Différences comportementales concernant des requêtes DNS et résolution de nom de domaine dans différents systèmes d'exploitation

Contenu

Introduction

Ce document décrit comment différentes requêtes de Système de noms de domaine (DNS) de traitement de systèmes d'exploitation (systèmes d'exploitation) et les affects sur la résolution de nom de domaine avec le Cisco AnyConnect et le Tunnellisation fendu ou plein.

Fractionnement contre les DN standard

Quand vous utilisez fractionnement-incluez le Tunnellisation, là sont trois options pour des DN :

1. **DN fendus** - Les requêtes DNS qui apparie les noms de domaine, sont configurées sur l'appliance de sécurité adaptable Cisco (ASA). Ils se déplacent par le tunnel (aux serveurs DNS qui sont définis sur l'ASA, par exemple) alors que d'autres ne font pas.

2. On permet à trafic DNS réservé de Tunnel-tout-**DN aux** serveurs DNS qui sont définis par l'ASA. Cette configuration est configurée dans la stratégie de groupe.

3. **DN standard** - Toutes les requêtes DNS se déplacent par les serveurs DNS qui sont définis par l'ASA. Dans le cas d'une réponse négative, les requêtes DNS pourraient également aller aux serveurs DNS qui sont configurés sur l'adaptateur physique.

   Note: La commande de fractionnement-tunnel-tout-**dn** a été mise en application la première fois dans la version 8.2(5) ASA. Avant cette version, vous pourriez seulement faire les DN fendus ou les DN standard.

Dans des tous les cas, les requêtes DNS qui sont définies pour se déplacer par le tunnel, vont à tous les serveurs DNS qui sont définis par ASA. S'il n'y a aucun serveur DNS défini par l'ASA, alors les configurations de DN sont vides pour le tunnel. Si vous n'avez pas séparé des DN définis, alors toutes les requêtes DNS sont envoyées aux serveurs DNS qui sont définis par l'ASA. Cependant, les comportements qui sont décrits dans ce document peuvent être différents, selon le système d'exploitation (SYSTÈME D'EXPLOITATION).

Note: Évitez l'utilisation du NSLookup quand vous testez la résolution de noms sur le client. Au lieu de cela, comptez sur un navigateur ou utilisez la **commande ping**. C'est parce que NSLookup ne se fonde pas sur le résolveur de DN de SYSTÈME D'EXPLOITATION. AnyConnect ne force pas la demande de DN par l'intermédiaire d'une certaine interface mais la permet ou la rejette dépendante sur la configuration DNS fendue. Afin de forcer le résolveur de DN à juger un serveur DNS acceptable pour une demande, il est important que l'essai fendu de DN soit seulement réalisé avec les applications qui se fondent sur le résolveur indigène de DN pour la résolution de nom de domaine (toutes les applications excepté NSLookup, fouille, et applications semblables qui traitent la résolution de DN seuls, par exemple).

Rectifiez contre les DN fendus de meilleur effort

La version 2.4 d'AnyConnect prend en charge le retour fendu de DN (DN fendus de meilleur effort), qui n'est pas les véritables DN fendus et est trouvé dans le client existant d'IPsec. Si la demande apparie un domaine fendu de DN, AnyConnect permet la demande d'être percé un tunnel dans l'ASA. Si le serveur ne peut pas résoudre le nom d'hôte, le résolveur de DN continue et envoie la même requête au serveur DNS qui est tracé à l'interface physique.

D'autre part, si la demande n'apparie pas les domaines fendus l'uns des de DN, AnyConnect ne la perce pas un tunnel dans l'ASA. Au lieu de cela, il établit une réponse de DN de sorte que le résolveur de DN tombe de retour et envoie la requête au serveur DNS qui est tracé à l'interface physique. C'est pourquoi cette caractéristique ne s'appelle pas split DNS, mais retour de DN pour la Segmentation de tunnel. Non seulement AnyConnect s'assure-t-il que seulement des demandes qui visent les domaines fendus de DN sont percées un tunnel dedans, il compte également sur le comportement de résolveur de DN de SYSTÈME D'EXPLOITATION de client pour la résolution de noms d'hôte.

Ceci soulève des problèmes de sécurité dus à une fuite privée potentielle de nom de domaine. Par exemple, le client DNS indigène peut envoyer une requête pour un nom de domaine privé à

un serveur DNS public spécifiquement quand le serveur de nom DNS VPN ne pourrait pas résoudre la requête DNS.

*Référez-vous à l'*ID de bogue Cisco CSCtn14578, actuellement résolu sur Microsoft Windows seulement, en date de la version 3.0(4235). La solution implémente de véritables DN fendus, elle questionne strictement les noms de domaine configurés qu'on permet des correspondances et aux serveurs DNS VPN. On permet seulement toutes autres requêtes à d'autres serveurs DNS, comme ceux configurés sur les adaptateurs physiques.

Percez un tunnel tous et percez un tunnel tous les DN

Quand la Segmentation de tunnel est désactivée (le **tunnel toute la** configuration), on permet strictement le trafic DNS par l'intermédiaire du tunnel. On permet strictement le **tunnel que toute la configuration DNS** (configurée dans la stratégie de groupe) envoie tous les DN à des consultations par le tunnel, avec un certain type de Segmentation de tunnel, et trafic DNS par l'intermédiaire du tunnel.

C'est compatible à travers des Plateformes à une mise en garde sur Microsoft Windows : quand n'importe quel **tunnel tout** ou **percent un tunnel tous les DN** est configuré, AnyConnect permet le trafic DNS strictement aux serveurs DNS qui sont configurés sur la passerelle sécurisée (appliquée à l'adaptateur VPN). C'est une amélioration de la sécurité mise en application avec la véritable solution fendue précédemment mentionnée de DN.

Si ceci prouve problématique dans certains scénarios (par exemple, la mise à jour de DN/demandes d'enregistrement doit être envoyée aux serveurs DNS non-VPN), alors terminez-vous ces étapes :

1. Si la configuration en cours est **tunnel tout**, alors l'enable fractionnement-**excluent le Tunnellisation**. N'importe quel seul hôte, fractionnement-excluent le réseau est acceptable pour l'usage, tel qu'une adresse locale à la liaison.

2. Assurez-vous que le **tunnel tous les DN** n'est pas configuré dans la stratégie de groupe.

Problème de performance de DN résolu dans la version 3.0(4235) d'AnyConnect

Cette question de Microsoft Windows est en grande partie de dessous répandu ces conditions :

- Avec l'installation de routeur domestique, les DN et les serveurs DHCP sont assignés la même adresse IP (AnyConnect crée une artère nécessaire au serveur DHCP).

- Un grand nombre de domaines de DN sont dans la stratégie de groupe.

- **Une Tunnel-toute** configuration est utilisée.

- La résolution de noms est exécutée par un nom d'hôte non-qualifié, qui implique que le résolveur doit essayer un certain nombre de suffixes de DN sur tous les serveurs DNS disponibles jusqu'à ce que celui concernant le nom d'hôte questionné soit tenté.

Cette question est due au client DNS indigène qui tente d'envoyer des requêtes DNS par

l'intermédiaire de l'adaptateur physique, qu'AnyConnect bloque (donné la tunnel-**toute** configuration). Ceci mène à un retard de résolution de noms qui peut être significatif, particulièrement si un grand nombre de suffixes de DN sont poussés par le headend. Le client DNS doit marcher par tous les requêtes et serveurs DNS disponibles jusqu'à ce qu'il reçoive une réaction favorable.

Ce problème est résolu dans la version 3.0(4235) d'AnyConnect. Mettez en référence les id CSCtq02141 et CSCtn14578 de bogue Cisco, avec l'introduction à la véritable solution fendue précédent-mentionnée de DN, pour en savoir plus.

Si une mise à jour ne peut pas être mise en application, alors ce sont les contournements possibles :

- L'enable fractionnement-**excluent le Tunnellisation** pour une adresse IP, qui permet les demandes locales de DN de traverser l'adaptateur physique. Vous pouvez utiliser une adresse du sous-réseau linklocal **169.254.0.0/16** parce qu'il est peu probable que n'importe quel périphérique envoie le trafic à une de ces adresses IP au-dessus du VPN. Après que vous activiez le **Tunnellisation de fractionnement-exclure**, activez l'accès local au LAN sur le profil de client ou sur le client lui-même, et désactivez le **tunnel tous les DN**.

  Sur l'ASA, apportez ces modifications de configuration :

  ```
  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 de client, vous devez ajouter cette ligne :

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

  Vous pouvez également activer ceci sur une base de par-client dans le GUI de client d'AnyConnect. Naviguez vers le **menu préférences d'AnyConnect**, et vérifiez la case d'**accès local au LAN d'enable**.

- Utilisez les noms de domaine complet (FQDN) au lieu des noms d'hôte sans réserve pour les résolutions de noms.

- Utilisez une adresse IP différente pour le serveur DNS sur l'interface physique.

DN avec la Segmentation de tunnel sur différents systèmes d'exploitation

Différentes recherches de DN de traitement de systèmes d'exploitation dans différentes manières une fois utilisé avec la Segmentation de tunnel (sans DN fendus) pour AnyConnect. Cette section décrit ces différences.

Microsoft Windows

Sur des systèmes de Microsoft Windows, les configurations de DN sont par-interface. Si la Segmentation de tunnel est utilisée, les requêtes DNS peuvent retomber aux serveurs DNS physiques d'adaptateur après qu'elles échouent sur l'adaptateur de tunnel VPN. Si la Segmentation de tunnel sans DN fendus est définie, alors la résolution interne et externe de DN fonctionne parce qu'elle retombe aux serveurs DNS externes.

Il y a eu un changement du comportement dans le mécanisme de manipulation de DN sur AnyConnect pour Windows, dans la version 4.2 après la difficulté pour CSCuf07885.

Windows 7+

Tunnel-toute configuration (et Segmentation de tunnel avec tunnel-tous DN activés)

Pré AnyConnect 4.2 :

On permet seulement des demandes de DN aux serveurs DNS configurés dans le cadre de la stratégie de groupe (serveurs DNS de tunnel). Le gestionnaire d'AnyConnect répond à toutes autres demandes avec une réponse de « aucun un tel nom ». En conséquence, la résolution de DN peut seulement être exécutée utilisant les serveurs DNS de tunnel.

AnyConnect 4.2 +

On permet des demandes de DN à tous les serveurs DNS, tant que elles sont provenues de l'adaptateur VPN et sont envoyées à travers le tunnel. Toutes autres demandes sont répondues avec la réponse de « aucun un tel nom », et la résolution de DN peut seulement être exécutée par l'intermédiaire du tunnel VPN

Avant la difficulté CSCuf07885, le courant alternatif limite les serveurs DNS de cible, toutefois avec la difficulté pour CSCuf07885, il limite quels adaptateurs réseau peuvent initier des demandes de DN.

Fractionnement-incluez la configuration (tunnel-tous DN désactivés et aucun split-dns)

Le gestionnaire d'AnyConnect ne gêne pas le résolveur indigène de DN. Par conséquent, les DN que la résolution est exécutée ont basé sur l'ordre des adaptateurs réseau où AnyConnect est toujours l'adaptateur préféré quand le VPN est connecté. D'ailleurs, une requête DNS est d'abord envoyée par l'intermédiaire du tunnel et si elle n'obtient pas résolu, des tentatives de résolveur de la résoudre par l'intermédiaire de l'interface publique. L'access-list includes de fractionnement-inclure le sous-réseau qui couvre les serveurs de DN de tunnel. Pour démarrer avec AnyConnect 4.2, des routes hôte pour les serveurs de DN de tunnel sont automatiquement ajoutées comme fractionnement-incluent des réseaux (sécurisez les artères) par le client d'AnyConnect, et donc la liste d'accès de fractionnement-inclure n'exige plus l'ajout explicite du sous-réseau de serveur DNS de tunnel.

Fractionnement-excluez la configuration (tunnel-tous DN désactivés et aucun split-dns)

Le gestionnaire d'AnyConnect ne gêne pas le résolveur indigène de DN. Par conséquent, les DN que la résolution est exécutée ont basé sur l'ordre des adaptateurs réseau où AnyConnect est toujours l'adaptateur préféré quand le VPN est connecté. D'ailleurs, une requête DNS est d'abord envoyée par l'intermédiaire du tunnel et si elle n'obtient pas résolu, des tentatives de résolveur de la résoudre par l'intermédiaire de l'interface publique. La liste d'accès de fractionnement-exclure ne devrait pas inclure le sous-réseau couvrant les serveurs de DN de tunnel. Pour démarrer avec AnyConnect 4.2, des routes hôte pour les serveurs de DN de tunnel sont automatiquement ajoutées comme fractionnement-incluent des réseaux (sécurisez les artères) par le client d'AnyConnect, et empêchent donc la mauvaise configuration dans la liste d'accès de fractionnement-exclure.

Split-dns (tunnel-tous DN désactivés, fractionnement-incluent configuré)

Pré AnyConnect 4.2

Des demandes de DN, qui s'assortit avec les domaines de split-dns sont permises de percer un tunnel des serveurs DNS, mais ne sont pas permises à d'autres serveurs DNS. Pour empêcher de telles requêtes DNS internes de couler le tunnel, le gestionnaire d'AnyConnect répond avec « aucun un tel nom » si la requête est envoyée à d'autres serveurs DNS. Par conséquent, les domaines de split-dns peuvent seulement être résolus par l'intermédiaire des serveurs DNS de tunnel.

Des demandes de DN, qui ne s'assortit pas avec les domaines de split-dns sont permises à d'autres serveurs DNS, mais ne sont pas permises pour percer un tunnel des serveurs DNS. Même dans ce cas, le gestionnaire d'AnyConnect répond avec « aucun un tel nom » si une requête pour non des domaines de split-dns est tentée par l'intermédiaire du tunnel. Par conséquent, non les domaines de split-dns peuvent seulement être résolus par l'intermédiaire des serveurs DNS publics en dehors du tunnel.

AnyConnect 4.2 +

On permet des demandes de DN, qui s'assortit avec les domaines de split-dns à tous les serveurs DNS, tant que elles proviennent de l'adaptateur VPN. Si la requête est lancée par l'interface publique, le gestionnaire d'AnyConnect répond avec un « aucun tel nom » pour forcer le résolveur pour utiliser toujours le tunnel pour la résolution de noms. Par conséquent, les domaines de split-dns peuvent seulement être résolus par l'intermédiaire du tunnel.

On permet des demandes de DN, qui ne s'assortit pas avec les domaines de split-dns à tous les serveurs DNS tant que elles proviennent de l'adaptateur physique. Si la requête est lancée par l'adaptateur VPN, AnyConnect répond avec « aucun un tel nom » pour forcer le résolveur pour tenter toujours la résolution de noms par l'intermédiaire de l'interface publique. Par conséquent, non les domaines de split-dns peuvent seulement être résolus par l'intermédiaire de l'interface publique.

MAC OSx

Sur des systèmes macintoshs, les configurations de DN sont globales. Si la Segmentation de

tunnel est utilisée, mais des DN de fractionnement n'est pas utilisés, il n'est pas possible que les requêtes DNS atteignent des serveurs DNS en dehors de du tunnel. Vous pouvez seulement résoudre intérieurement, pas extérieurement.

Ceci est documenté dans les id CSCtf20226 et CSCtz86314 de bogue Cisco. Dans des les deux cas, ce contournement devrait résoudre le problème :

- Spécifiez une adresse IP externe de serveur DNS dans le cadre de la stratégie de groupe et utilisez un FQDN pour les requêtes DNS internes.

- Si les noms externes sont résolubles par le tunnel, alors naviguez vers **avancé > Segmentation de tunnel** et désactivez les DN fendus par l'intermédiaire de la suppression des noms DNS qui sont configurés dans la stratégie de groupe. Ceci exige l'utilisation d'un FQDN pour les requêtes DNS internes.

La caisse fendue de DN est résolue dans la version 3.1 d'AnyConnect. Cependant, vous devez s'assurer qu'une de ces conditions est remplie :

- Des DN fendus doivent être activés pour les deux protocoles IP, qui exige la version 9.0 ou ultérieures de Cisco ASA.

- Des DN fendus doivent être activés pour un protocole IP. Si vous exécutez la version 9.0 ou ultérieures de Cisco ASA, alors utilisez le protocole de contournement de client pour l'autre protocole IP. Par exemple, assurez-vous qu'il n'y a aucun pool d'adresses et que le **contournement Protocol de client** est activé dans la stratégie de groupe. Alternativement, si vous exécutez une version ASA qui est plus tôt que la version 9.0, assurez-vous qu'il n'y a aucun pool d'adresses configuré pour l'autre protocole IP. Ceci implique que l'autre protocole IP est IPv6.

> **Note**: AnyConnect ne change pas le **fichier resolv.conf** sur l'OS X de Macintosh, mais change plutôt des configurations de DN de X-particularité de SYSTÈME D'EXPLOITATION. L'OS X de Macintosh tient le resolv.conffile à jour pour des raisons de compatibilité. Utilisez le scutil**--les dn commandent** afin de visualiser les configurations de DN sur l'OS X de Macintosh.

Tunnel-toute configuration (et Segmentation de tunnel avec tunnel-tous DN activés)

Quand AnyConnect est connecté, seulement des serveurs DNS de tunnel sont mis à jour dans la configuration DNS de système, et donc des demandes de DN peut seulement être envoyé aux serveurs de DN de tunnel.

Fractionnement-incluez la configuration (tunnel-tous DN désactivés et aucun split-dns)

AnyConnect ne gêne pas le résolveur indigène de DN. Les serveurs DNS de tunnel sont configurés en tant que résolveurs préférés, qui a la priorité au-dessus des serveurs DNS publics, ainsi il s'assure que la demande initiale de DN d'une résolution de noms est envoyée au-dessus du tunnel. Puisque les configurations de DN sont globales sur le Mac OS X, il n'est pas possible que les requêtes DNS utilisent les serveurs DNS publics en dehors du tunnel comme documenté dans CSCtf20226. Pour démarrer avec AnyConnect 4.2, des routes hôte pour les serveurs de DN

de tunnel sont automatiquement ajoutées comme fractionnement-incluent des réseaux (sécurisez les artères) par le client d'AnyConnect, et donc la liste d'accès de fractionnement-inclure n'exige plus l'ajout explicite du sous-réseau de serveur DNS de tunnel.

Fractionnement-excluez la configuration (tunnel-tous DN désactivés et aucun split-dns)

AnyConnect ne gêne pas le résolveur indigène de DN. Les serveurs DNS de tunnel sont configurés pendant que les résolveurs préférés, ayant la priorité au-dessus des serveurs DNS publics, ainsi elle s'assure que la demande initiale de DN d'une résolution de noms est envoyée au-dessus du tunnel. Puisque les configurations de DN sont globales sur le Mac OS X, il n'est pas possible que les requêtes DNS utilisent les serveurs DNS publics en dehors du tunnel comme documenté dans CSCtf20226. Pour démarrer avec AnyConnect 4.2, des routes hôte pour les serveurs de DN de tunnel sont automatiquement ajoutées comme fractionnement-incluent des réseaux (sécurisez les artères) par le client d'AnyConnect, et donc la liste d'accès de fractionnement-inclure n'exige plus l'ajout explicite du sous-réseau de serveur DNS de tunnel.

Split-dns (tunnel-tous DN désactivés, fractionnement-incluent configuré)

Si le split-dns est activé pour les deux ipv4 et IPv6) de protocoles IP (ou il est seulement activé pour un protocole et il n'y a aucun pool d'adresses configuré pour l'autre protocole :
Le split-dns vrai, semblable à Windows, est imposé. Le split-dns vrai signifie cette demande que des correspondances avec les domaines de split-dns sont seulement résolu par l'intermédiaire du tunnel, ils n'est pas coulé aux serveurs DNS en dehors du tunnel.

Si le split-dns est activé pour seulement un protocole et une adresse du client est assignée pour l'autre protocole, seulement le **retour de DN pour la Segmentation de tunnel** est imposé. Ceci signifie que le courant alternatif permet seulement la demande de DN qui apparie les domaines de split-dns par l'intermédiaire du tunnel (d'autres demandes sont répondues par courant alternatif avec la réponse « refusée » de forcer le Basculement aux serveurs DNS publics), mais ne peut pas imposer la demande qui s'assortit avec les domaines de split-dns qui ne sont pas envoyés en clair, par l'intermédiaire de l'adaptateur public.

Linux

Tunnel-toute configuration (et Segmentation de tunnel avec tunnel-tous DN activés)

Quand AnyConnect est connecté, seulement des serveurs DNS de tunnel sont mis à jour dans la configuration DNS de système, et donc des demandes de DN peut seulement être envoyé aux serveurs de DN de tunnel.

Fractionnement-incluez la configuration (tunnel-tous DN désactivés et aucun split-dns)

AnyConnect ne gêne pas le résolveur indigène de DN. Les serveurs DNS de tunnel sont configurés en tant que résolveurs préférés, qui a la priorité au-dessus des serveurs DNS publics, ainsi il s'assure que la demande initiale de DN d'une résolution de noms est envoyée au-dessus du tunnel.

Fractionnement-excluez la configuration (tunnel-tous DN désactivés et aucun split-dns)

AnyConnect ne gêne pas le résolveur indigène de DN. Les serveurs DNS de tunnel sont configurés en tant que résolveurs préférés, qui a la priorité au-dessus des serveurs DNS publics, ainsi il s'assure que la demande initiale de DN d'une résolution de noms est envoyée au-dessus du tunnel.

Split-dns (tunnel-tous DN désactivés, fractionnement-incluent configuré)

Si le split-dns est activé, seulement le **retour de DN pour la Segmentation de tunnel** est imposé. Ceci signifie que le courant alternatif permet seulement la demande de DN qui s'assortit avec les domaines de split-dns par l'intermédiaire du tunnel (d'autres demandes sont répondues par courant alternatif avec la réponse « refusée » de forcer le Basculement aux serveurs DNS publics), mais ne peut pas imposer cette demande qui s'assortit avec les domaines de split-dns qui ne sont pas envoyés en clair, par l'intermédiaire de l'adaptateur public.

iPhone

L'iPhone est l'opposé complet du système macintosh et n'est pas semblable à Microsoft Windows. Si la Segmentation de tunnel est définie mais des DN séparés n'est pas définis, alors les requêtes DNS quittent par le serveur DNS global qui est défini. Par exemple, les entrées fendues de domaine de DN sont obligatoires pour la résolution interne. Ce comportement est documenté dans l'ID de bogue Cisco CSCtq09624 et est réparé dans la version 2.5.4038 pour le client IOS AnyConnect d'Apple.

> **Note**: Rendez-vous compte que les requêtes DNS d'iPhone ignorent des **domaines .local**. Ceci est documenté dans l'ID de bogue Cisco CSCts89292. Les ingénieurs d'Apple confirment que la question est provoqué par par la fonctionnalité du SYSTÈME D'EXPLOITATION. C'est le comportement conçu, et Apple confirme là n'est aucune modification pour elle.

Informations connexes

- CSCsv34395 - Ajoutez le support dans AnyConnect pour proxying le FQDN au serveur DHCP
- CSCtn14578 - AnyConnect pour prendre en charge de véritables DN fendus ; pas retour
- CSCtq02141 - Question de DN d'AnyConnect quand les DNSs du FAI est sur le même sous-réseau que l'IP de public
- CSCtn14578 - AnyConnect pour prendre en charge de véritables DN fendus ; pas retour
- CSCtf20226 - Faites à des DN d'AnyConnect avec le comportement de tunnel partagé pour le MAC mêmes que des fenêtres

- CSCtz86314 - MAC : Requêtes DNS inexactement non envoyées par l'intermédiaire du tunnel avec les DN fendus
- CSCtq09624 - Faites à des DN d'iPhone d'AnyConnect avec le comportement de Segmentation de tunnel mêmes que Windows
- CSCts89292 - Le courant alternatif pour des requêtes DNS d'iPhone ignorent des domaines .local
- Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems