# Client VPN incapable de vérifier correctement l'erreur de modification de la table de transfert IP sur le ; Client sécurisé RAVPN Split-Tunnel/DNS par défaut

## Table des matières

## Problème

Les utilisateurs Mac rencontrent des échecs intermittents lors de la tentative d'authentification CLI sur des applications internes alors qu'ils sont connectés au VPN Cisco Secure Client. Les échecs se présentent sous la forme d'erreurs « host not found » pendant l'authentification CLI et lors de l'utilisation de commandes telles que `curl`. Cependant, les commandes de résolution DNS telles que `nslookup` et `dig` réussissent. Le problème se produit de manière aléatoire et peut être résolu temporairement en reconnectant le VPN, après quoi la connectivité fonctionne pendant une courte période avant que le problème ne se reproduise. Le VPN de tunnel partagé est utilisé et Cisco Umbrella est actif. Le problème ne se produit pas lors de l'utilisation du VPN Palo Alto GlobalProtect.

- Message d'erreur : « host not found » sur les commandes CLI authentication et `curl`.
- Message d'erreur : Le client VPN ne peut pas vérifier correctement les modifications de la table de transfert IP. Problème de résolution du serveur de noms de domaine (DNS) lors de la connexion des ressources privées
- `Les` commandes `nslookup` et `dig` aboutissent
- Connectivité intermittente après la reconnexion du VPN
- VPN d'accès à distance à tunnel partagé et module Umbrella activé
- Problème reproductible uniquement avec Cisco Secure Client VPN sur les périphériques MacOS

## Environnement

- Produit : Cisco Secure Client (CSC) avec plusieurs modules
- Plate-forme : périphériques Mac d'entreprise
- Configuration du profil VPN : Profil VPN d'accès à distance - Contourner l'accès sécurisé - Mode tunnel partagé et mode DNS sélectionné comme « DNS par défaut »
- Filtrage DNS : Cisco Umbrella activé
- Versions du module :
  - Gestion du cloud v1.0.0.23
  - VPN AnyConnect v5.1.13.17

    - Umbrella v5.1.13.177
    - DART v5.1.13.177
    - Posture du pare-feu sécurisé v5.1.13.17
    - Module de visibilité réseau v5.1.13.177
- Données de diagnostic : ensembles DART collectés pour analyse
- Observé uniquement sur Cisco Secure Client VPN (pas sur Palo Alto GlobalProtect)

# Résolution

- Lors du débogage de la configuration du tunnel partagé du profil VPN (`naic.org`) et de la table de routage VPN AnyConnect côté client, ce comportement a été observé :
    - Scénario fonctionnel : lors de l'exécution d'une `nslookup` pour les domaines locaux non prod du coffre-fort, les requêtes DNS traitées par les serveurs DNS configurés dans le profil VPN sont résolues correctement en adresses 10.x. De même, la table de routage a été mise à jour avec l'adresse IP résolue (par exemple, 10.59.130.193) sous des routes non sécurisées.
    - Scénario non fonctionnel : cependant, lorsque les mêmes requêtes DNS ont été traitées par le DNS local du système macOS (192.168.x.x) configuré sur une carte untun4 et en0 au lieu des serveurs DNS définis dans le profil VPN, ce comportement a été clairement observé à partir de la capture de paquets alors que le problème était détecté.
    - les domaines privés ont été résolus en plage IP de 34.x.x.x , ce qui a conduit au problème de connectivité. La capture Wireshark a aidé à identifier la cause sous-jacente du problème.
- Du point de vue de la conception et de la configuration, avec une configuration de profil VPN à tunnel partagé, il est recommandé d'utiliser le DNS partagé plutôt que de se fier au DNS du système local/DNS par défaut.
- En outre, l'entrée `us-east-eks-amazonaws.com` a été ajoutée pour garantir que le trafic de ce cluster EKS est correctement dirigé via l'interface du tunnel distant.
- Il a également été discuté que l'interface RAVPN doit avoir priorité sur le module Umbrella et ne doit pas entrer en conflit avec le fichier `OrgInfo.json` contenant l'ID d'organisation Umbrella.
- Au cours de notre processus de dépannage, nous avons fait une nouvelle installation du client CSC sans module Umbrella, avec ce scénario, nous n'avons pas pu voir le problème. J'ai pu examiner du point de vue Umbrella aussi bien, le domaine racine naic.org configuré dans la liste des domaines internes pour contourner Umbrella, ce qui signifie que les résolutions de domaine local sont transmises au système DNS configuré par macOS non intercepté par le module DNS Umbrella au niveau de l'interface de bouclage au niveau du noyau.

Cela correspond à la résolution des problèmes lorsqu'aucun module Umbrella n'est en place. Avec une configuration de profil VPN appropriée incluant les domaines corrects dans la règle de direction du trafic et la configuration DNS partagée, nous ne devrions pas voir le problème même avec le modèle Umbrella activé.

L'utilisateur a confirmé que le problème a été résolu après avoir modifié le mode DNS en tunnel

partagé et modifié la configuration du profil VPN.

## Motif

Profil VPN - Contourner l'accès sécurisé - Mode DNS supposé être défini sur Tunnel partagé (options les plus fréquemment vues dans des scénarios d'utilisation) et inclure tous les domaines d'application privés/internes dans la configuration DNS partagée pour résoudre le problème.

## Autres informations utiles

- Assistance technique de Cisco et téléchargements

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.