

Dépannage de l'API VPN native de Windows 10 (applications modernes/Metro)

Table des matières

[Introduction](#)

[Incidence](#)

[Cause première](#)

[Résolution](#)

Introduction

Ce document décrit l'utilisation des applications VPN construites sur la [plate-forme universelle Windows](#) (UWP) de [Microsoft](#). Ces applications apparaissent généralement sous la forme d'applications dans l'interface Metro/Modern de Windows 8 ou version ultérieure. Les applications de bureau et les programmes Windows traditionnels n'utilisent pas le UWP et ne sont pas affectés.

Si vous rencontrez des problèmes avec le VPN Windows de style non-App ou toujours sur VPN, consultez notre remarque sur le VPN Windows sur Umbrella Roaming Client : Guide de compatibilité des logiciels et des VPN .

Le module d'itinérance AnyConnect Umbrella n'entraîne pas le même problème d'interopérabilité.

Incidence

Lorsque le client d'itinérance est actif, les utilisateurs de l'application VPN UWP reçoivent un message d'erreur « No such host is known » ou similaire lorsqu'ils tentent d'initier une session VPN. Cela empêche l'utilisateur de se connecter correctement au VPN. Cette erreur n'apparaît pas si le client en itinérance est arrêté ou si l'édition de bureau du client VPN est utilisée.

Par exemple, ceux-ci ne fonctionnent pas :

- Application Pulse Secure + client itinérant
- SonicWall MobileConnect + client itinérant

Pour ceux-ci, la connexion à la même tête de réseau VPN fonctionne :

- Application de bureau Pulse Secure + client itinérant
- Application SonicWall NetExtender ou SonicWall Desktop + client itinérant
- Application Pulse Secure + module d'itinérance AnyConnect Umbrella*
- Module d'itinérance SonicWall MobileConnect + AnyConnect Umbrella*

*Le module AnyConnect Umbrella ne définit pas 127.0.0.1 (une autre interface) comme paramètre

DNS, mais redirige le DNS vers 127.0.0.1 à l'aide d'un pilote de noyau. Les applications UWP ne savent pas qu'elles utilisent un adaptateur différent pour DNS et ne sont pas affectées pour le moment.

Cause première

Par conception, Microsoft a construit des applications "modernes" dans Windows 8+ pour être plus sandboxed. L'une de ces limitations s'applique aux applications VPN. Les VPN construits sur le UWP (applications) sont limités à l'utilisation de l'interface générant la requête. Puisque le client d'itinérance Umbrella écoute sur 127.0.0.1 - une interface I/O différente - la requête n'atteint donc jamais le client d'itinérance (ou tout autre transfert DNS exécuté sur 127.0.0.1).

L'appel suivant permet de limiter la création d'un socket à une seule interface. C'est le cas pour les applications VPN UWP connues qui contraignent DNS à leur interface :

`ConnectAsync(HostName, String, SocketProtectionLevel, NetworkAdapter)`

«Le mécanisme de résolution de noms utilisé par la méthode `ConnectAsync(Hostname, String, SocketProtectionLevel, NetworkAdapter)` est limité à l'interface spécifiée pour l'espace de noms DNS (Domain Name System).» <https://learn.microsoft.com/en-us/uwp/api/windows.networking.sockets.streamsocket>

On pense que l'API VPN Windows utilise ce mécanisme de connexion ou un mécanisme similaire, ce qui a pour conséquence que les VPN de type « app » UWP ne fonctionnent pas avec le client d'itinérance en raison de l'utilisation de 127.0.0.1 pour DNS. Par conséquent, les connexions VPN échouent lorsque le DNS est envoyé à 127.0.0.1 ; toutefois, en raison des limitations de l'appel, le client itinérant ne le reçoit ni ne répond. Par conséquent, la connexion VPN échoue en raison d'une défaillance DNS.

La cause première est similaire dans son origine à une limitation de conception à l'indicateur de connectivité NCSI de Windows où 127.0.0.1 n'est jamais interrogé pour confirmer la connectivité DNS (résolue par Microsoft).

Résolution

Actuellement, pour le client d'itinérance autonome, il n'existe aucune mise à jour du client d'itinérance qui puisse modifier ce comportement Windows suite à la définition de 127.0.0.1 en tant que serveur DNS local. C'est un noyau la configuration requise pour le fonctionnement du client d'itinérance. Jusqu'à ce que Microsoft autorise l'utilisation de 127.0.0.1 pour DNS par une application VPN UWP, la seule option est de basculer vers l'édition de bureau du client VPN ou d'utiliser le module d'itinérance AnyConnect qui utilise un pilote de noyau pour diriger DNS.

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.