

Gestion des conflits entre Pulse Secure et Umbrella Roaming Client

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Déploiements non pris en charge de Pulse Secure](#)

[Pulse Windows 10 App style connexion.](#)

[Impulsion Sécurisée](#)

[Sécurisation des impulsions avec tunnel partagé basé sur FQDN avec Split-DNS](#)

Introduction

Ce document décrit comment gérer les conflits entre Pulse Secure et Umbrella Roaming Client.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Umbrella Roaming Client.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Si vous utilisez actuellement Pulse Secure comme client VPN et que vous cherchez à installer le client d'itinérance Umbrella, cet article est à lire absolument. Bien que certains utilisateurs aient signalé un succès limité dans l'obtention du client d'itinérance Cisco Umbrella pour fonctionner avec Pulse Secure VPN, il a de nombreuses incompatibilités et n'est pas pris en charge pour le moment.

Si vous rencontrez des problèmes de compatibilité avec le client Umbrella Roaming, la solution

prise en charge consiste à passer au module de sécurité AnyConnect Umbrella Roaming. Ce module est inclus dans votre abonnement Umbrella DNS à partir d'avril 2021. Le titulaire du compte principal peut accéder à ce logiciel à l'adresse software.cisco.com. Si vous ne savez pas quel compte a accès ou si vous rencontrez un problème d'accès, veuillez contacter votre gestionnaire de compte ou l'équipe d'assistance Umbrella à l'adresse umbrella-support@cisco.com pour contacter votre gestionnaire de compte en votre nom.

Déploiements non pris en charge de Pulse Secure

Pulse Secure est connu pour être en conflit avec le client d'itinérance Umbrella dans les deux scénarios suivants :

Pulse Windows 10 App style connexion.

- Incidence: Impulsion non connectée

Impulsion Sécurisée

- Incidence: Lors de la déconnexion, le DNS local enregistré peut rester sur les valeurs VPN ou 127.0.0.1 plutôt que sur les valeurs WiFi/Ethernet en raison de la modification d'impulsion pendant la connexion VPN. Cette modification est un conflit entre les modifications Umbrella et les modifications Pulse sur la carte réseau non VPN.
 - La connectivité utilisateur est interrompue après la déconnexion jusqu'au renouvellement du bail DHCP.
- Solution :
 - Passez au module de sécurité d'itinérance Umbrella dans AnyConnect. (VPN AnyConnect non requis. La licence AnyConnect pour utilisation Umbrella est incluse dans votre package DNS ou peut être fournie pour résoudre ce conflit connu.)

Sécurisation des impulsions avec tunnel partagé basé sur FQDN avec Split-DNS

- Incidence: Le module RSM CA ne passe pas en mode chiffré/protégé lorsqu'il est utilisé avec un VPN de tunnel partagé basé sur le FQDN par impulsions. La configuration VPN split-DNS ne fonctionne pas comme prévu et se comporte comme un DNS « tunnel-all ». Split-DNS pour Pulse VPN fonctionne correctement uniquement lorsque le RSM AC est désactivé.
- Solution :
 - Passage à un tunnel partagé basé sur IP pour la configuration VPN

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.