Comprendre les conflits de logiciels connus pour CSC

Table des matières

[Introduction](#)

[Quels sont les conflits logiciels connus pour Cisco Security Connector ?](#)

Introduction

Ce document décrit les conflits logiciels connus pour Cisco Security Connector (CSC).

Quels sont les conflits logiciels connus pour Cisco Security Connector ?

Le connecteur de sécurité Cisco (CSC) est connu pour ne pas fonctionner correctement en présence de certains logiciels et de certains scénarios.

Dans ces conditions, le CSC peut signaler Protected, mais le trafic Web n'applique pas la politique :

- VPN : Selon la conception d'Apple, le CSC ne peut pas recevoir de paquets DNS pour le trafic destiné à un VPN. C’est un comportement attendu.
- Hotspot mobile : Les clients connectés à un iPhone exécutant un point d'accès sans fil ne sont pas couverts par le CSC. Le téléphone qui gère le point d'accès peut continuer à être couvert.
- Wandera "Passerelle" : Apple reconnaît le proxy Wandera comme une passerelle de type VPN. Par conséquent, tout trafic envoyé via Wandera ne peut pas bénéficier de la couverture CSC. CSC peut voir de nombreuses requêtes DNS vers *.proxy.wandera.com comme un signe que Wandera est actif.

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.