Contenu

Introduction

Ce document décrit certaines des limites en cours et les contournements disponibles pour faire AnyConnect et le client d'itinérance d'OpenDNS travaillent ensemble.

Conditions préalables

Connaissances pratiques du client d'itinérance d'AnyConnect et d'OpenDNS.

Connaissance de configuration de headend ASA ou IOS/IOS-XE (groupe de tunnels/stratégie de groupe) pour AnyConnect VPN.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Headend ASA ou IOS/IOS-XE
- Point final exécutant le client d'itinérance de client vpn et d'OpenDNS d'AnyConnect

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 9.4 courante de headend ASA
- Windows 7
- Client 4.2.00096 d'AnyConnect
- Client 2.0.154 d'itinérance d'OpenDNS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

OpenDNS développe un module d'extension d'AnyConnect avec l'équipe de Cisco AnyConnect pour être disponible à l'avenir. Tandis qu'aucune date n'a été fixée, cette intégration permettra au client d'itinérance pour fonctionner avec le client d'AnyConnect sans contournements adressés. Ceci permettra également à AnyConnect d'être un mécanisme de mise en oeuvre pour le client d'itinérance.

Fonctionnalité

Manipulation de DN d'AnyConnect

Le headend VPN peut être configuré de différentes manières d'un couple de traiter le trafic du client d'AnyConnect.

1. Pleine configuration de tunnel (tunnel-toute) : Ceci force tout le trafic du point final à envoyer à travers le tunnel VPN chiffré, et donc le trafic ne laisse jamais l'adaptateur d'interface publique en texte clair
2. Configuration de tunnel partagé :

   a. Fractionnement-incluez le Tunnellisation : Le trafic a destiné seulement aux sous-réseaux spécifiques ou des hôtes définis sur le headend VPN est envoyés à travers le tunnel, tout autre trafic est envoyés en dehors du tunnel en texte clair

   b. Fractionnement-excluez le Tunnellisation : Le trafic a destiné seulement aux sous-réseaux spécifiques ou des hôtes définis sur le headend VPN est exclus du cryptage et part de l'interface publique en texte clair, tout autre trafic est chiffré et seulement envoyé à travers le tunnel

Chacune de ces configurations détermine comment la résolution de DN est traitée par le client d'AnyConnect, selon le système d'exploitation sur le point final. 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, et AnyConnect est toujours l'adaptateur préféré quand le VPN est connecté. Ainsi une requête DNS sera d'abord envoyée par l'intermédiaire du tunnel et s'il n'obtient pas résolu, le résolveur tentera de le résoudre par l'intermédiaire de l'interface publique. La liste d'accès de fractionnement-inclure devra inclure le sous-réseau couvrant les serveurs de DN de tunnel. Commençant par 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, et AnyConnect est toujours l'adaptateur préféré quand le VPN est connecté. Ainsi une requête DNS sera d'abord envoyée par l'intermédiaire du tunnel et s'il n'obtient pas résolu, le résolveur tentera de le 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. Commençant par AnyConnect 4.2, des routes hôte pour les serveurs de DN de tunnel sont automatiquement ajoutées comme fractionnement-incluent les réseaux (sécurisez les artères) par le client d'AnyConnect, et donc qui empêchera 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 appariant les domaines de split-dns sont permises pour 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. Ainsi des domaines de split-dns peuvent seulement être résolus par l'intermédiaire des serveurs DNS de tunnel.

Les DN demande ne pas apparier le split-dns on permet que des domaines à d'autres serveurs DNS, mais non laissé 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. Tellement non des 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 appariant 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. Ainsi des domaines de split-dns peuvent seulement être résolus par l'intermédiaire du tunnel.

Les DN demande ne pas apparier le split-dns que des domaines sont permis à tous les serveurs DNS tant que ils 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. Tellement non des domaines de split-dns peuvent seulement être résolus par l'intermédiaire de l'interface publique.

Mac OS X

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, ayant la priorité au-dessus des serveurs DNS publics, de ce fait s'assurant 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. Commençant par 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 en tant que résolveurs préférés, ayant la priorité au-dessus des serveurs DNS publics, de ce fait s'assurant 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. Commençant par 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 que des demandes appariant les domaines de split-dns sont seulement résolues 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 des demandes de DN appariant 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 que des demandes appariant des domaines de split-dns ne soient pas envoyées 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, ayant la priorité au-dessus des serveurs DNS publics, de ce fait s'assurant 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, ayant la priorité au-dessus des serveurs DNS publics, de ce fait s'assurant 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 des demandes de DN appariant 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 que des demandes appariant des domaines de split-dns ne soient pas envoyées en clair, par l'intermédiaire de l'adaptateur public.

Client d'itinérance d'OpenDNS

Le client d'itinérance est un composant logiciel qui gère des services DNS sur le point final, et utilise les serveurs DNS publics d'OpenDNS pour sécuriser et chiffrer le trafic DNS.

Dans le meilleur des cas, le client devrait être dans un état protégé et chiffré. Cependant, si le client ne peut pas établir une session de TLS avec le serveur public de résolveur d'OpenDNS (208.67.222.222), il tente d'envoyer le trafic DNS décrypté sur le port UDP 53 à 208.67.222.222. Le client d'itinérance utilise exclusivement l'adresse IP publique 208.67.222.222 du résolveur d'OpenDNS (il y a quelques autres tel que 208.67.220.220, 208.67.222.220, et 208.67.220.222). Le client d'itinérance une fois installé, place 127.0.0.1 (localhost) en tant que serveur DNS local et ignore les configurations en cours de DN de par-interface. Des configurations en cours de DN sont enregistrées dans des fichiers locaux resolv.conf (même sur Windows) dans le répertoire de configuration de client d'itinérance. OpenDNS de sauvegarde même ces serveurs DNS qui sont appris par l'intermédiaire de l'adaptateur d'AnyConnect. Par exemple, si 192.168.92.2 est le serveur DNS sur l'adaptateur public, OpenDNS créera le resolv.conf à l'emplacement suivant :

```
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
nameserver 192.168.92.2
```

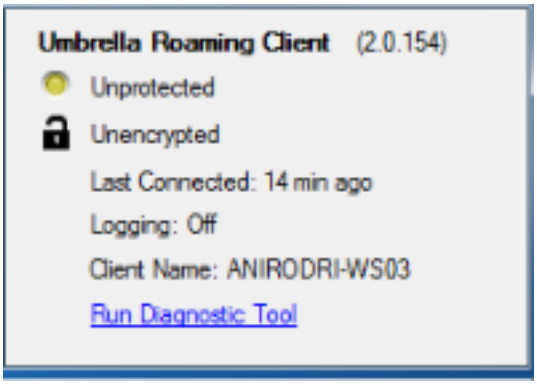
Le client d'itinérance chiffrera chaque paquet réglé à OpenDNS ; cependant, il ne met pas en marche ou utilise un tunnel de chiffrement à 208.67.222.222. Le client d'itinérance a une

caractéristique facultative d'application de couche IP qui ouvrira une connexion d'IPSec pour que les dn non-bloquent des adresses IP. Ceci désactivera automatiquement en présence d'une connexion active d'AnyConnect. Il lie également à 127.0.0.1:53 pour recevoir des requêtes localement générées sur l'ordinateur. Quand le point final doit résoudre un nom, les requêtes locales sont dirigées vers 127.0.0.1 dû au dépassement, et puis le processus sous-jacent du dnscrypt-proxy du client d'itinérance en avant ils des serveurs publics d'OpenDNS au-dessus du canal chiffré.

Si on ne permet pas à des des DN pour circuler à 127.0.0.1:53, alors le client d'itinérance ne pourra pas fonctionner et ce qui suit se produira. Si le client ne peut pas atteindre les serveurs DNS publics ou l'adresse attachée de 127.0.0.1:53, elle transition à un état échec-ouvert et restaurer les configurations de DN sur les adaptateurs locaux. À l'arrière-plan, il continue à envoyer des sondes à 208.67.222.222 et peut transition au mode actif si la connexion sécurisée est rétablie.

Limites

Après avoir regardé la fonctionnalité de haut niveau des deux clients, il est évident que le client d'itinérance doive avoir la capacité de changer les configurations locales de DN et de lier à 127.0.0.1:53 pour expédier des requêtes à travers le canal de sécuriser. Quand le VPN est connecté, les seules configurations où AnyConnect ne gêne pas le résolveur indigène de DN sont le fractionnement-inclure et fractionnement-exclure (fractionnement-tunnel-tous DN étant désactivé). Par conséquent, il est actuellement recommandé pour utiliser une de ces configurations, quand le client d'itinérance est également en service. Le client d'itinérance restera dans état non protégé/décrypté si tunnel-toute configuration est utilisée, ou fractionnement-tunnel-tous DN est activés, suivant les indications de l'image.



Contournement

Si l'intention est de protéger la transmission entre le client d'itinérance et les serveurs d'OpenDNS à l'aide du tunnel VPN, alors un simulacre fractionnement-excluent la liste d'accès peut être utilisé sur le headend VPN. Ce sera la chose la plus étroite à une pleine configuration de tunnel. S'il n'y a aucune une telle condition requise, alors fractionnement-incluez peut être utilisé où la liste d'accès n'inclut pas les serveurs publics d'OpenDNS, ou fractionnement-les excluent peut être utilisé où l'access-list includes les serveurs de public d'OpenDNS.

Supplémentaire, en utilisant le client d'itinérance, des modes de split-dns ne peuvent pas être utilisés car ceci aura comme conséquence une perte de résolution locale de DN. Fractionnement-

tunnel-tous DN devraient également demeurer handicapés ; cependant, il est partiellement pris en charge et devrait permettre au client d'itinérance pour devenir POST-Basculement chiffré.

Configurations

Le trafic d'OpenDNS de tunnel

Cet exemple utilise une adresse IP factice dans la liste d'accès de fractionnement-exclure. Avec cette configuration, toute la transmission avec 208.67.222.222 se produit à travers le tunnel VPN, et le client d'itinérance fonctionne dans un état chiffré et protégé.

Excluez le trafic d'OpenDNS du tunnel VPN

Cet exemple utilise l'adresse de résolveur d'OpenDNS dans la liste d'accès de fractionnement-exclure. Avec cette configuration, toute la transmission avec 208.67.222.222 se produit en dehors du tunnel VPN, et le client d'itinérance fonctionne dans un état chiffré et protégé.

Cet exemple affiche une configuration de fractionnement-inclure pour un sous-réseau 192.168.1.0/24 interne. Avec cette configuration, le client d'itinérance fonctionnera toujours dans un état chiffré et protégé puisque le trafic à 208.67.222.222 n'est pas envoyé par l'intermédiaire du tunnel.

Vérifiez

Quand le VPN est connecté, le client d'itinérance devrait afficher protégé et chiffré suivant les indications de cette image :