionnez Bloquer, le trafic est bloqué par le client Netskope. Par défaut, toutes les applications sont contournées, mais le paramètre requis est de contourner le service du client d'itinérance.

Pour modifier les applications de certificat épinglées et ajouter le service client d'itinérance Umbrella, procédez comme suit :

1. Accédez à Paramètres > Gérer > Applications épinglées par certificat > Paramètres avancés. La fenêtre Advanced Settings s'affiche.
2. Dans la fenêtre Advanced Settings, sélectionnez Custom Settings for Each Application. Utilisez ces sous-étapes pour ajouter un service/une application personnalisée
 - Dans la liste Application, sélectionnez Microsoft Office 365 Outlook.com (il n'y a pas d'option Umbrella, cela nous permet d'avancer) et pour Action, sélectionnez Contourner.
 - Pour Mode, sélectionnez Direct.
 - Dans le champ Plugin Process, saisissez « ercservice.exe » pour le client d'itinérance autonome. Pour le module d'itinérance AnyConnect, entrez « acumbrellaplugin.exe ».
3. Cliquez sur Submit. La fenêtre Paramètres avancés se ferme.
4. Sur l'ordinateur client, redémarrez l'agent Netskope pour extraire immédiatement ces nouveaux paramètres. (Normalement, le client effectue les mises à jour dans l'heure qui suit, lorsqu'il contacte Netskope pour obtenir des mises à jour.)

Les paramètres avancés existent. Chacun de ces scénarios est considéré comme efficace ; Toutefois, il est recommandé de contourner + direct.

1. Contournement + Direct : Si vous sélectionnez cette option, ignorez les applications/domaines configurés du client. Il ne se rend pas à Netskope.
2. Contournement + tunnel : Si vous sélectionnez cette option, le client effectue un tunnel entre le trafic des applications/domaines, mais le proxy Netskope le contourne. Cette option est utile pour les domaines associés à un service d'authentification SSO, car ces services utilisent l'adresse IP source du cloud Netskope pour déterminer si l'accès à l'application cloud est protégé par Netskope.

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.