Résoudre les modes client itinérant non protégés ou non chiffrés

Table des matières

Introduction

Ce document décrit la signification des états non protégés et non chiffrés dans le client d'itinérance Umbrella et comment les dépanner.

États non protégés et non chiffrés

Lorsque le client d'itinérance Umbrella est en mode non protégé ou non chiffré, l'icône de la barre d'état système (Windows) ou la barre de menus (OS X) affiche un état jaune. L'état est à la fois Non protégé et Non chiffré.

Exigences de communication

Pour assurer la sécurité et le filtrage du contenu, le client d'itinérance Umbrella doit communiquer avec Umbrella à l'aide des protocoles UDP et TCP sur les ports et les destinations fournis, en plus des destinations HTTP répertoriées dans l'article Conditions préalables du client d'itinérance :

Port	Protocol	IPv4	IPv6
53	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
53	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35

Le client d'itinérance Umbrella ne peut pas protéger l'ordinateur si les deux conditions suivantes sont réunies :

- L'ordinateur est derrière une connexion qui n'autorise pas les requêtes DNS tierces.
- L'ordinateur est derrière une connexion qui a une stratégie de pare-feu de refus de trafic sortant par défaut.

Lorsque ces conditions sont remplies, le client d’itinérance Umbrella restaure les serveurs DNS délégués DHCP sur les propriétés de connexion réseau et poursuit le test jusqu’à ce qu’il puisse contacter les serveurs DNS Umbrella et recommencer à assurer la sécurité et le filtrage du contenu. Pendant les périodes où la communication avec les serveurs DNS Umbrella n'est pas possible, l'application des stratégies et la création de rapports ne sont pas disponibles.

Test de la connectivité réseau

Pour vérifier si le réseau autorise la communication avec les serveurs DNS Umbrella, exécutez manuellement une requête DNS. Si le réseau bloque les requêtes, le résultat est le suivant :

```
$ nslookup opendns.com 208.67.222.222
;; connection timed out; no servers could be reached
```

Si le test réussit mais que le client Umbrella Roaming signale toujours « Unprotected/Unencryption », ouvrez un ticket d'assistance et fournissez les résultats d'un test de diagnostic. Une requête réussie s'affiche comme suit :

```
$ nslookup opendns.com 208.67.222.222
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: opendns.com
```

État non chiffré uniquement

Si le client d'itinérance Umbrella affiche Non crypté, il ne peut pas communiquer sur le port 443/UDP. Pour des raisons de sécurité, il est recommandé d'autoriser ce port à traverser votre pare-feu, mais le client continue de fonctionner sans requêtes DNS chiffrées. Pour plus de détails, référez-vous à l'article Conditions préalables du client d'itinérance.

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.