Gestion de la compatibilité entre Umbrella Roaming Client et VPN

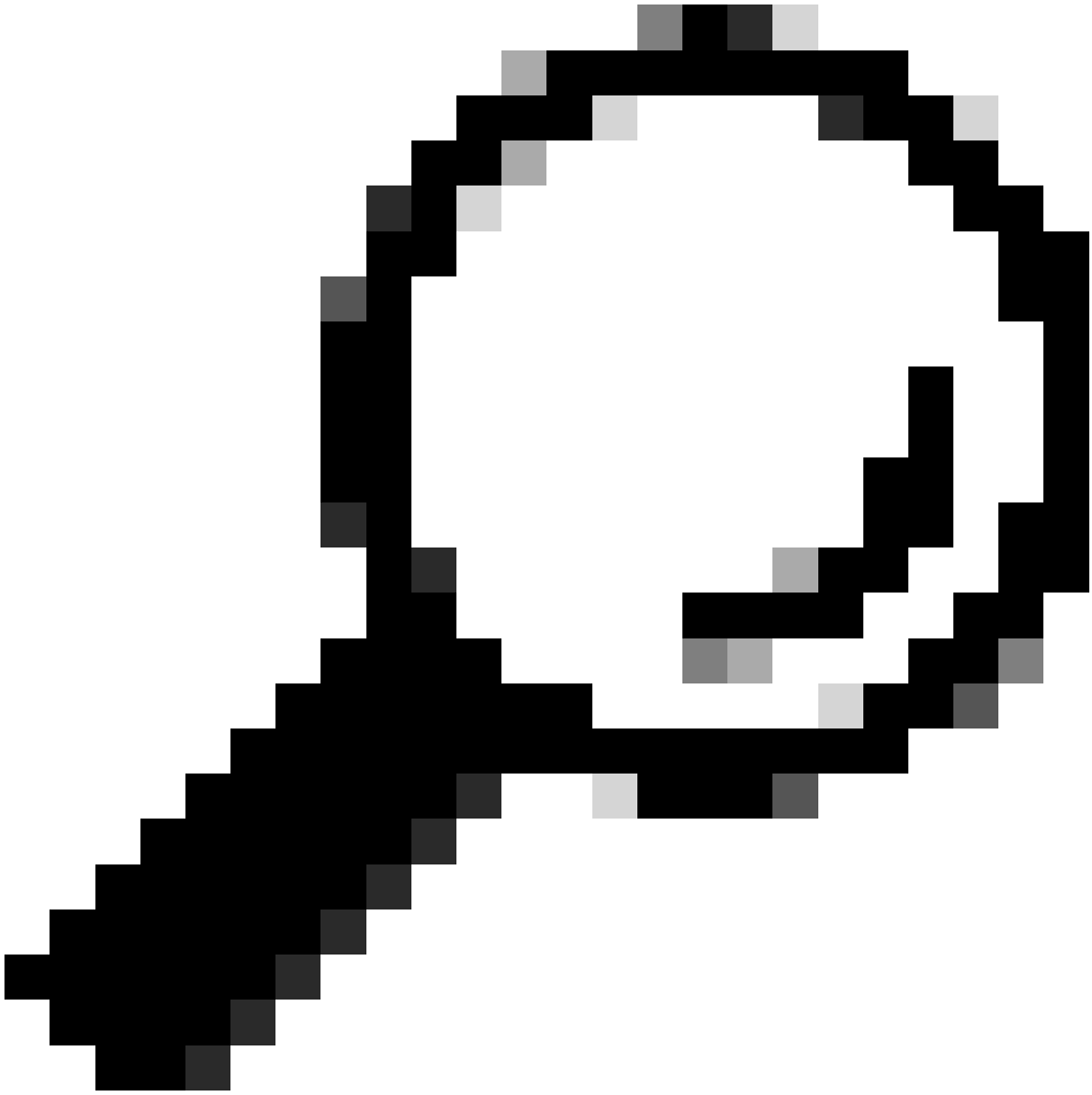
Table des matières

Introduction

Ce document décrit l'interaction et la compatibilité de Cisco Umbrella Roaming Client avec divers logiciels VPN.

Aperçu

Cisco Umbrella Roaming Client fonctionne avec la plupart des logiciels VPN, mais des étapes supplémentaires peuvent être nécessaires pour le fonctionnement attendu. Cisco Umbrella recommande de déployer le module Cisco Secure Client and Roaming Security pour une compatibilité maximale. Ce module peut être déployé sans les composants VPN.



Conseil : Le présent document constitue une orientation générale et ne constitue pas une liste officielle des logiciels pris en charge. Cisco Umbrella ne teste, ne valide ni ne certifie la fonctionnalité d'aucun logiciel ou client VPN tiers.

Ce document fournit des informations techniques et un contexte supplémentaire pour des clients VPN spécifiques qui peuvent nécessiter d'autres configurations. Pour une liste de logiciels VPN incompatibles connus, référez-vous à la section Incompatibilités du client d'itinérance Umbrella. L'incompatibilité DNS avec le client d'itinérance peut également entraîner l'échec du module Cisco Secure Client + Roaming Security avec SWG, car le client SWG dépend également de l'établissement réussi d'une connexion DNS.

Fonctionnement du client d'itinérance Umbrella avec les clients

VPN

Le client d’itinérance Umbrella se lie à toutes les cartes réseau et modifie les paramètres DNS de l’ordinateur en 127.0.0.1 (localhost). Cela permet au client d'itinérance Umbrella de transférer toutes les requêtes DNS directement à Umbrella tout en permettant la résolution des domaines locaux via la fonctionnalité Domaines internes. Lors de l'établissement d'une connexion à un serveur VPN, le client d'itinérance Umbrella détecte une nouvelle connexion réseau dans le système et modifie les paramètres DNS de connexion pour pointer vers le client d'itinérance Umbrella. Le client d’itinérance Umbrella s’appuie sur l’exécution de recherches DNS sur les adresses IP DNS Umbrella AnyCast (208.67.222.222/208.67.220.220).

Si un utilisateur se connecte à un VPN, le pare-feu associé au VPN doit autoriser l'accès à Umbrella.

Incompatibilités client d'itinérance Umbrella

Le client Umbrella Roaming assure actuellement l’application de la couche DNS. La couche DNS est la fonction principale du client d’itinérance, qui applique des stratégies de sécurité basées sur DNS sur n’importe quel réseau. Cette fonction du client d'itinérance peut présenter des incompatibilités logicielles connues. La couche DNS du client d’itinérance Umbrella est incompatible avec les clients répertoriés ci-dessous, selon les tests effectués par l’équipe de support. Cisco Umbrella Engineering ne vérifie ni ne teste ces clients, et toutes les entrées sont sujettes à examen. Cet article fait référence au client d'itinérance autonome Umbrella. Pour consulter un article complémentaire sur le module de sécurité d'itinérance Umbrella pour Cisco Secure Client (et les anciens systèmes), reportez-vous à la documentation appropriée.

Client VPN	Problème/Incompatibilité	Résolution
Impulsion Sécurisée	Lors de la déconnexion, le DNS local enregistré peut rester des valeurs VPN plutôt que des valeurs WiFi/Ethernet en raison de la modification d'impulsion pendant la connexion VPN.	Résolu avec le module Umbrella - inclus dans la plupart des licences.
VPN Avaya	Incompatible.	Résolu avec le module Umbrella - inclus dans la plupart des licences.
VPN Windows (notamment Always On VPN)	Peut entraîner l'échec de la résolution du DNS local vers la réponse interne, même si les noms d'hôte DNS figurent dans la liste des domaines internes.	Résolu avec le module Umbrella - inclus dans la plupart des licences.

Client VPN	Problème/Incompatibilité	Résolution
« Applications » VPN créées sur la plateforme universelle Windows	Ces applications doivent utiliser une API de connexion Microsoft qui exige que DNS soit envoyé à la carte réseau locale, et non à 127.0.0.1. Par conséquent, l'application affiche une erreur indiquant qu'elle ne peut pas se connecter.	Résolu avec le module Umbrella - inclus dans la plupart des licences.
OpenVPN	Incompatible.	Aucun correctif disponible.
Palo Alto GlobalProtect VPN	Ne fonctionne avec aucun client d'itinérance autonome après la version 3.0.10.	Correction grâce au module Umbrella - inclus dans la plupart des licences.
VPN F5	Incompatible.	Corrigé par le module Umbrella - inclus dans la plupart des licences.
VPN de point de contrôle	macOS Only, mode split-tunnel uniquement.	Désactivez le split-tunnel sur macOS.
SonicWall NetExtender	Incompatible.	Corrigé par le module Umbrella - inclus dans la plupart des licences.
VPN Zscaler	Incompatible.	Corrigé par le module Umbrella - inclus dans la plupart des licences.
Protection des terminaux Akamai (client ETP)	Incompatible.	Corrigé par le module Umbrella - inclus dans la plupart des licences.
NordVPN	Utilisez la solution.	Il existe deux options pour ajouter la compatibilité : 1. Utilisez la méthode de connexion OpenVPN décrite dans Comment configurer une connexion manuelle sur Windows à

Client VPN	Problème/Incompatibilité	Résolution
		l'aide d'OpenVPN 2. Autoriser DNS personnalisé sous paramètres avancés. Définissez DNS sur 208.67.220.220 et 208.67.222.222.
VPN Azure	Incompatible.	Corrigé par le module Umbrella - inclus dans la plupart des licences.
VPN AWS	Utilisez la solution.	Modifiez le fichier de configuration (téléchargé manuellement depuis AWS) pour obtenir une deuxième ligne de pull-filter ignore "block-outside-dns".
VPN Pritunl	Incompatible.	Corrigé par le module Umbrella - inclus dans la plupart des licences.

Raisons d'incompatibilité pour les clients VPN

Certains clients VPN ont un comportement DNS similaire à celui d'Umbrella Roaming Client. Si le serveur DNS de connexion VPN prend une valeur inattendue, le logiciel VPN redéfinit les paramètres DNS du système sur la valeur définie par le VPN lors de la connexion initiale. Le client d'itinérance Umbrella effectue également la même opération, en rétablissant tous les serveurs DNS sur 127.0.0.1. Ce comportement de va-et-vient crée un conflit entre le VPN et le client d'itinérance Umbrella. Ce conflit entraîne un cycle sans fin des serveurs DNS pour la réinitialisation de la connexion VPN. Le client d'itinérance détecte cela et se désactive pour maintenir la connexion VPN si possible.

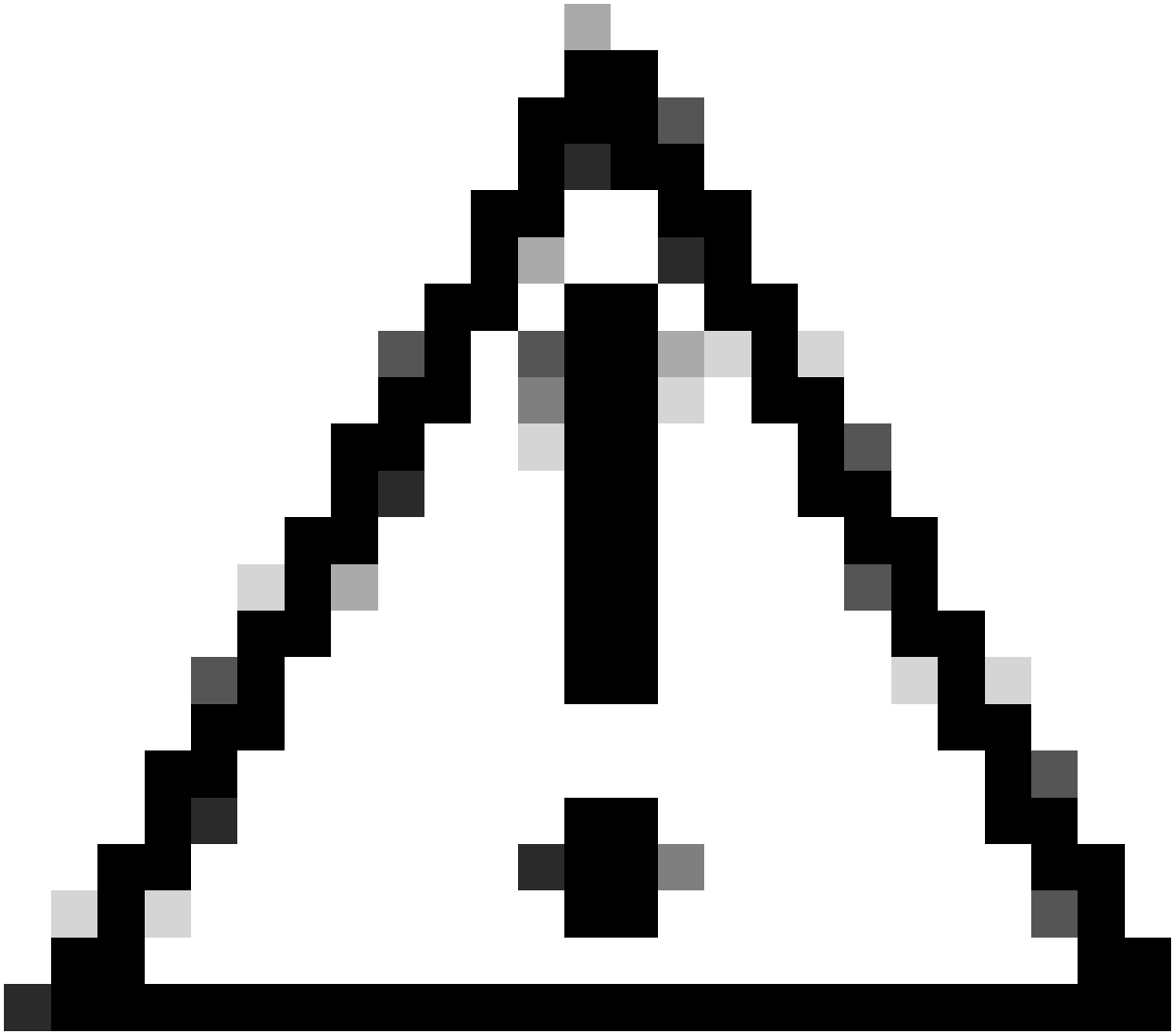
Appliances virtuelles et réseaux protégés

Le client d'itinérance Umbrella se comporte différemment lorsqu'il est connecté à un réseau qui utilise la fonctionnalité Umbrella Virtual Appliances (VA) ou Protected Networks. Cela s'applique qu'un utilisateur se connecte au réseau localement ou via un VPN. Pour plus d'informations, reportez-vous à la documentation relative aux clients itinérants et aux appareils virtuels ou aux réseaux protégés.

Considérations spéciales sur les modules de sécurité Cisco Secure Client + Roaming autonomes et autonomes

Les informations fournies ici sont spécifiques au client d'itinérance Umbrella autonome et ne s'étendent pas au Cisco Secure Client (CSC) + module de sécurité d'itinérance. Les utilisateurs à la recherche d'une installation facile de plugin peuvent utiliser Umbrella Roaming intégré dans CSC. Les utilisateurs VPN Cisco Secure Client doivent migrer vers le module CSC + Roaming Security en cas de problème de fonctionnement du VPN. Cisco Umbrella nécessite une validation sur le module CSC + Roaming Security et recommande une migration complète.

Le logiciel Cisco Secure Client VPN fournit des options pour la façon dont le système gère le DNS lorsqu'une connexion VPN est établie. Consultez l'article Différences de comportement concernant les requêtes DNS et la résolution de noms de domaine dans différents systèmes d'exploitation pour plus de détails. Ces informations sont basées sur l'expérience d'utilisation de Cisco Secure Client et d'Umbrella Roaming Client. Il est recommandé de tester le client d'itinérance Umbrella avec le VPN Cisco Secure Client activé pour garantir les fonctions de résolution DNS interne et externe comme prévu.



Mise en garde : Cisco exige que vous utilisiez le module de sécurité CSC + Roaming si vous utilisez également le client sécurisé Cisco pour la compatibilité des services DNS. Les étapes fournies s'appliquent au client d'itinérance non intégré uniquement si nécessaire. Ces étapes ne sont pas requises pour le module CSC + Roaming Security.

En mode Full Tunnel et en mode split Tunnel, des instructions spéciales sont requises pour permettre au client d'itinérance de fonctionner lorsque le client sécurisé Cisco est connecté. Ceci est nécessaire afin de permettre au DNS de circuler vers le client d'itinérance plutôt que d'être remplacé par le pilote du noyau. Pour un tunnel complet, le symptôme est que le client est forcé de désactiver. Dans le cas de la transmission tunnel partagée, le symptôme est une perte de DNS interne lors de la connexion au VPN.

Ordre de liaison DNS Mode de compatibilité VPN pour Windows 10 et 11

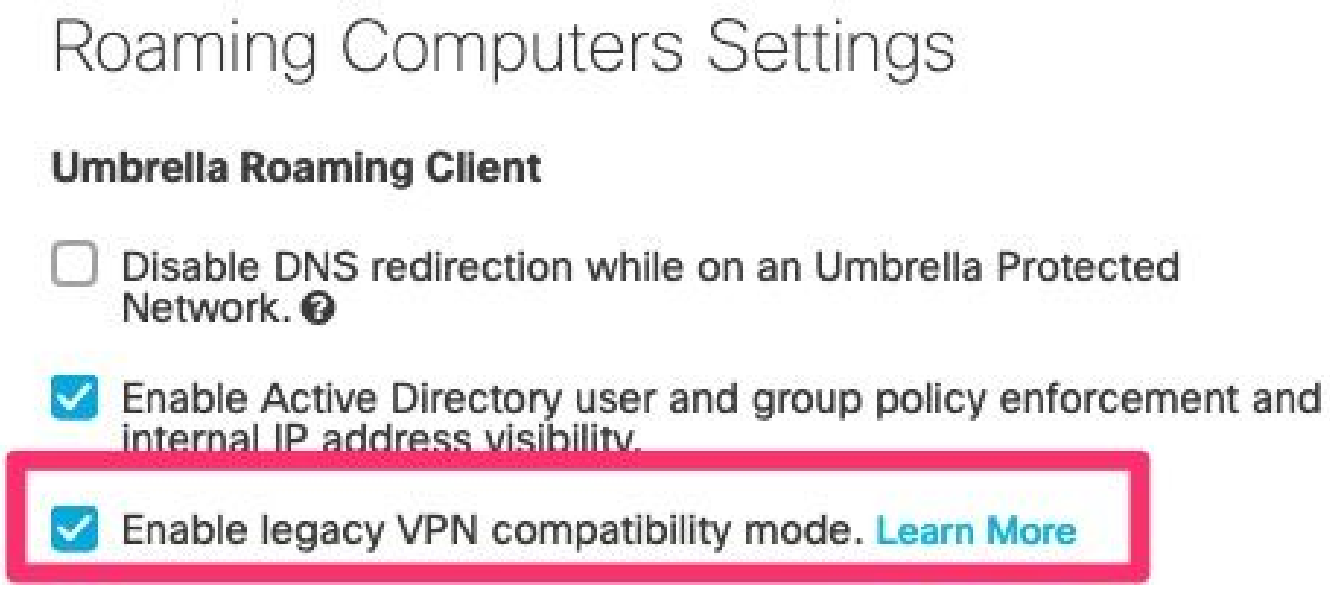
Un nombre limité d'utilisateurs de Windows 10 rencontrent un problème spécifique où le LAN local est prioritaire au lieu de la carte réseau VPN pour DNS. Dans ce cas, le DNS local de la liste des domaines internes du client d'itinérance ne peut pas être résolu alors que le DNS public

fonctionne sans problème. Cela concerne les versions 2.0.338 et 2.0.341 (par défaut) et toutes les versions ultérieures. Le problème ne s'est pas produit sur la version 2.0.255.

Les clients VPN précédemment affectés sont les suivants :

- AnyConnect 3.x
- AnyConnect 4.x (AnyConnect Umbrella ou CSC + module d'itinérance n'est pas affecté)
- VPN Sophos
- Certaines configurations Palo Alto GlobalProtect sur des versions plus anciennes
- VPN mobile WatchGuard
- Shrew Soft VPN
- VPN Barracuda

Résolution
Activez le paramètre du client d'itinérance Activer le mode de compatibilité VPN hérité sur Activé.



360027547111

Pour vérifier s'il s'agit du problème, exécutez le test de diagnostic et cliquez sur les résultats pour resolv.confs. Si l'adaptateur VPN est répertorié en premier, le problème n'affecte pas l'utilisateur. Si l'adaptateur VPN apparaît en deuxième position, le problème peut affecter l'utilisateur.

Exemple de résultat resolv.confs

```
Results for: resolv.confs
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Local Area Connection
nameserver 192.168.2.1
```

```
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Cisco AnyConnect Secure Mobility
nameserver 10.1.1.27
nameserver 10.1.1.28
```

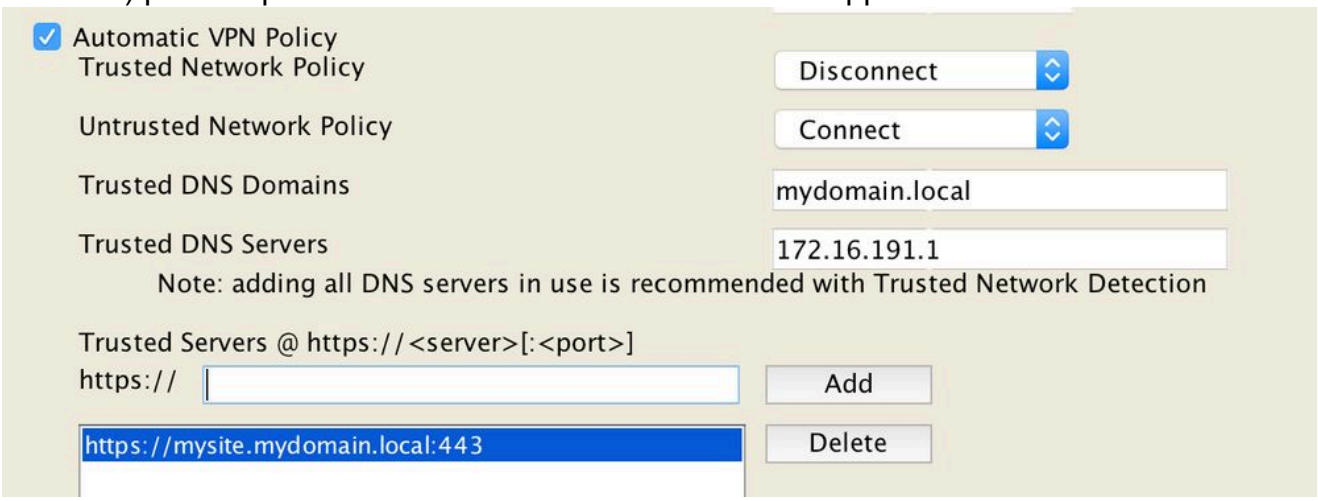
Considérations spéciales pour les VPN tiers

VPN toujours actif

Le client d'itinérance autonome est incompatible avec le paramètre Cisco Secure Client Always On VPN lorsque des serveurs DNS de confiance sont définis. Lorsqu'il est actif, le client d'itinérance autonome définit toujours DNS sur 127.0.0.1, éliminant ainsi tous les serveurs DNS approuvés des paramètres de la carte réseau. Le client d'itinérance peut être désactivé sur le réseau pour restaurer les paramètres DHCP ; cependant, toutes les protections associées au client d'itinérance cessent lorsqu'elles sont configurées. Contactez le support Umbrella pour en savoir plus sur la désactivation du client sur un réseau approuvé.

Solutions

- Le module CSC + Roaming Security Module (Roaming Client for Cisco Secure Client) n'est pas affecté et fonctionne efficacement avec une stratégie VPN automatique.
- Ajoutez 127.0.0.1 à la liste des serveurs DNS approuvés.
- Assurez-vous que d'autres méthodes de détection approuvées sont définies (noms DNS et serveurs) pour empêcher tous les réseaux d'être déclarés approuvés.



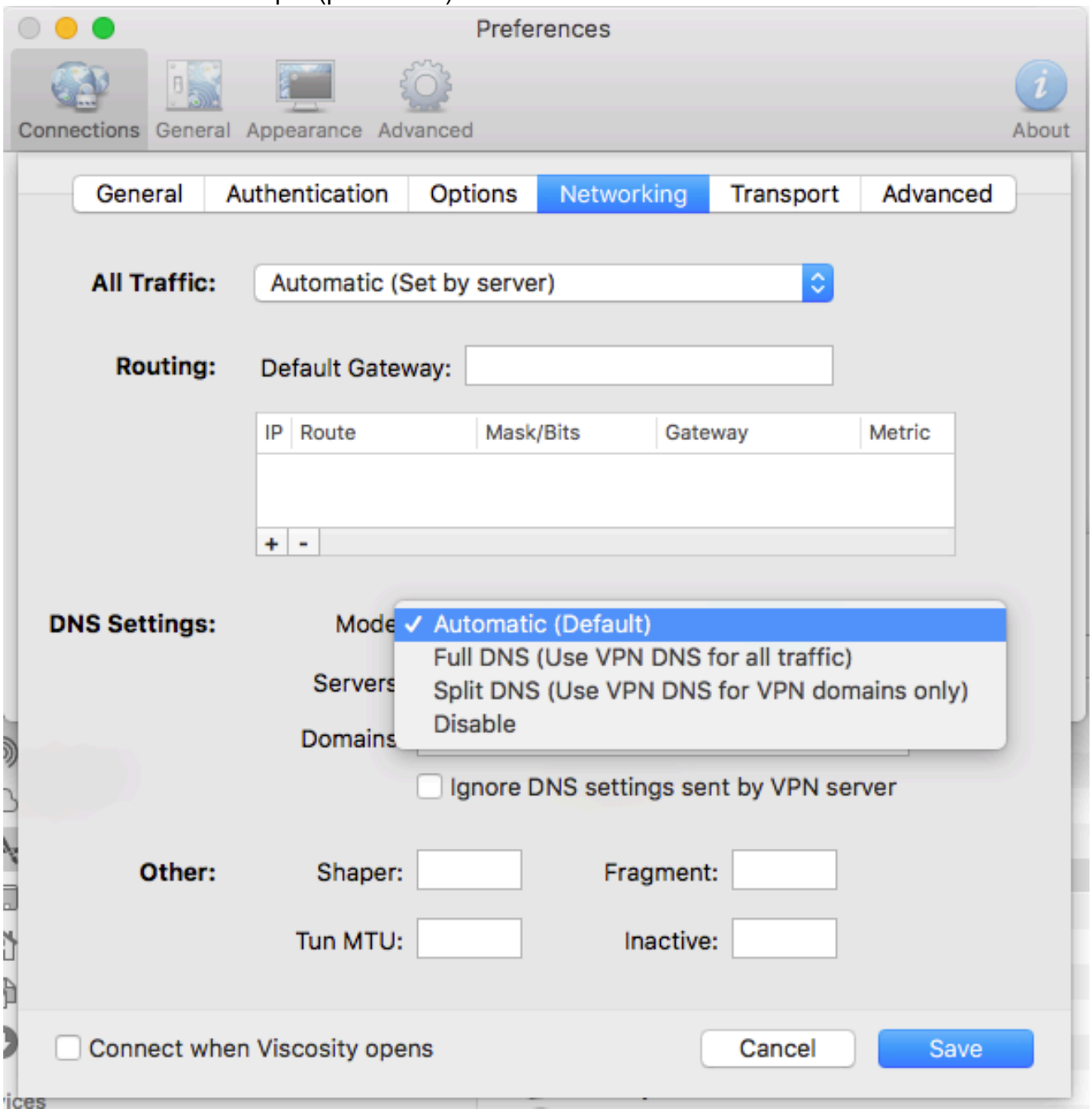
360031250911

VPN de viscosité

Viscosity VPN nécessite une modification des paramètres pour fonctionner avec le client d'itinérance Umbrella. Si ce changement n'est pas effectué, le comportement par défaut de Viscosity imite celui d'autres VPN incompatibles. Cette modification indique à Viscosity d'utiliser les paramètres DNS transmis via le serveur Umbrella pour tous les domaines du domaine de recherche, et 127.0.0.1 continue d'être utilisé pour toutes les autres requêtes.

Configurer la viscosité

1. Dans Viscosity, accédez à Preferences > Connections > <your connection> (site specific) > Networking > DNS Settings.
2. Sélectionnez Automatique (par défaut).



115013433283

Lors de l'utilisation d'un serveur OpenVPN, assurez-vous que persist-tun n'est pas activé côté serveur pour garantir que les modifications du réseau se déclenchent lors de la déconnexion ou de la reconnexion.

Tunnelblick

Tunnelblick nécessite deux modifications pour :

- Autoriser la modification des serveurs DNS de la carte.
- Appliquez les paramètres DNS après l'établissement du tunnel.

En vérifiant les paramètres fournis dans le menu Advanced, Tunnelblick fonctionne avec le client d'itinérance Umbrella :

Dans l'onglet Connexion et déconnexion, activez les deux paramètres suivants :

- Vider le cache DNS après la connexion ou la déconnexion (par défaut)
- Définir le DNS après la définition des routes et non avant celle des routes

Dans l'onglet Pendant la connexion, modifiez ce paramètre en Ignorer :

- DNS: Serveurs > Quand change à la valeur pré-VPN, Quand change à autre chose.

Lors de l'utilisation d'un serveur OpenVPN, assurez-vous que persist-tun n'est pas activé côté serveur pour vous assurer que les modifications du réseau se déclenchent lors de la déconnexion ou de la reconnexion.

Problèmes de déconnexion VPN Tunnelblick

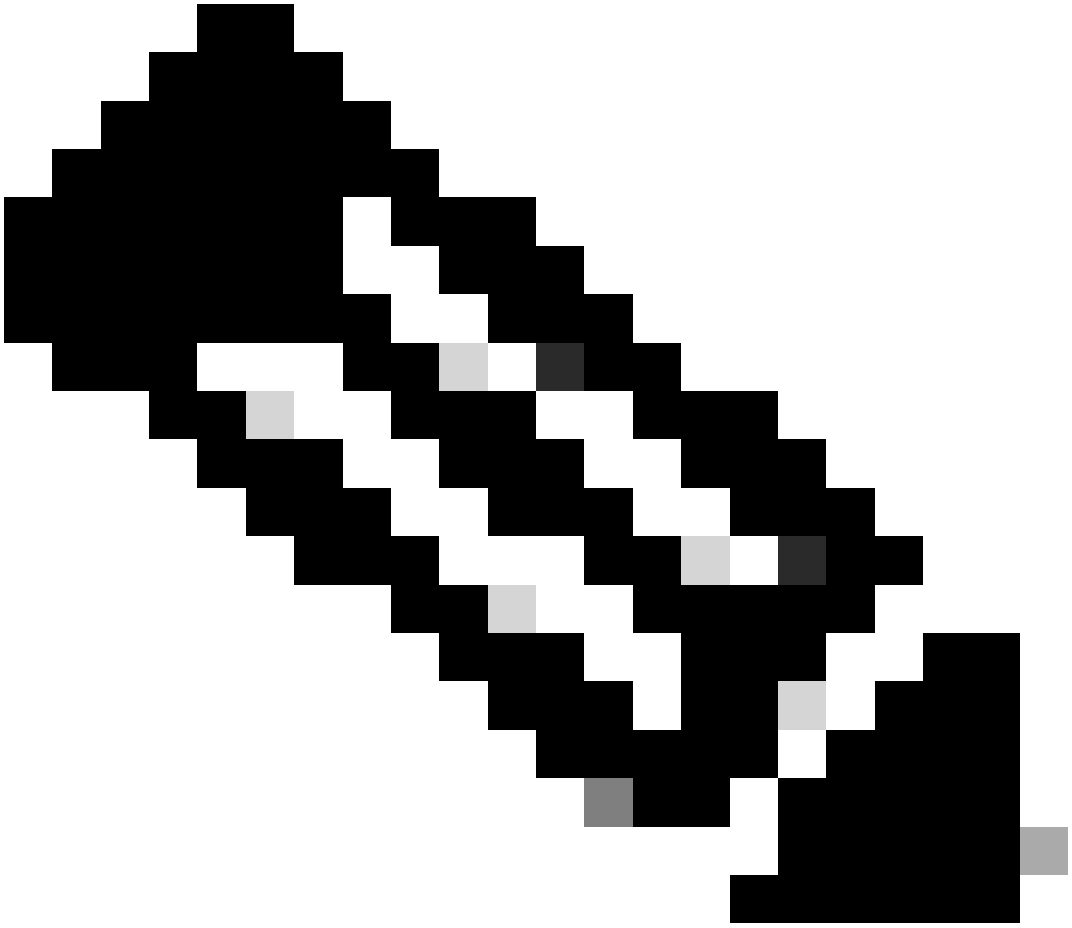
Avec certaines versions de Tunnelblick, le client d'itinérance ne peut pas correctement identifier les serveurs DNS internes corrects après une déconnexion VPN. Si des problèmes avec les domaines internes se produisent après une déconnexion VPN, Umbrella recommande ces étapes :

Cette modification entraîne Tunnelblick à mettre hors service et en service l'interface réseau principale après la déconnexion du VPN. Cette opération est gérée dans l'onglet Settings du panneau de configuration Tunnelblick :

- Dans les versions plus anciennes de Tunnelblick (antérieures à 3.7.5beta03), utilisez la case à cocher Reset the primary interface after disconnection.
- Sur les versions plus récentes de Tunnelblick (3.7.5beta03 et ultérieures), définissez les paramètres On attendu disconnect et On unknown disconnect sur Reset Primary Interface.

Fusée À Vitesse Légère

Lightspeed Rocket dispose de certaines fonctionnalités qui ne sont pas compatibles avec le client d'itinérance. Plus précisément, la modification DNS pour la redirection No SSL Search et SafeSearch CNAME de www.google.com vers nosslsearch.google.com et forcesafesearch.com respectivement entraîne l'échec de toutes les résolutions de DNS de www.google.com tant que la redirection de DNS Lightspeed Rocket est activée.



Remarque : Cet article fait référence au client d'itinérance autonome Umbrella. Pour obtenir un article complémentaire sur le module de sécurité d'itinérance Umbrella pour le client sécurisé Cisco et les logiciels hérités, reportez-vous à la documentation appropriée.

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.