Examiner le comportement des requêtes DNS et la résolution des noms de domaine

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Séparation par rapport au DNS standard
  - Test du DNS : important
- Vrai contre DNS fractionné au mieux
- Tunnel-all et Tunnel-all DNS
  - Tunnel-all-DNS et Cisco Secure Client Umbrella Module
- Problème de performances DNS résolu dans AnyConnect version 3.0 (4235)
  - Solutions de contournement (si aucune mise à niveau n'est possible)
- DNS avec split tunneling sur différents systèmes d'exploitation clients
  - Microsoft Windows (Windows 10 et Windows 11)
    - Configuration de tous les tunnels (et transmission tunnel partagée avec Tunnel-all-DNS activé)
    - Configuration du Split-include (Tunnel-all-DNS Disabled, No Split-DNS)
    - Configuration de l'exclusion du fractionnement (Tunnel-all-DNS Disabled, no Split-DNS)
    - Split-DNS (Tunnel-all-DNS désactivé, Split-include configuré)
    - Split-DNS avec fractionnement-exclusion Tunneling (Secure Client 5.x)
    - DNS chiffré (DoH/DoT) sous Windows
  - macOS
    - Configuration de tous les tunnels (et transmission tunnel partagée avec Tunnel-all-DNS activé)
    - Split-include / Split-exclude (Tunnel-all-DNS désactivé, pas de Split-DNS)
    - Split-DNS (Tunnel-all-DNS désactivé, Split-include configuré)
  - Linux
    - Configuration de tous les tunnels (et transmission tunnel partagée avec Tunnel-all-DNS activé)
    - Split-include / Split-exclude (Tunnel-all-DNS désactivé, pas de Split-DNS)
    - Split-DNS (Tunnel-all-DNS désactivé, Split-include configuré)
    - VM et conteneurs Linux
  - Apple iOS (iPhone et iPad)
- Tunnellisation partagée dynamique et DNS (Secure Client 4.5+)
- Versions client historiques (référence)
- Informations de bogue associées
- Informations connexes
- Historique de révision
- Le document s'applique

Introduction

Ce document décrit comment les systèmes d'exploitation clients gèrent les requêtes DNS et les effets sur la résolution de noms de domaine à l'aide du client sécurisé Cisco IOS®.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Les exemples de travaux pratiques utilisent les stratégies de groupe ASA/FTD de pare-feu sécurisé et Cisco Secure Client sur Windows, macOS, Linux et Apple iOS.

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.

Séparation par rapport au DNS standard

Ce document explique comment les systèmes d'exploitation clients gèrent les requêtes DNS et les effets sur la résolution de noms de domaine lors de l'utilisation de Cisco Secure Client (anciennement Cisco AnyConnect) avec la transmission tunnel partagée ou complète. Les têtes de réseau VPN abordées incluent Cisco Secure Firewall ASA et FTD (anciennement ASA) ; les paramètres de stratégie de groupe tels que split-dns, dns-server, et split-tunnel-all-dns s'appliquent aux deux, sauf indication contraire.

Si une section fait explicitement référence à d'anciennes versions du client, le comportement décrit pour Secure Client 4.2 et versions ultérieures (y compris les versions actuelles de Secure Client 5.x) s'applique. Cisco AnyConnect 4.x est arrivé en fin de vie ; migrer vers Cisco Secure Client pour bénéficier des fonctionnalités DNS et de tunnellisation prises en charge.

Le comportement de résolution DNS dépend de trois facteurs :

- Politique DNS VPN : Configuré sur la tête de réseau (DNS fractionné, tunnel-all-DNS ou DNS standard)
- Mode split-tunneling : Tunnel-all, split-include ou split-exclude
- Système d'exploitation client : Architecture du résolveur DNS (par interface ou globale)

Lorsque vous exécutez la commande split-include tunneling, voici les trois options DNS disponibles dans la stratégie de groupe :

Mode	Description
Fractionner DNS	Les requêtes DNS qui correspondent aux noms de domaine configurés sur la tête de réseau (split-dns) sont envoyées via le tunnel aux serveurs DNS VPN (`dns-server`). Toutes les autres requêtes utilisent le résolveur du système d'exploitation client et les serveurs DNS de la carte physique.
Tunnel-all-DNS	Seul le trafic DNS vers les serveurs DNS définis par la tête de réseau est autorisé. Configuré avec split-tunnel-all-dns enable dans la stratégie de groupe.
DNS standard	Toutes les requêtes DNS sont d'abord envoyées aux serveurs DNS VPN définis par la tête de réseau. En cas de réponse négative (NXDOMAIN ou pas de réponse), le résolveur peut également essayer des serveurs DNS sur la carte physique.



Remarque : La commande split-tunnel-all-dns a d'abord été implémentée dans ASA version 8.2(5). Avant cette version, seul le DNS fractionné ou le DNS standard était disponible. Dans tous les cas, les requêtes DNS définies pour se déplacer dans le tunnel sont transmises à n'importe quel serveur DNS défini par la tête de réseau. Si aucun serveur DNS n'est défini sur la tête de réseau, les paramètres DNS du tunnel sont vides.

Si les DNS partagés ne sont pas définis, toutes les requêtes DNS sont envoyées aux serveurs DNS définis par la tête de réseau (en fonction du comportement spécifique au système d'exploitation décrit plus loin dans ce document). Cependant, les comportements décrits dans ce document peuvent varier en fonction du système d'exploitation.

Test du DNS : important



Remarque : Évitez d'utiliser NSLookup ou dig lors du test de la résolution de nom sur le client. Utilisez plutôt un navigateur Web ou exécutez la commande ping. NSLookup et dig n'utilisent pas le résolveur DNS du système d'exploitation de la même manière que la plupart des applications. Secure Client ne force pas chaque requête DNS via une interface spécifique ; elle autorise ou rejette les requêtes basées sur la politique DNS fractionnée et tunnel-all-DNS.

Pour observer un comportement de basculement correct, testez uniquement les applications qui reposent sur le résolveur DNS du système d'exploitation natif (navigateurs, requêtes ping et la plupart des applications professionnelles). Les outils qui effectuent leur propre résolution DNS (NSLookup, dig et certaines applications personnalisées) peuvent afficher des erreurs trompeuses même lorsque le client fonctionne correctement.

Vrai contre DNS fractionné au mieux

La version 2.4 d'AnyConnect a introduit la reprise DNS partagée (DNS partagé au mieux), qui n'est pas un véritable DNS divisé et qui a également été trouvée dans le client IPsec hérité.

Comportement au mieux (de secours) :

- Si la demande correspond à un domaine DNS partagé, le client sécurisé autorise la transmission tunnel de la demande vers la tête de réseau.
- Si le serveur DNS VPN ne peut pas résoudre le nom d'hôte, le résolveur DNS du système d'exploitation continue et peut envoyer la même requête à un serveur DNS sur l'interface physique.
- Si la requête ne correspond à aucun domaine DNS partagé, le client sécurisé ne la tunnellise pas. Il peut synthétiser une réponse pour que le résolveur revienne aux serveurs DNS de l'interface physique.

C'est pourquoi la fonctionnalité héritée est appelée DNS fallback pour le split tunneling, qui n'est pas un vrai split DNS. Le client sécurisé garantit que seules les requêtes de domaine DNS partagé correspondantes entrent dans le tunnel, mais s'appuie toujours sur le comportement du résolveur du système d'exploitation pour la résolution finale.

Problème de sécurité : Un nom de domaine privé peut fuir vers un serveur DNS public lorsque le serveur DNS VPN retourne NXDOMAIN ou ne parvient pas à résoudre ; et le résolveur réessaie sur la carte physique.

Véritable DNS fractionné : ID de bogue Cisco CSCtn14578

Résolu sous Microsoft Windows dans AnyConnect 3.0(4235) et conservé dans Secure Client 4.2+) :

- Les requêtes pour les domaines DNS partagés configurés sont autorisées uniquement via le chemin VPN (serveurs DNS de tunnel/adaptateur VPN, selon la plate-forme et la version).
- Toutes les autres requêtes sont autorisées uniquement via des serveurs DNS non VPN (adaptateur physique).



Remarque : Seuls les utilisateurs Cisco enregistrés ont accès aux outils de bogue Cisco internes et aux informations détaillées sur les bogues.

Tunnel-all et Tunnel-all DNS

Lorsque la transmission tunnel partagée est désactivée (configuration tunnel-all), le trafic DNS est autorisé uniquement via le tunnel.

La configuration tunnel-all-DNS (split-tunnel-all-dns enable dans la stratégie de groupe) envoie toutes les recherches DNS via le tunnel alors qu'une certaine forme de split tunneling est également configurée, et le trafic DNS est autorisé strictement via l'interface de tunnel.

Ceci est cohérent entre les plates-formes avec une mise en garde sur Microsoft Windows, quand le tunnel-all ou le tunnel-all-DNS est configuré, le client sécurisé autorise le trafic DNS strictement aux serveurs DNS configurés sur la passerelle sécurisée (appliquée à l'adaptateur VPN). Cette amélioration de la sécurité a été mise en oeuvre avec un véritable DNS divisé. Si cela pose problème (par exemple, la mise à jour/l'enregistrement DNS doit atteindre des serveurs DNS non VPN), procédez comme suit :

1. Si la configuration actuelle est tunnel-all, activez la transmission tunnel split-exclude. Tout réseau à hôte unique à exclusion fractionnée est acceptable, par exemple une adresse link-local.

2. Assurez-vous que tunnel-all-DNS n'est pas activé dans la stratégie de groupe (split-tunnel-all-dns disable.)

Tunnel-all-DNS et Cisco Secure Client Umbrella Module

Lorsque la transmission tunnel partagée et tunnel-all-DNS sont toutes deux activées, DNS est intercepté au niveau du noyau et bloqué s'il ne sort pas de l'interface VPN correcte. Le module Secure Client Umbrella (anciennement AnyConnect Roaming Security) peut être affecté sur les réseaux où le DNS chiffré n'est pas disponible. En effet, le module peut tenter un DNS standard via l'interface LAN alors que le tunnel-all-DNS nécessite un DNS via le VPN.

Par défaut, le module Umbrella utilise le DNS chiffré (port UDP 443), qui n'est généralement pas bloqué par tunnel-all-DNS. Le problème apparaît principalement lorsque le cryptage n'est pas disponible et que le DNS simple est utilisé.

Recommandation : Ajoutez les adresses de résolution Cisco Umbrella à la liste d'inclusion partagée si vous utilisez tunnel-all-DNS avec le module Umbrella. Ou référez-vous au document Enable Tunnel All DNS for Secure Client with Umbrella Module (ID de document : 224809.)

Problème de performances DNS résolu dans AnyConnect version 3.0 (4235)

Ce problème Microsoft Windows est le plus courant dans les conditions suivantes :

- Configuration d'un routeur domestique où les serveurs DNS et DHCP partagent la même adresse IP (le client sécurisé crée une route nécessaire vers le serveur DHCP)
- Un grand nombre de suffixes/domaines DNS dans la stratégie de groupe.
- Une configuration tunnel-all.
- La résolution de noms utilise un nom d'hôte non qualifié. Ainsi, le résolveur essaie plusieurs suffixes DNS sur tous les serveurs DNS disponibles.
- Le client DNS natif tente d'envoyer des requêtes DNS via l'adaptateur physique, que le client sécurisé bloque sous tunnel-all.

Cela peut entraîner des délais de résolution de noms importants, en particulier lorsque la tête de réseau envoie de nombreux suffixes DNS. Le résolveur doit parcourir les suffixes et les serveurs

jusqu'à ce qu'il reçoive une réponse positive.

Ce problème est résolu dans AnyConnect 3.0(4235) et les versions ultérieures de Secure Client. Référez-vous à l'ID de bogue Cisco CSCtq02141 et à l'ID de bogue Cisco CSCtn14578 pour plus de détails.

Remarque : Seuls les utilisateurs Cisco enregistrés ont accès aux outils de bogue Cisco internes.

Solutions de contournement (si aucune mise à niveau n'est possible)

Activez la tunnellisation à exclusion partagée pour une adresse IP afin que le DNS local puisse utiliser la carte physique. Une adresse du sous-réseau link-local 169.254.0.0/16 est généralement utilisée car le trafic vers ces adresses ne traverse probablement pas le VPN.

Après avoir activé la transmission tunnel à exclusion partagée, activez l'accès au réseau local sur le profil client ou le client, et désactivez tunnel-all-DNS. Voici un exemple de configuration ASA/FTD :

```
access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
group-policy gp_access-14 attributes
split-tunnel-policy excludespecified
split-tunnel-network-list value acl_linklocal_169.254.1.1
split-tunnel-all-dns disable
exit
```

XML du profil client :

```
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
```

Vous pouvez également l'activer dans l'interface utilisateur graphique Secure Client : Préférences → Activer Autoriser l'accès local (LAN) lors de l'utilisation du VPN

1. Utilisez des noms de domaine complets (FQDN) au lieu de noms d'hôtes non qualifiés.
2. Utilisez une adresse IP différente pour le serveur DNS sur l'interface physique (distincte de DHCP sur le même sous-réseau).

DNS avec split tunneling sur différents systèmes d'exploitation clients

Différents systèmes d'exploitation clients gèrent le DNS différemment avec le split tunneling (sans le split DNS) pour le client sécurisé ; cette section décrit ces différences.

Microsoft Windows (Windows 10 et Windows 11)

Sous Windows, les paramètres DNS sont définis par interface réseau. Avec la transmission tunnel partagée, les requêtes DNS peuvent revenir aux serveurs DNS de la carte physique après leur défaillance sur la carte tunnel VPN. Si la transmission tunnel partagée est utilisée sans DNS partagé, la résolution interne et externe peut fonctionner car le résolveur peut revenir à des serveurs DNS externes. Il y a eu un changement significatif dans Secure Client pour Windows dans la version 4.2 après le correctif pour l'ID de bogue Cisco CSCuf0785. Ce comportement est inchangé dans Secure Client 5.x.



Remarque : Seuls les utilisateurs Cisco enregistrés ont accès aux outils de bogue Cisco internes.

Configuration de tous les tunnels (et transmission tunnel partagée avec Tunnel-all-DNS activé)

Pre-Secure Client 4.2 (AnyConnect 4.1 et versions antérieures) :

- Seules les requêtes DNS aux serveurs DNS configurés dans la stratégie de groupe (serveurs DNS de tunnel) sont autorisées.
- Le pilote du client sécurisé répond à toutes les autres requêtes sans ce nom.
- La résolution DNS peut uniquement utiliser des serveurs DNS de tunnel.

Secure Client 4.2 et versions ultérieures :

- Les requêtes DNS vers n'importe quel serveur DNS sont autorisées si elles proviennent de l'adaptateur VPN et sont envoyées via le tunnel.
- Toutes les autres demandes ne reçoivent pas ce nom ; résolution via le tunnel VPN uniquement.
- Avant l'ID de bogue Cisco CSCuf07885, le client sécurisé limitait les serveurs DNS cibles. Après cette correction, il restreint les cartes réseau qui peuvent lancer des requêtes DNS.

Configuration du Split-include (Tunnel-all-DNS Disabled, No Split-DNS)

Le pilote du client sécurisé n'interfère pas avec le résolveur DNS natif. La résolution est conforme à l'ordre de la carte réseau ; Secure Client est l'adaptateur préféré lorsque le VPN est connecté.

Une requête DNS est d'abord envoyée via le tunnel ; s'il n'est pas résolu, le résolveur peut essayer l'interface publique. La liste de contrôle d’accès à inclusion partagée doit inclure le sous-réseau couvrant le ou les serveurs DNS du tunnel dans les versions antérieures à la version 4.2. À partir de la version 4.2 du client sécurisé, les routes d’hôte pour le ou les serveurs DNS du tunnel sont automatiquement ajoutées en tant que réseaux à inclusion partagée (routes sécurisées), de sorte que la liste de contrôle d’accès à inclusion partagée ne nécessite plus de sous-réseaux de serveurs DNS du tunnel explicites.

Configuration de l'exclusion du fractionnement (Tunnel-all-DNS Disabled, no Split-DNS)

Le même comportement de résolveur que le split-include, d'abord le tunnel, puis le fallback de l'interface publique. La liste d'accès à exclusion fractionnée ne doit pas inclure le sous-réseau couvrant le ou les serveurs DNS du tunnel. À partir de Secure Client 4.2, les routes d'hôte automatiques pour les serveurs DNS de tunnel empêchent les erreurs de configuration courantes de split-exclude.

Split-DNS (Tunnel-all-DNS désactivé, Split-include configuré)

Le Split-DNS sous Windows nécessite le tunneling split-include (split-tunnel-policy tunnelspecified). Il ne prend pas en charge les politiques de tunnel split-exclude-only pour la

configuration du DNS partagé.

Client pré-sécurisé 4.2 :

- Requêtes de domaine DNS fractionné : Autorisé à tunnel les serveurs DNS uniquement ; aucun nom de ce type si envoyé à d'autres serveurs.
- Requêtes de domaine DNS non partagé : Autorisé pour les autres serveurs DNS uniquement ; pas de nom de ce type si tenté via tunnel.

Secure Client 4.2 et versions ultérieures (true split DNS sous Windows) :

- Requêtes de domaine DNS fractionné : Autorisé sur n'importe quel serveur DNS uniquement s'ils proviennent de l'adaptateur VPN. Les requêtes de l'interface publique ne reçoivent pas ce nom pour forcer l'utilisation du tunnel.
- Requêtes de domaine DNS non partagé : Autorisé sur tout serveur DNS uniquement s'ils proviennent de la carte physique. Les requêtes de l'adaptateur VPN ne reçoivent pas ce nom pour forcer la résolution de l'interface publique.

Split-DNS avec fractionnement-exclusion Tunneling (Secure Client 5.x)

La documentation d'administration de Secure Client 5.x ajoute le DNS fractionné pour les configurations à exclusion fractionnée. Reportez-vous au Guide de l'administrateur de Secure Client 5.x — Configure Split DNS for Split Exclude Tunneling pour les exigences de tête de réseau et de stratégie. Les règles d'application au niveau du système d'exploitation continuent à s'appliquer une fois le DNS partagé actif.

DNS chiffré (DoH/DoT) sous Windows

Les applications ou les fonctionnalités du système d'exploitation qui utilisent DNS sur HTTPS (DoH) ou DNS sur TLS (DoT) peuvent contourner le chemin de résolution de stub Windows que le client sécurisé filtre. Si le DNS partagé semble échouer pour des applications spécifiques mais fonctionne dans un navigateur, vérifiez si ces applications utilisent un DNS chiffré ou personnalisé. Le test DNS fractionné standard doit utiliser le résolveur du système d'exploitation (navigateur, ping) et non NSLookup/dig.

---

macOS

Sur macOS, les paramètres DNS sont globaux (et non par interface). Si la transmission tunnel partagée est utilisée sans DNS partagé, les requêtes DNS ne peuvent souvent pas atteindre les serveurs DNS en dehors du tunnel comme prévu, vous pouvez résoudre les noms internes uniquement, et non les noms externes via le chemin public. Ceci est documenté dans l'ID de bogue Cisco CSCtf20226 et l'ID de bogue Cisco CSCtz86314.

Contournements :

- Spécifiez une adresse IP de serveur DNS externe dans la stratégie de groupe et utilisez des noms de domaine complets pour les requêtes internes.
- Si les noms externes peuvent être résolus par le tunnel, désactivez le DNS partagé dans Advanced > Split Tunneling en supprimant les noms DNS de la stratégie de groupe et utilisez les noms de domaine complets pour les requêtes internes.

Le DNS fractionné sur macOS est pris en charge à partir d'AnyConnect 3.1, sous réserve des conditions suivantes :

- Split DNS activé pour les deux protocoles IP (ASA 9.0+/FTD équivalent requis) ou ;
- Split DNS activé pour un protocole IP et Client Bypass Protocol activé pour l'autre avec aucun pool d'adresses pour le protocole contourné (ou aucun pool IPv6 sur les versions ASA antérieures à 9.0).

Remarque : Secure Client ne gère pas principalement la résolution de noms via /etc/resolv.conf sur macOS ; Il configure les paramètres DNS au niveau du système d'exploitation. macOS peut maintenir resolv.conf à jour pour des raisons de compatibilité. Exécutez scutil —dns pour afficher la configuration DNS effective.

Configuration de tous les tunnels (et transmission tunnel partagée avec Tunnel-all-DNS activé)

Lorsque le client sécurisé est connecté, seuls les serveurs DNS de tunnel restent dans la configuration DNS du système ; les requêtes ne procèdent qu'au tunnel du ou des serveurs DNS.

Split-include / Split-exclude (Tunnel-all-DNS désactivé, pas de Split-DNS)

Le client sécurisé n'interfère pas avec le résolveur natif. Les serveurs DNS de tunnel sont préférés

aux résolveurs publics, de sorte que la première tentative de requête passe par le tunnel. Comme le DNS est global sur macOS, les requêtes n'utilisent pas toujours de manière fiable le DNS public en dehors du tunnel (ID de bogue Cisco : CSCtf2026).

À partir de Secure Client 4.2, les routes d'hôte pour les serveurs DNS de tunnel sont ajoutées automatiquement en tant que routes sécurisées.

Split-DNS (Tunnel-all-DNS désactivé, Split-include configuré)

Le vrai DNS fractionné (similaire à Windows) s'applique lorsque :

- Split-DNS est activé pour IPv4 et IPv6, ou ;
- Le Split-DNS est activé pour un protocole et aucun pool d'adresses client n'existe pour l'autre protocole.

Un vrai DNS partagé signifie que les domaines DNS partagés correspondants sont résolus uniquement via le tunnel et ne sont pas transmis à des résolveurs externes.

Si le split-DNS est activé pour un seul protocole et qu'une adresse de client est attribuée pour l'autre protocole, seul le fallback DNS pour le split tunneling est appliqué : Le client sécurisé autorise les requêtes correspondantes via le tunnel (d'autres requêtes peuvent être refusées pour forcer le basculement), mais ne peut pas empêcher complètement les fuites de requêtes de domaine DNS partagé envoyées en clair via l'adaptateur public.

Prise en charge de la plate-forme (guide d'administration Secure Client) : Le DNS partagé complet est pris en charge sous Windows et macOS. Linux a une prise en charge limitée (voir la section Linux).

Linux

Configuration de tous les tunnels (et transmission tunnel partagée avec Tunnel-all-DNS activé)

Lorsque le client sécurisé est connecté, seuls les serveurs DNS de tunnel sont gérés dans la configuration DNS du système.

Split-include / Split-exclude (Tunnel-all-DNS désactivé, pas de Split-DNS)

Le client sécurisé n'interfère pas avec le résolveur natif. Les serveurs DNS de tunnel sont préférés ; la première tentative de résolution passe par le tunnel.

Split-DNS (Tunnel-all-DNS désactivé, Split-include configuré)

Si le split-DNS est activé, seul le fallback DNS pour le split tunneling est appliqué sous Linux :

- Le client sécurisé autorise les requêtes de domaine DNS partagé via le tunnel.
- D'autres requêtes peuvent être refusées pour encourager le basculement vers le DNS public.
- Le client sécurisé ne peut pas appliquer complètement les requêtes de domaine DNS partagé, car elles ne sont jamais envoyées en clair via l'adaptateur public.

Le guide d'administration du client sécurisé note un DNS partagé limité sur Linux : seules les requêtes DNS tunnelisées sont entièrement soumises à la politique DNS partagée ; certaines requêtes en dehors du tunnel ne peuvent pas se conformer à la stratégie DNS partagée.

VM et conteneurs Linux

Le client sécurisé prend en charge un attribut personnalisé tunnel-from-any-source, de sorte que les paquets avec n'importe quelle adresse source peuvent être routés en mode split-include ou split-exclude dans des instances de VM ou des conteneurs Docker. Reportez-vous au guide Secure Client 5.x Administrator Guide pour obtenir des détails sur la configuration.

Apple iOS (iPhone et iPad)

Le comportement d'iOS diffère de celui de macOS et n'est pas identique à Windows. Si la transmission tunnel partagée est configurée sans DNS partagé, les requêtes DNS utilisent généralement le serveur DNS global défini pour le périphérique, et non le même modèle de secours que Windows.

Impact pratique : Les entrées de domaine DNS fractionné sont souvent requises pour une résolution de noms interne fiable lors de l'utilisation de la transmission tunnel fractionnée sans

DNS fractionné.

Correction historique : ID de bogue Cisco CSCtq09624 - (AnyConnect pour iOS 2.5.4038 et versions ultérieures.) Le client sécurisé actuel pour iOS obéit aux mêmes exigences générales ; configurez le service DNS partagé pour les domaines internes lorsque vous utilisez le service split-include/split et exclude sans recourir à la reprise de type Windows.

Remarque : Les requêtes DNS iOS ignorent les domaines .local (ID de bogue Cisco CSCts89292).

Apple considère cela comme un comportement conçu ; ne vous attendez pas à une résolution .local via le DNS fractionné standard sur iOS. Sur iOS, le comportement du DNS partagé du client sécurisé diffère également des autres plates-formes lorsque la transmission tunnel partagée est combinée à certaines configurations de liste DNS partagée. Reportez-vous à la section Guide de l'administrateur du client sécurisé Comportement de résolution DNS partagée avec le tunnel partagé pour les combinaisons de stratégies spécifiques à iOS (split-dns none, default-domain, etc.)

Tunnellisation partagée dynamique et DNS (Secure Client 4.5+)

Le split tunneling dynamique résout les FQDN au moment de la connexion ou à la demande, et ajuste le routage et les filtres pour le trafic vers les domaines spécifiés. Ceci est inclus ou exclu du tunnel sans listes d'adresses IP statiques.

Fonctionnalité	Description
Exclure le fractionnement dynamique	Les domaines (exemple.com) sont exclus du tunnel au moment de l'exécution lorsque les applications résolvent ces noms.
Diviser dynamiquement inclure	Les domaines sont inclus dynamiquement dans le tunnel.
Séparation dynamique améliorée	Listes de domaines d'inclusion/exclusion combinées avec des règles de priorité (comme l'exclusion de example.com, mais l'inclusion de mail.example.com).

La transmission tunnel partagée dynamique utilise la résolution DNS pour générer les modifications de routage. Il est configuré via les attributs personnalisés du client sécurisé sur la tête de réseau (par exemple dynamic-split-exclude-domains, dynamic-split-include-domains.)

La transmission tunnel partagée dynamique s'applique aux politiques tunnel-all et split-exclude (dynamic exclude) ou split-include (dynamic include). Il ne remplace pas la stratégie DNS partagée, mais il la complète : diviser les contrôles DNS pour savoir quelles requêtes sont tunnellisées ; Le split tunneling dynamique contrôle le trafic IP tunnellisé en fonction des noms résolus. Reportez-vous aux détails de configuration : Configure Dynamic Split Tunneling et le Guide d'administration de Secure Client 5.x.

Basculement en mode « split exclude » (client sécurisé 5.x) : L'attribut personnalisé facultatif SplitExcludeFailoverEnabled achemine le trafic via le VPN lorsque le chemin public n'a pas de connectivité aux cibles d'exclusion de fractionnement. Reportez-vous au guide de l'administrateur pour la configuration des attributs personnalisés.

Versions client historiques (référence)

Le tableau suivant s'applique uniquement aux déploiements hérités qui exécutent encore des clients obsolètes :

Version	Pertinence
AnyConnect 2.4	Introduction de la reprise DNS partagée au mieux
AnyConnect 2.5 (iOS)	ID de bogue Cisco : CSCtq09624 alignement DNS iOS
AnyConnect 3.0(4235)	Véritable DNS fractionné sous Windows ; Correctifs de performances DNS
AnyConnect 3.1 (macOS)	Prise en charge du DNS fractionné avec conditions IPv4/IPv6
AnyConnect 4.2	ID de bogue Cisco : CSCuf0785 application basée sur la carte ; Tunnel automatique Routes d'hôtes DNS

Déployez Secure Client 5.x sur toutes les plates-formes prises en charge pour obtenir les correctifs et fonctionnalités actuels.

Informations de bogue associées

Remarque : Seuls les utilisateurs Cisco enregistrés ont accès aux outils de bogue Cisco internes.

- ID de bogue Cisco : CSCtn14578 - Vrai DNS fractionné (pas de secours) - Windows, 3.0(4235)+
- ID de bogue Cisco : CSCtq02141 - Délai DNS lorsque le DNS du FAI se trouve sur le même sous-réseau que l'IP publique
- ID de bogue Cisco : CSCuf07885 - DNS Windows : Restreindre par adaptateur et non par serveur cible - 4.2+
- ID de bogue Cisco : CSCtf2026 - DNS de tunnel partagé macOS contrairement à Windows
- ID de bogue Cisco : CSCtz86314 - requêtes DNS fractionnées macOS non envoyées via le tunnel
- ID de bogue Cisco : CSCtq09624 - comportement DNS du tunnel partagé iOS
- ID de bogue Cisco : CSCts89292 - iOS ignore les domaines .local DNS
- ID de bogue Cisco : CSCsv34395 - Prise en charge du proxy FQDN vers le serveur DHCP

Informations connexes

- Examiner le comportement des requêtes DNS et la résolution de noms de domaine (Cisco.com) — ID de document 116016
- Guide d'administration de Cisco Secure Client 5.x — Configuration de l'accès VPN/DNS partagé
- Configuration de la transmission tunnel partagée dynamique ASA/AnyConnect — ID de document 215383
- Module Enable Tunnel All DNS for Secure Client with Umbrella — ID de document 224809
- Interopérabilité entre AnyConnect et le client d'itinérance OpenDNS — ID de document 200395
- Assistance technique de Cisco et téléchargements

Historique de révision

Révision	Date	Commentaires
4.0	28-juil-2026	Mise à jour complète : Personnalisation sécurisée du client, actualisation de la plate-forme, transmission tunnel partagée dynamique, Umbrella/tunnel-all-DNS, correctifs de typo et de configuration, liens connexes corrigés
3.0	23-mai-	Recertification (Cisco.com)

Révision	Date	Commentaires
	2024	
1.0	12-juin-2014	Première publication

Le document s'applique

- Cisco Secure Client (y compris AnyConnect) : Windows, macOS, Linux, iOS
- Stratégies de groupe VPN d'accès à distance Cisco Secure Firewall ASA et FTD

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.