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
- Vrai contre DNS fractionné au mieux
- Tunnel-all et Tunnel-all DNS
- Problème de performances DNS résolu dans AnyConnect version 3.0(4235)
- DNS avec split tunneling sur les différents systèmes d'exploitation Cisco
  - Microsoft Windows
    - Windows 7+
    - Configuration de Split-Incluse (tunnel-all DNS désactivé et no split-DNS)
    - Configuration de l'exclusion partagée (DNS avec tous les tunnels désactivé et pas de DNS divisé)
    - Split-DNS (tunnel-all DNS désactivé, split-include configuré)
  - Mac OSx
    - Configuration de tous les tunnels (et split-tunneling avec tunnel-all DNS activé)
    - Configuration de Split-Incluse (tunnel-all DNS désactivé et no split-DNS)
    - Configuration de l'exclusion partagée (DNS avec tous les tunnels désactivé et pas de DNS divisé)
    - Split-DNS (tunnel-all DNS désactivé, split-include configuré)
  - Linux
    - Configuration de tous les tunnels (et split-tunneling avec tunnel-all DNS activé)
    - Configuration de Split-Incluse (tunnel-all DNS désactivé et no split-DNS)
    - Configuration de l'exclusion partagée (DNS avec tous les tunnels désactivé et pas de DNS divisé)
    - Split-DNS (tunnel-all DNS désactivé, split-include configuré)
  - iPhone
  - Informations de bogue associées
- Informations connexes

Introduction

Ce document décrit comment Cisco OS® gère les requêtes DNS et les effets sur la résolution de noms de domaine avec Cisco AnyConnect et la transmission tunnel partagée ou intégrale.

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.

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

Lorsque vous utilisez la transmission tunnel à inclusion partagée, voici les trois options disponibles pour le système de noms de domaine (DNS) :

1. Split DNS : les requêtes DNS qui correspondent aux noms de domaine sont configurées sur l'appareil de sécurité adaptatif Cisco (ASA). Ils se déplacent dans le tunnel (vers les serveurs DNS qui sont définis sur l'ASA, par exemple) tandis que d'autres ne le font pas.

2. Tunnel-all-DNS - Seul le trafic DNS vers les serveurs DNS qui sont définis par l'ASA est autorisé. Ce paramètre est configuré dans la stratégie de groupe.

3. DNS standard : toutes les requêtes DNS transitent par les serveurs DNS définis par l'ASA. Dans le cas d'une réponse négative, les requêtes DNS peuvent également aller aux serveurs DNS qui sont configurés sur la carte physique.

Remarque : la commande split-tunnel-all-dns a été implémentée pour la première fois dans ASA Version 8.2(5). Avant cette version, vous ne pouviez faire que diviser DNS ou DNS standard.

Dans tous les cas, les requêtes DNS qui sont définies pour se déplacer dans le tunnel, vont à tous les serveurs DNS qui sont définis par ASA. Si aucun serveur DNS n'est défini par l'ASA, les paramètres DNS sont vides pour le tunnel. Si vous n'avez pas de DNS partagé défini, toutes les requêtes DNS sont envoyées aux serveurs DNS qui sont définis par l'ASA. Cependant, les comportements décrits dans ce document peuvent être différents, en fonction du système d'exploitation.

Remarque : évitez d'utiliser NSLookup lorsque vous testez la résolution de noms sur le client. Utilisez plutôt un navigateur ou utilisez la commande ping. Cela est dû au fait que NSLookup ne dépend pas du résolveur DNS du système d'exploitation. AnyConnect ne force pas la requête DNS via une certaine interface, mais l’autorise ou la rejette en fonction de la configuration DNS fractionnée. Afin de forcer le résolveur DNS à essayer un serveur DNS acceptable pour une requête, il est important que le test DNS partagé soit effectué uniquement avec les applications qui s'appuient sur le résolveur DNS natif pour la résolution

---

de noms de domaine (toutes les applications à l'exception de NSLookup, Dig et les applications similaires qui gèrent la résolution DNS par elles-mêmes, par exemple).

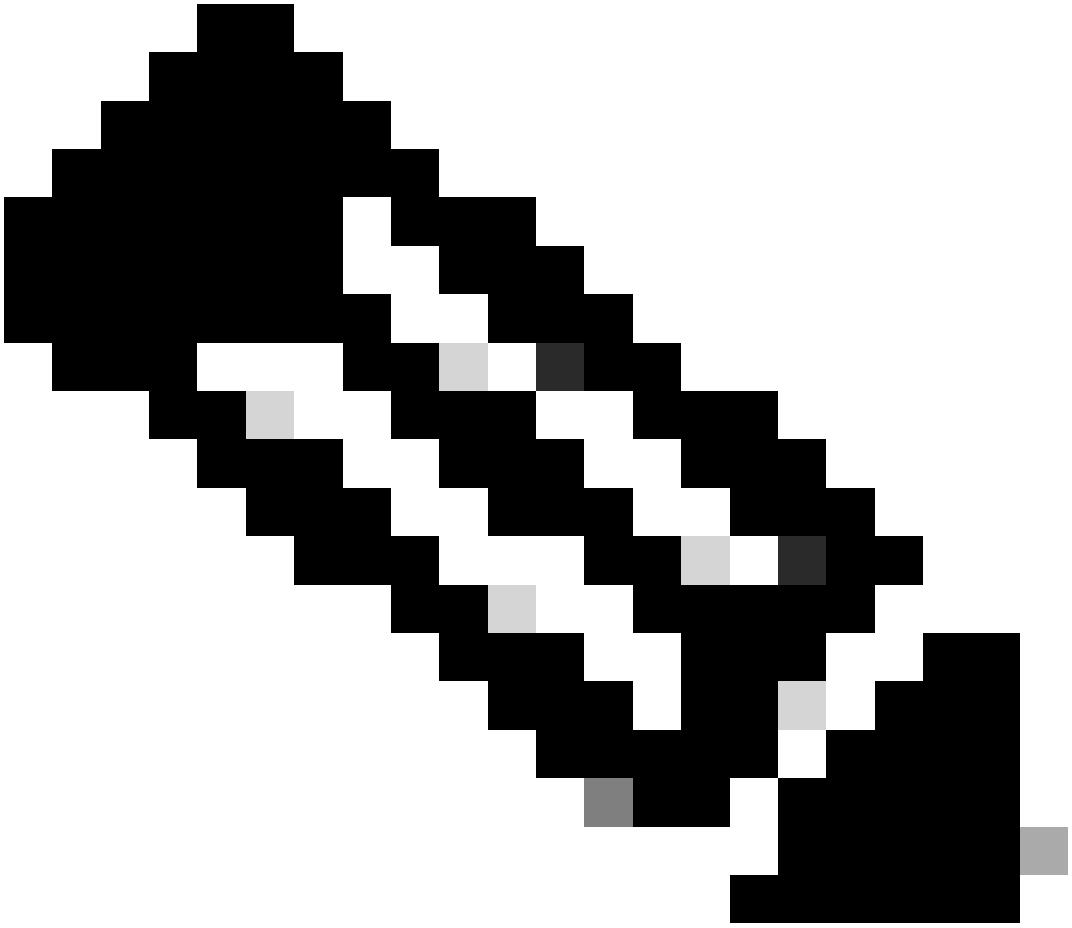
Vrai contre DNS fractionné au mieux

AnyConnect version 2.4 prend en charge le Split DNS Fallback (Best Effort Split DNS), qui n'est pas le véritable DNS partagé et qui se trouve dans le client IPsec hérité. Si la demande correspond à un domaine DNS fractionné, AnyConnect permet à la demande d'être tunnellisée dans l'ASA. Si le serveur ne peut pas résoudre le nom d'hôte, le résolveur DNS continue et envoie la même requête au serveur DNS mappé à l'interface physique.

D'autre part, si la requête ne correspond à aucun des domaines DNS fractionnés, AnyConnect ne le tunnellise pas dans l'ASA. Au lieu de cela, il crée une réponse DNS de sorte que le résolveur DNS revienne et envoie la requête au serveur DNS qui est mappé à l'interface physique. C'est pourquoi cette fonctionnalité n'est pas appelée DNS partagé, mais DNS de secours pour la transmission tunnel partagée. Non seulement AnyConnect garantit que seules les demandes de domaines DNS partagés cibles sont tunnellisées, mais il s'appuie également sur le comportement du résolveur DNS du système d'exploitation client pour la résolution des noms d'hôtes.

Cela pose des problèmes de sécurité en raison d'une fuite potentielle de nom de domaine privé. Par exemple, le client DNS natif peut envoyer une requête pour un nom de domaine privé à un serveur DNS public, en particulier lorsque le serveur de noms DNS VPN ne peut pas résoudre la requête DNS.

Référez-vous à l'ID de bogue Cisco CSCtn14578, actuellement résolu sur Microsoft Windows uniquement, à partir de la version 3.0(4235). La solution met en oeuvre un véritable DNS divisé, elle interroge strictement les noms de domaine configurés qui correspondent et sont autorisés à accéder aux serveurs DNS VPN. Toutes les autres requêtes ne sont autorisées que vers d'autres serveurs DNS, tels que ceux configurés sur la ou les cartes physiques.



Remarque : Seuls les utilisateurs Cisco inscrits ont accès aux renseignements et aux outils internes.

Tunnel-all et Tunnel-all DNS

Lorsque la transmission tunnel partagée est désactivée (la configuration Tunnel-all), le trafic DNS est strictement autorisé via le tunnel. La configuration Tunnel-all DNS (configurée dans la stratégie de groupe) envoie toutes les recherches DNS via le tunnel, ainsi qu'un certain type de tunnellisation partagée, et le trafic DNS est strictement autorisé via le tunnel.

Ceci est cohérent entre les plates-formes avec une mise en garde sur Microsoft Windows : quand un DNS Tunnel-all ou Tunnel-all est configuré, AnyConnect autorise le trafic DNS strictement aux serveurs DNS qui sont configurés sur la passerelle sécurisée (appliquée à l'adaptateur VPN). Il s’agit d’une amélioration de la sécurité mise en oeuvre avec la solution DNS véritablement partagée mentionnée précédemment.

Si cela s'avère problématique dans certains scénarios (par exemple, les demandes de mise à

jour/enregistrement DNS doivent être envoyées à des serveurs DNS non VPN), procédez comme suit :

1. Si la configuration actuelle est Tunnel-all, alors activez le split-exclude tunneling . Tout réseau à hôte unique et à exclusion fractionnée peut être utilisé, par exemple une adresse link-local.

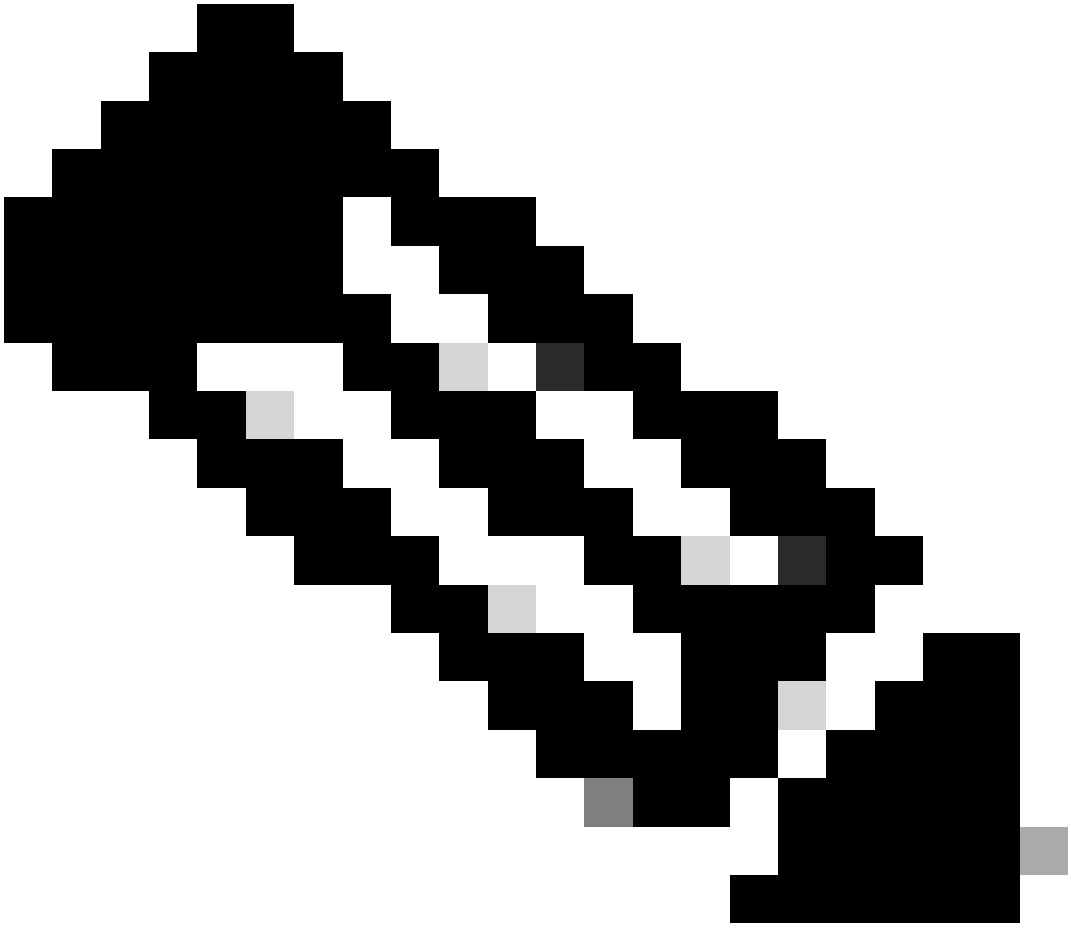
2. Assurez-vous que Tunnel-all DNS n'est pas configuré dans la stratégie de groupe.

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

Ce problème lié à Microsoft Windows est le plus fréquent dans les conditions suivantes :

- Avec la configuration du routeur domestique, les serveurs DNS et DHCP se voient attribuer la même adresse IP (AnyConnect crée une route nécessaire vers le serveur DHCP).
- Un grand nombre de domaines DNS figurent dans la stratégie de groupe.
- Une configuration « Tunnel-all » est utilisée.
- La résolution de noms est effectuée par un nom d'hôte non qualifié, ce qui implique que le résolveur doit essayer un certain nombre de suffixes DNS sur tous les serveurs DNS disponibles jusqu'à ce que celui correspondant au nom d'hôte interrogé soit tenté. Ce problème est dû au client DNS natif qui tente d'envoyer des requêtes DNS via la carte physique, qu'AnyConnect bloque (étant donné la configuration Tunnel-all). Cela entraîne un délai de résolution de nom qui peut être important, en particulier si un grand nombre de suffixes DNS sont poussés par la tête de réseau. Le client DNS doit parcourir toutes les requêtes et tous les serveurs DNS disponibles jusqu'à ce qu'il reçoive une réponse positive.

Ce problème est résolu dans AnyConnect Version 3.0(4235). Référez-vous aux ID de bogue Cisco CSCtq02141 et à l'ID de bogue Cisco CSCtn14578, ainsi qu'à l'introduction à la vraie solution DNS partagée mentionnée précédemment, pour plus d'informations.



Remarque : Seuls les utilisateurs Cisco inscrits ont accès aux renseignements et aux outils internes.

Si une mise à niveau ne peut pas être implémentée, voici les solutions possibles :

- Activez le split-exclude tunneling pour une adresse IP, qui permet aux requêtes DNS locales de circuler à travers la carte physique. Vous pouvez utiliser une adresse du sous-réseau link-local 169.254.0.0/16 car il est peu probable qu'un périphérique envoie du trafic à l'une de ces adresses IP sur le VPN. Une fois que vous avez activé le tunneling split-exclude, activez l'accès au LAN local sur le profil client ou sur le client lui-même, et désactivez Tunnel-all dDNS.

  Sur l'ASA, effectuez les modifications de configuration suivantes :

```
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
```

Sur le profil client, vous devez ajouter cette ligne :

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

Vous pouvez également activer cette option pour chaque client dans l'interface utilisateur graphique du client AnyConnect. Accédez au menu Préférences AnyConnect et cochez la case Activer l'accès au réseau local .

- Utilisez les noms de domaine complets (FQDN) au lieu des noms d'hôtes non qualifiés pour les résolutions de noms.
- Utilisez une adresse IP différente pour le serveur DNS sur l'interface physique.

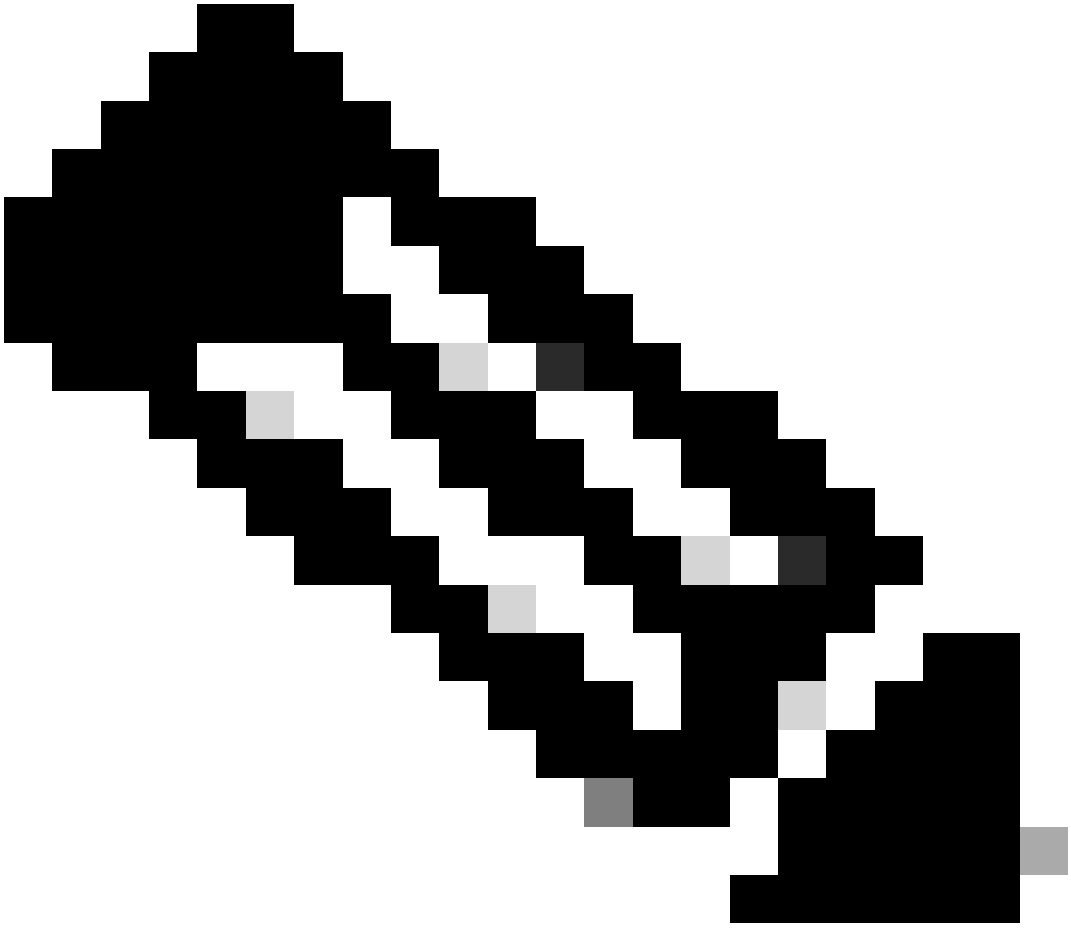
DNS avec split tunneling sur les différents systèmes d'exploitation Cisco

Les différents systèmes d’exploitation Cisco gèrent les recherches DNS de différentes manières lorsqu’ils sont utilisés avec la transmission tunnel partagée (sans DNS divisé) pour AnyConnect. Cette section décrit ces différences.

Microsoft Windows

Sur les systèmes Microsoft Windows, les paramètres DNS sont définis par interface. Si la transmission tunnel partagée est utilisée, les requêtes DNS peuvent revenir aux serveurs DNS de l'adaptateur physique après leur échec sur l'adaptateur de tunnel VPN. Si la transmission tunnel partagée sans DNS partagé est définie, la résolution DNS interne et externe fonctionne car elle revient aux serveurs DNS externes.

Un changement de comportement s'est produit dans le mécanisme DNS qui gère cela sur AnyConnect pour Windows, dans la version 4.2 après le correctif pour l'ID de bogue Cisco CSCuf07885.



Remarque : Seuls les utilisateurs Cisco inscrits ont accès aux renseignements et aux outils internes.

Windows 7+

Configuration de tous les tunnels (et split-tunneling avec tunnel-all DNS activé)

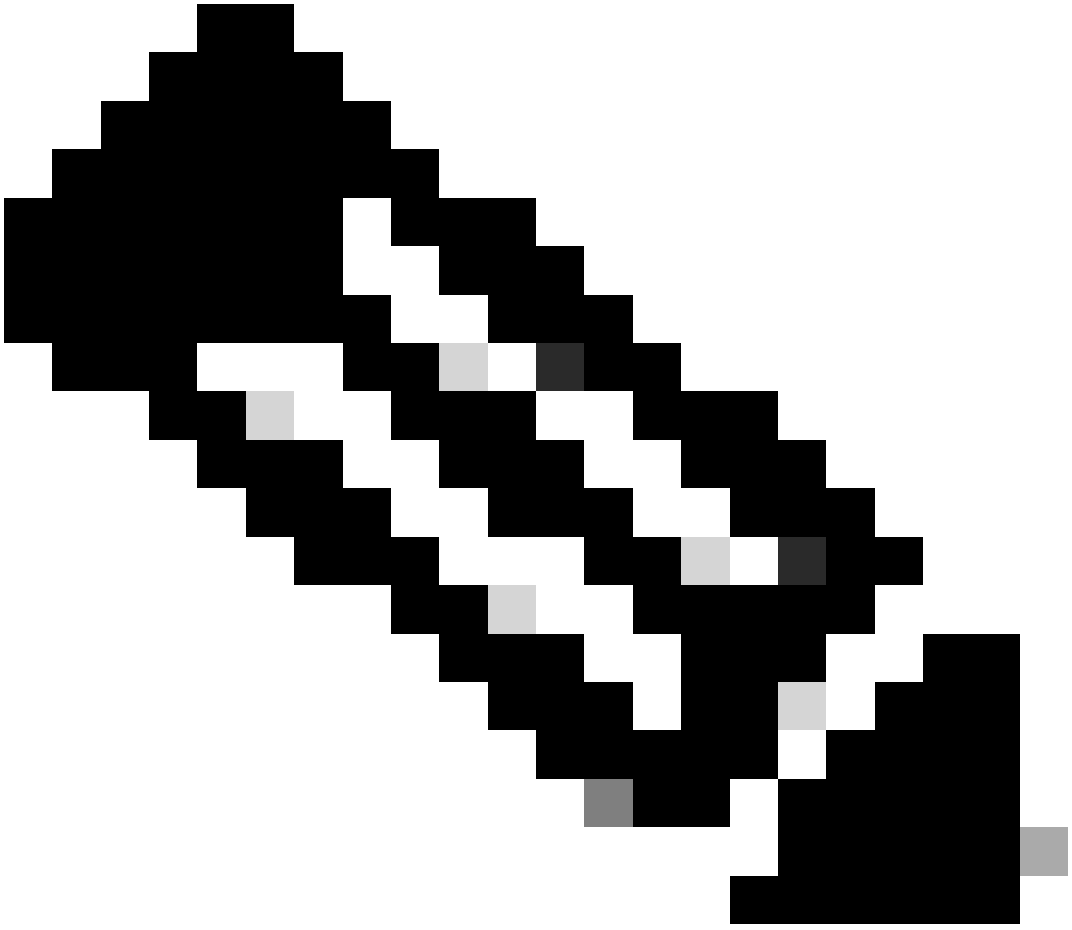
Antérieure à AnyConnect 4.2 :

Seules les requêtes DNS aux serveurs DNS configurés dans la stratégie de groupe (serveurs DNS de tunnel) sont autorisées. Le pilote AnyConnect répond à toutes les autres requêtes par une réponse « no such name ». Par conséquent, la résolution DNS ne peut être effectuée qu'avec les serveurs DNS du tunnel.

AnyConnect 4.2 +

Les requêtes DNS vers n'importe quel serveur DNS sont autorisées, à condition qu'elles proviennent de l'adaptateur VPN et qu'elles soient envoyées via le tunnel. Toutes les autres requêtes reçoivent une réponse sans ce nom, et la résolution DNS ne peut être effectuée que via le tunnel VPN.

Avant la correction du bogue Cisco ID CSCuf07885, AC a restreint les serveurs DNS cibles, mais avec la correction de ce bogue, il restreint désormais les cartes réseau qui peuvent initier des requêtes DNS.



> Remarque : Seuls les utilisateurs Cisco inscrits ont accès aux renseignements et aux outils internes.

Configuration de Split-Incluse (tunnel-all DNS désactivé et no split-DNS)

Le pilote AnyConnect n'interfère pas avec le résolveur DNS natif. Par conséquent, la résolution DNS est effectuée en fonction de l'ordre des cartes réseau, où AnyConnect est toujours la carte préférée lorsque le VPN est connecté. De plus, une requête DNS est d'abord envoyée via le tunnel et si elle n'est pas résolue, le résolveur tente de la résoudre via l'interface publique. La liste d'accès split-include inclut le sous-réseau qui couvre le ou les serveurs DNS du tunnel. Pour commencer avec AnyConnect 4.2, les routes d'hôte pour le ou les serveurs DNS de tunnel sont automatiquement ajoutées en tant que réseaux à inclusion partagée (routes sécurisées) par le client AnyConnect, et par conséquent, la liste d'accès à inclusion partagée ne nécessite plus l'ajout explicite du sous-réseau du serveur DNS de tunnel.

Configuration de l'exclusion partagée (DNS avec tous les tunnels désactivé et pas de DNS divisé)

Le pilote AnyConnect n'interfère pas avec le résolveur DNS natif. Par conséquent, la résolution DNS est effectuée en fonction de l'ordre des cartes réseau, où AnyConnect est toujours la carte préférée lorsque le VPN est connecté. De plus, une requête DNS est d'abord envoyée via le tunnel et si elle n'est pas résolue, le résolveur tente de la résoudre via l'interface publique. La liste de contrôle d'accès split-exclude ne doit pas inclure le sous-réseau qui couvre le ou les serveurs DNS du tunnel. Pour commencer avec AnyConnect 4.2, les routes d'hôte pour le ou les serveurs DNS du tunnel sont automatiquement ajoutées en tant que réseaux à inclusion partagée (routes sécurisées) par le client AnyConnect, et évitent ainsi la mauvaise configuration dans la liste d'accès à exclusion partagée.

Split-DNS (tunnel-all DNS désactivé, split-include configuré)

Pre AnyConnect 4.2

Les requêtes DNS, qui correspondent aux domaines DNS partagés, sont autorisées à tunnelliser les serveurs DNS, mais pas les autres serveurs DNS. Pour éviter que de telles requêtes DNS internes ne sortent du tunnel, le pilote AnyConnect répond par « no such name » si la requête est envoyée à d'autres serveurs DNS. Par conséquent, les domaines split-dns ne peuvent être résolus que via des serveurs DNS de tunnel.

Les requêtes DNS, qui ne correspondent pas aux domaines DNS partagés, sont autorisées vers d'autres serveurs DNS, mais ne sont pas autorisées à tunnelliser les serveurs DNS. Même dans ce cas, le pilote AnyConnect répond par « no such name » si une requête pour des domaines non-split-dns est tentée via un tunnel. Par conséquent, les domaines non split-dns peuvent uniquement être résolus via des serveurs DNS publics en dehors du tunnel.

AnyConnect 4.2 +

Les requêtes DNS, qui correspondent aux domaines de dns partagés, sont autorisées vers tous les serveurs DNS, à condition qu'elles proviennent de l'adaptateur VPN. Si la requête provient de l’interface publique, le pilote AnyConnect répond par un « no such name » pour forcer le résolveur

à toujours utiliser le tunnel pour la résolution de noms. Par conséquent, les domaines split-dns ne peuvent être résolus que par tunnel.

Les requêtes DNS, qui ne correspondent pas aux domaines DNS partagés, sont autorisées vers tous les serveurs DNS tant qu'elles proviennent de la carte physique. Si la requête provient de l'adaptateur VPN, AnyConnect répond par « no such name » pour forcer le résolveur à toujours tenter la résolution de noms via l'interface publique. Par conséquent, les domaines non split-dns ne peuvent être résolus que via une interface publique.

Mac OSx

Sur les systèmes Macintosh, les paramètres DNS sont globaux. Si la transmission tunnel partagée est utilisée, mais que la transmission DNS partagée n'est pas utilisée, les requêtes DNS ne peuvent pas atteindre les serveurs DNS en dehors du tunnel. Vous pouvez résoudre les problèmes uniquement en interne, pas en externe.

Ceci est documenté dans l'ID de bogue Cisco CSCtf20226 et l'ID de bogue Cisco CSCtz86314. Dans les deux cas, cette solution de contournement doit résoudre le problème :

- Spécifiez une adresse IP de serveur DNS externe dans la stratégie de groupe et utilisez un nom de domaine complet pour les requêtes DNS internes.

- Si les noms externes peuvent être résolus via le tunnel, accédez à Advanced > Split Tunneling et désactivez le DNS partagé en supprimant les noms DNS configurés dans la stratégie de groupe. Cela nécessite l'utilisation d'un nom de domaine complet pour les requêtes DNS internes.

Le cas du DNS partagé est résolu dans AnyConnect version 3.1. Cependant, vous devez vous assurer que l'une de ces conditions est remplie :

- Le DNS partagé doit être activé pour les deux protocoles IP, ce qui nécessite Cisco ASA version 9.0 ou ultérieure.

- Le DNS fractionné doit être activé pour un protocole IP. Si vous exécutez Cisco ASA version 9.0 ou ultérieure, utilisez le protocole de contournement client pour l'autre protocole IP. Par exemple, assurez-vous qu'il n'y a pas de pool d'adresses et que le protocole de contournement client est activé dans la stratégie de groupe. Si vous exécutez une version ASA antérieure à la version 9.0, vérifiez qu'aucun pool d'adresses n'est configuré pour l'autre protocole IP. Cela implique que l'autre protocole IP est IPv6.

Remarque : AnyConnect ne modifie pas le fichier resolv.conf sur Macintosh OS X, mais modifie plutôt les paramètres DNS spécifiques à OS X. Macintosh OS X conserve le fichier resolv.conf à jour pour des raisons de compatibilité. Utilisez la commande scutil —dns afin d'afficher les paramètres DNS sur Macintosh OS X.

Configuration de tous les tunnels (et split-tunneling avec tunnel-all DNS activé)

Lorsqu'AnyConnect est connecté, seuls les serveurs DNS de tunnel sont maintenus dans la configuration DNS du système. Par conséquent, les requêtes DNS ne peuvent être envoyées qu'au(x) serveur(s) DNS de tunnel.

Configuration de Split-Incluse (tunnel-all DNS désactivé et no split-DNS)

AnyConnect n'interfère pas avec le résolveur DNS natif. Les serveurs DNS du tunnel sont configurés en tant que résolveurs préférés, qui ont priorité sur les serveurs DNS publics, ce qui garantit que la demande DNS initiale pour une résolution de noms est envoyée sur le tunnel. Comme les paramètres DNS sont globaux sur Mac OS X, il n'est pas possible pour les requêtes DNS d'utiliser des serveurs DNS publics en dehors du tunnel comme documenté dans l'ID de bogue Cisco CSCtf20226 . Pour commencer avec AnyConnect 4.2, les routes d'hôte pour le ou les serveurs DNS de tunnel sont automatiquement ajoutées en tant que réseaux à inclusion partagée (routes sécurisées) par le client AnyConnect, et par conséquent, la liste d'accès à inclusion partagée ne nécessite plus l'ajout explicite du sous-réseau du serveur DNS de tunnel.

Configuration de l'exclusion partagée (DNS avec tous les tunnels désactivé et pas de DNS divisé)

AnyConnect n'interfère pas avec le résolveur DNS natif. Les serveurs DNS du tunnel sont configurés comme résolveurs préférés, ils sont prioritaires sur les serveurs DNS publics, ce qui garantit que la requête DNS initiale pour une résolution de noms est envoyée sur le tunnel. Comme les paramètres DNS sont globaux sur Mac OS X, il n'est pas possible pour les requêtes DNS d'utiliser des serveurs DNS publics en dehors du tunnel comme documenté dans l'ID de bogue Cisco CSCtf20226 . Pour commencer avec AnyConnect 4.2, les routes d'hôte pour le ou les serveurs DNS de tunnel sont automatiquement ajoutées en tant que réseaux à inclusion partagée (routes sécurisées) par le client AnyConnect, et par conséquent, la liste d'accès à inclusion partagée ne nécessite plus l'ajout explicite du sous-réseau du serveur DNS de tunnel.

Split-DNS (tunnel-all DNS désactivé, split-include configuré)

Si le DNS partagé est activé pour les deux protocoles IP (IPv4 et IPv6) ou s'il est activé pour un seul protocole et qu'aucun pool d'adresses n'est configuré pour l'autre protocole :
Un vrai DNS divisé, semblable à Windows, est appliqué. La valeur True split-DNS signifie que les requêtes qui correspondent aux domaines split-DNS sont résolues uniquement via le tunnel, elles ne sont pas transmises aux serveurs DNS en dehors du tunnel.

Si le DNS divisé est activé pour un seul protocole et si une adresse de client est attribuée pour l'autre protocole, seul un DNS de secours pour la tunnellisation divisée est activée. Cela signifie qu'AC autorise uniquement les requêtes DNS qui correspondent aux domaines DNS partagés via un tunnel (les autres requêtes reçoivent une réponse « refusé » de AC pour forcer le basculement

vers les serveurs DNS publics), mais ne peut pas appliquer la requête qui correspond aux domaines DNS partagés qui ne sont pas envoyés en clair, via un adaptateur public.

Linux

Configuration de tous les tunnels (et split-tunneling avec tunnel-all DNS activé)

Lorsqu'AnyConnect est connecté, seuls les serveurs DNS de tunnel sont maintenus dans la configuration DNS du système. Par conséquent, les requêtes DNS ne peuvent être envoyées qu'au(x) serveur(s) DNS de tunnel.

Configuration de Split-Incluse (tunnel-all DNS désactivé et no split-DNS)

AnyConnect n'interfère pas avec le résolveur DNS natif. Les serveurs DNS du tunnel sont configurés en tant que résolveurs préférés, qui ont priorité sur les serveurs DNS publics, ce qui garantit que la demande DNS initiale pour une résolution de noms est envoyée sur le tunnel.

Configuration de l'exclusion partagée (DNS avec tous les tunnels désactivé et pas de DNS divisé)

AnyConnect n'interfère pas avec le résolveur DNS natif. Les serveurs DNS du tunnel sont configurés en tant que résolveurs préférés, qui ont priorité sur les serveurs DNS publics, ce qui garantit que la demande DNS initiale pour une résolution de noms est envoyée sur 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. Cela signifie qu'AC autorise uniquement les requêtes DNS qui correspondent aux domaines DNS partagés via un tunnel (les autres requêtes reçoivent une réponse AC avec une réponse « refusé » pour forcer le basculement vers les serveurs DNS publics), mais ne peut pas appliquer cette requête qui correspond aux domaines DNS partagés qui ne sont pas envoyés en clair, via l'adaptateur public.

iPhone

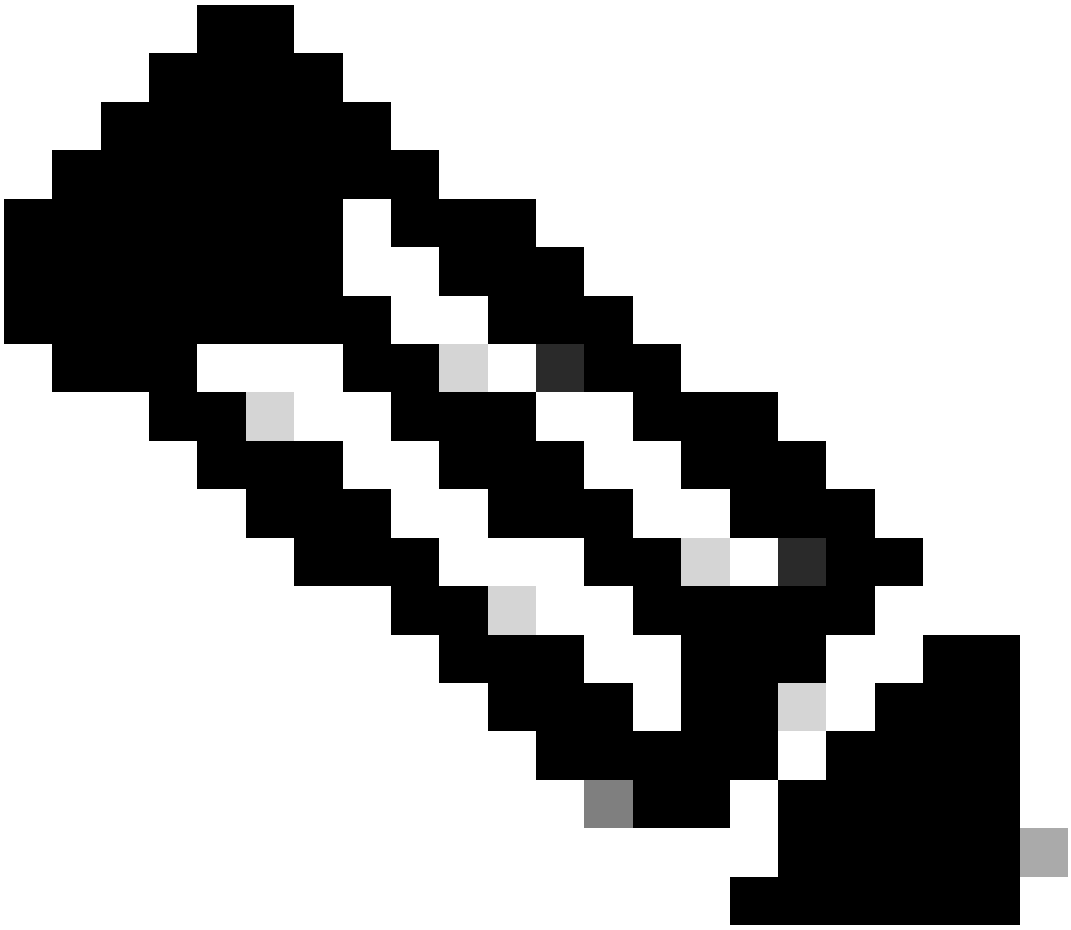
L'iPhone est tout le contraire du système Macintosh et n'est pas similaire à Microsoft Windows. Si la transmission tunnel partagée est définie mais que le DNS partagé n'est pas défini, les requêtes DNS quittent le serveur DNS global qui est défini. Par exemple, les entrées de domaine DNS fractionné sont obligatoires pour la résolution interne. Ce comportement est documenté dans l'ID de bogue Cisco CSCtq09624 et est corrigé dans la version 2.5.4038 pour le client Apple iOS AnyConnect.

Remarque : sachez que les requêtes DNS de l'iPhone ignorent les domaines .local. Ceci est documenté dans l'ID de bogue Cisco CSCts89292. Les ingénieurs Apple confirment que le

---

problème est dû à la fonctionnalité du système d'exploitation. C'est le comportement conçu, et Apple confirme qu'il n'y a pas de changement pour elle.

Informations de bogue associées



Remarque : Seuls les utilisateurs Cisco inscrits ont accès aux renseignements et aux outils internes.

- ID de bogue Cisco CSCsv34395 : ajout de la prise en charge dans AnyConnect pour qui proxie le nom de domaine complet au serveur DHCP
- ID de bogue Cisco CSCtn14578 - AnyConnect pour prendre en charge le véritable DNS fractionné ; pas de secours
- ID de bogue Cisco CSCtq02141 - Problème de DNS AnyConnect lorsque le DNS du FAI se trouve sur le même sous-réseau que l'IP publique

- ID de bogue Cisco CSCtf20226 - Rendre AnyConnect DNS avec le comportement de tunnel partagé pour Mac identique à Windows
- ID de bogue Cisco CSCtz86314 - Mac : les requêtes DNS n'ont pas été envoyées par erreur via le tunnel avec le DNS partagé
- ID de bogue Cisco CSCtq09624 - Rendre AnyConnect iPhone DNS avec le comportement de transmission tunnel partagée identique à Windows
- ID de bogue Cisco CSCts89292 - AC pour les requêtes DNS iPhone ignorent les domaines .local

Informations connexes

- Cisco IOS® Firewall
- 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.