Guide de déploiement de module de Sécurité d'itinérance d'AnyConnect OpenDNS

Contenu

Introduction

Ce document décrit l'installation, la configuration, et les étapes de dépannage pour le module d'itinérance d'OpenDNS (parapluie). Dans AnyConnect 4.3.X et plus tard, le client d'itinérance d'OpenDNS est maintenant disponible comme module intégré. On le connaît également comme module de Sécurité de nuage et il peut être déployé à l'avance au point final avec l'installateur d'AnyConnect, ou il peut être téléchargé de l'appliance de sécurité adaptable (ASA) par l'intermédiaire de Web-les déploient.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Mobilité sécurisée de Cisco AnyConnect
- OpenDNS/module itinérance de parapluie
- Cisco ASA

Composants utilisés

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

- Version 9.3(3)7 de Cisco ASA
- Client à mobilité sécurisé Cisco AnyConnect 4.3.01095
- Module 4.3.01095 d'itinérance d'OpenDNS
- Cisco Adaptive Security Device Manager (ASDM) 7.6.2 ou plus tard
- Microsoft Windows 8.1
- **Note**: Les conditions requises minimum de déployer le module de parapluie d'OpenDNS sont :
  - Version 4.3.01095 ou ultérieures d'AnyConnect VPN Client
  - Cisco ASDM 7.6.2 ou plus tard
  Le module d'itinérance d'OpenDNS n'est pas actuellement pris en charge sur la plate-forme Linux.

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelles commandes ou configuration.

Informations générales

OrgInfo.json

Pour que le module d'itinérance d'OpenDNS fonctionne correctement, un fichier OrgInfo.json doit être téléchargé du tableau de bord d'OpenDNS ou être poussé de l'ASA avant que le module soit utilisé. Quand le fichier est d'abord téléchargé, il est enregistré à un chemin spécifique qui dépend du système d'exploitation.

Pour le Mac OS X, OrgInfo.json est téléchargé à /opt/cisco/anyconnect/Umbrella.
Pour Microsoft Windows, OrgInfo.json est téléchargé au client \ au parapluie sécurisés de mobilité de C:\ProgramData\Cisco\Cisco AnyConnect.

```
{
"organizationId" : "XXXXXXX",
"fingerprint" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
"userId" : "XXXXXXX"
}
```

Comme affiché, le fichier utilise UTF-8 encodant et contient un organizationId, une empreinte digital, et un ID utilisateur. L'ID d'organisation représente les informations d'organisation pour l'utilisateur qui est actuellement connecté dans le tableau de bord d'OpenDNS. L'ID d'organisation est statique, seul, et automatique-généré par OpenDNS pour chaque organisation. L'empreinte digital est utilisée pour valider le fichier OrgInfo.json pendant l'enregistrement de périphérique et l'user-id représente un identificateur unique pour l'utilisateur ouvert une session.

Quand les débuts de module d'itinérance sur Windows, le fichier OrgInfo.json est copiés sur le répertoire des données sous le répertoire de parapluie et utilisés comme copie de travail. Sur le MAC OS X, les informations à partir de ce fichier sont enregistrées à updater.plist dans le répertoire des données sous le répertoire de parapluie. Une fois que le module a avec succès indiqué les informations à partir du fichier OrgInfo.json, il tente de s'inscrire à OpenDNS avec un nuage API. Cet enregistrement a comme conséquence OpenDNS assignant à un seul ID de périphérique à l'ordinateur cet enregistrement tenté. Si un ID de périphérique d'enregistrement antérieur est déjà disponible, le périphérique ignore l'enregistrement.

Après l'enregistrement est complet, le module d'itinérance exécute une exécution de sync afin de récupérer les informations de stratégie pour le point final. Un ID de périphérique est nécessaire pour que l'exécution de sync fonctionne. Les données de sync incluent les domaines syncInterval et whitelisted, et les adresses IP notamment. L'intervalle de sync est le nombre de minutes après quoi le module devrait tenter à la resync.

DN sondant le comportement

Sur l'enregistrement et le sync réussis, le module d'itinérance envoie des sondes de Système de noms de domaine (DNS) à ses résolveurs locaux. Ces demandes de DN incluent des requêtes TXT pour debug.opendns.com. Basé sur la réponse, le client peut déterminer si une appliance virtuelle d'OpenDNS de sur-site (VA) existe dans le réseau.

Si une appliance virtuelle (VA) est présente, les transitions de client à un mode « derrière-VA », et l'application de DN n'est pas exécutées sur le point final. Le client compte sur le VA pour l'application de DN au niveau du réseau.

Si un VA n'est pas présent, le client envoie une demande de DN aux résolveurs publics d'OpenDNS (208.67.222.222) utilisant UDP/443.

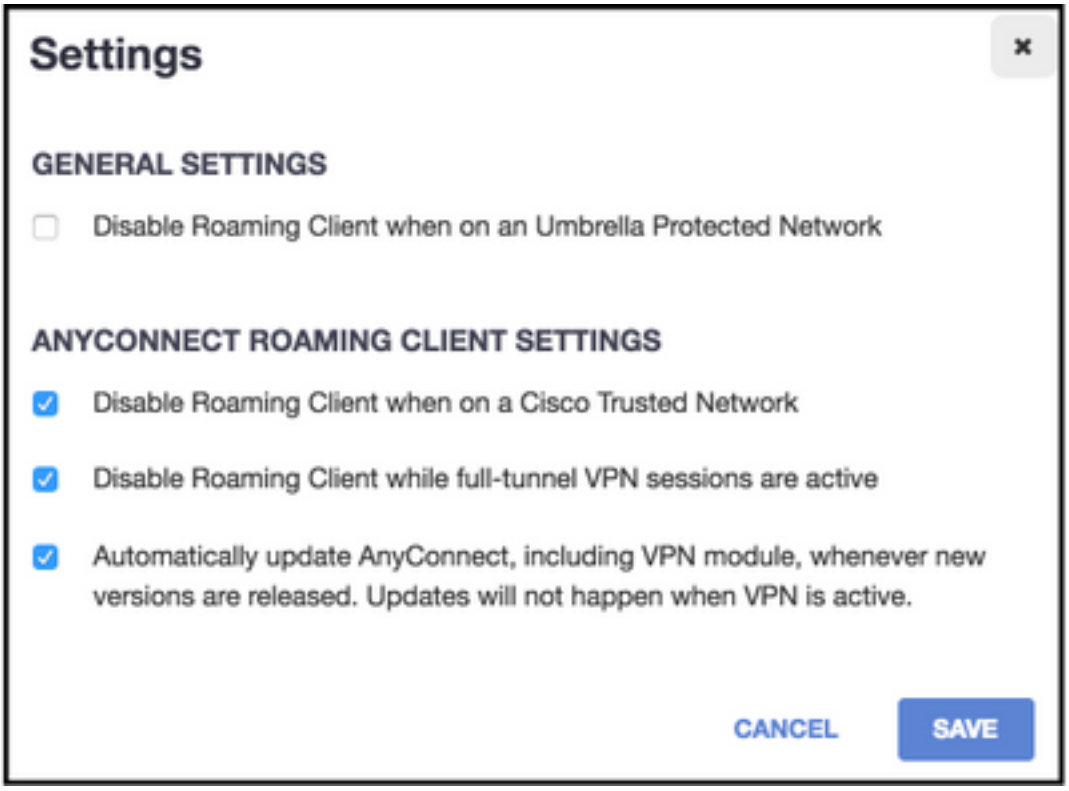
Une réaction favorable indique que le cryptage de DN est possible. Si une réponse négative est reçue, le client envoie une demande de DN aux résolveurs publics d'OpenDNS utilisant UDP/53.

Une réaction favorable à cette requête indique que la protection de DN est possible. Si une réponse négative est reçue, le client relance la requête en quelques secondes.

Dès réception d'un ensemble de réponses négatives, les transitions de client à l'état échec-ouvert. Un état échec-ouvert signifie que le cryptage et/ou la protection de DN n'est pas possible. Une fois que le module d'itinérance transitioned avec succès à un état protégé et/ou chiffré, toutes les requêtes DNS pour des domaines de recherche en dehors de des domaines locaux de recherche et des domaines de whitelist sont envoyées aux résolveurs d'OpenDNS pour la résolution de noms. L'état chiffré étant activé, toutes les transactions de DN sont chiffrées par le processus de dnscrypt.

Comportement de DN avec des modes de Tunnellisation d'AnyConnect

1. Tunnel-tout (ou tunnel-tout-DN activés)



Note: Comme affiché, le comportement par défaut est pour que le module d'itinérance désactive la protection de DN tandis qu'un tunnel VPN avec tunnel-toute configuration est en activité. Pour que le module soit en activité pendant un AnyConnect tunnel-toute configuration, le **client d'itinérance de débronchement tandis que les sessions VPN de plein-tunnel sont option active** doit être décoché sur le portail d'OpenDNS. La capacité d'activer cette caractéristique exige un niveau avancé d'abonnement avec OpenDNS. Les informations ci-dessous supposent que la protection de DN par l'intermédiaire du module d'itinérance est activée.

Pièce questionnée de domaine de Whitelist

Des demandes de DN qui proviennent de l'adaptateur de tunnel sont permises et envoyées aux serveurs DNS de tunnel, à travers le tunnel VPN. La requête demeurera non résolue si elle ne peut pas être résolue des serveurs DNS de tunnel.

Pièce questionnée de domaine pas de Whitelist

Des demandes de DN qui proviennent de l'adaptateur de tunnel sont permises, et proxied aux résolveurs publics d'OpenDNS par l'intermédiaire du module d'itinérance et seront envoyées à travers le tunnel VPN. Au client DNS il sera évident comme si la résolution de noms s'était produite par l'intermédiaire du serveur DNS VPN. Si la résolution de noms par l'intermédiaire des résolveurs d'OpenDNS n'est pas réussie, le module d'itinérance bascule aux serveurs DNS localement configurés, commençant par l'adaptateur VPN (qui est l'adaptateur préféré tandis que le tunnel est).

2. Split-dns (tunnel-tout-DN désactivés)

Note: Tous les domaines de split-dns sont automatiquement ajoutés au whitelist de module d'itinérance sur l'établissement de tunnel. Ceci est fait afin de fournir un mécanisme de manipulation cohérent de DN entre AnyConnect et le module d'itinérance. Assurez-vous que

dans une configuration de split-dns (avec fractionnement-incluez le Tunnellisation) les résolveurs publics d'OpenDNS ne sont pas inclus dans les réseaux de fractionnement-inclure.

Note: Sur le Mac OS X, 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.
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 qu'AnyConnect permet seulement les demandes de DN qui apparient 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 qui s'assortissent des domaines de split-dns ne soient pas envoyées en clair par l'intermédiaire de l'adaptateur public.

Pièce questionnée de domaine de Whitelist et également partie de domaines de split-dns

Des demandes de DN qui proviennent de l'adaptateur de tunnel sont permises et envoyées aux serveurs DNS de tunnel, à travers le tunnel VPN. Toutes autres demandes des domaines assortis d'autres adaptateurs seront répondues par le gestionnaire d'AnyConnect avec « aucun un tel nom » pour réaliser le split-dns vrai (empêchez le retour de DN). Par conséquent, seulement le trafic DNS de non-tunnel est protégé par le module d'itinérance.

Pièce questionnée de domaine de Whitelist, mais pas partie de domaines de split-dns

Des demandes de DN qui proviennent de l'adaptateur physique sont permises et envoyées aux serveurs DNS publics, en dehors du tunnel VPN. Toutes autres demandes des domaines assortis de l'adaptateur de tunnel seront répondues par le gestionnaire d'AnyConnect avec « aucun un tel nom » afin d'empêcher la requête d'être envoyé à travers le tunnel VPN.

Pièce questionnée de domaine pas de Whitelist ou de domaines de split-dns

Des demandes de DN qui proviennent de l'adaptateur physique sont permises et proxied aux résolveurs publics d'OpenDNS, et envoyées en dehors du tunnel VPN. Au client DNS il sera évident comme si la résolution de noms s'était produite par l'intermédiaire du serveur DNS public. Si la résolution de noms par l'intermédiaire des résolveurs d'OpenDNS est infructueuse, le module d'itinérance bascule aux serveurs DNS localement configurés, à l'exclusion de ceux configurés sur l'adaptateur VPN. Toutes autres demandes des domaines assortis de l'adaptateur de tunnel seront répondues par le gestionnaire d'AnyConnect sans un tel nom afin d'empêcher la requête d'être envoyé à travers le tunnel VPN.

3. Fractionnement-incluez ou Fractionnement-excluez le Tunnellisation (aucun split-dns et tunnel-tout-DN désactivés)

Pièce questionnée de domaine de Whitelist

Le résolveur indigène de SYSTÈME D'EXPLOITATION exécute la résolution de DN basée sur l'ordre des adaptateurs réseau, et AnyConnect est l'adaptateur préféré quand le VPN est en activité. Les demandes de DN d'abord proviendront de l'adaptateur de tunnel et seront envoyées aux serveurs DNS de tunnel, à travers le tunnel VPN. Si la requête ne peut pas être résolue des serveurs DNS de tunnel, le résolveur de SYSTÈME D'EXPLOITATION tentera de la résoudre par

l'intermédiaire des serveurs DNS publics.

Pièce questionnée de domaine pas de Whitelist

Le résolveur indigène de SYSTÈME D'EXPLOITATION exécute la résolution de DN basée sur l'ordre des adaptateurs réseau, et AnyConnect est l'adaptateur préféré quand le VPN est en activité. Les demandes de DN d'abord proviendront de l'adaptateur de tunnel et seront envoyées aux serveurs DNS de tunnel, à travers le tunnel VPN. Si la requête ne peut pas être résolue des serveurs DNS de tunnel, le résolveur de SYSTÈME D'EXPLOITATION tentera de la résoudre par l'intermédiaire des serveurs DNS publics.

Si les résolveurs publics d'OpenDNS font partie de la liste de fractionnement-inclure ou pas une partie de la liste de fractionnement-exclure, la demande proxied est envoyée à travers le tunnel VPN.

Si les résolveurs publics d'OpenDNS ne sont pas une partie de la liste de fractionnement-inclure ou une partie de la liste de fractionnement-exclure, la demande proxied est envoyée en dehors du tunnel VPN.

Si la résolution de noms par l'intermédiaire des résolveurs d'OpenDNS n'est pas réussie, le module d'itinérance bascule aux serveurs DNS localement configurés, commençant par l'adaptateur VPN (qui est l'adaptateur préféré tandis que le tunnel est). Si la réponse finale renvoyée par le module d'itinérance (et proxied de nouveau au client DNS indigène) n'est pas réussie, le client indigène tentera d'autres serveurs DNS, si disponible.

Installez et configurez le module d'itinérance de parapluie

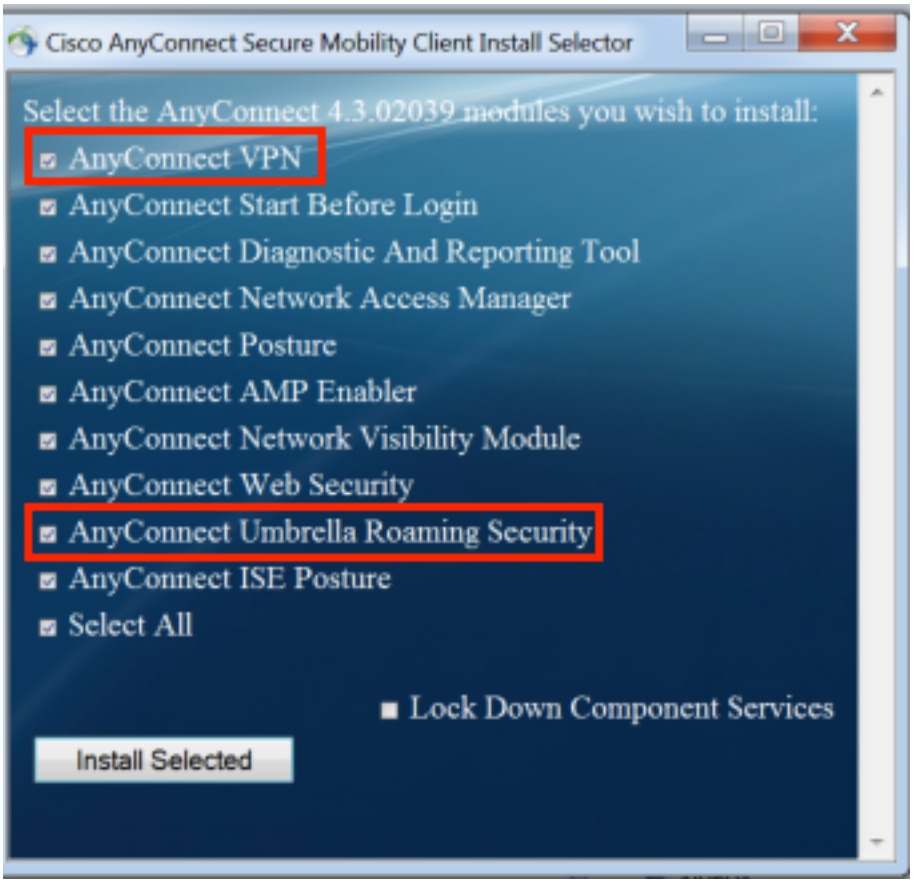
Afin d'intégrer le module d'itinérance d'OpenDNS avec le client vpn d'AnyConnect, le module doit être installé par l'intermédiaire de la méthode de déploiement de pre-deploment ou de Web :

méthode de Pré-déploiement (manuel)

le Pré-déploiement exige l'installation manuelle du module d'itinérance d'OpenDNS et de copier du fichier OrgInfo.json sur l'ordinateur d'utilisateur. Des déploiements à grande échelle sont typiquement réalisés avec les systèmes de gestion de logiciel d'entreprise (SMS).

Déployez le module d'itinérance d'OpenDNS

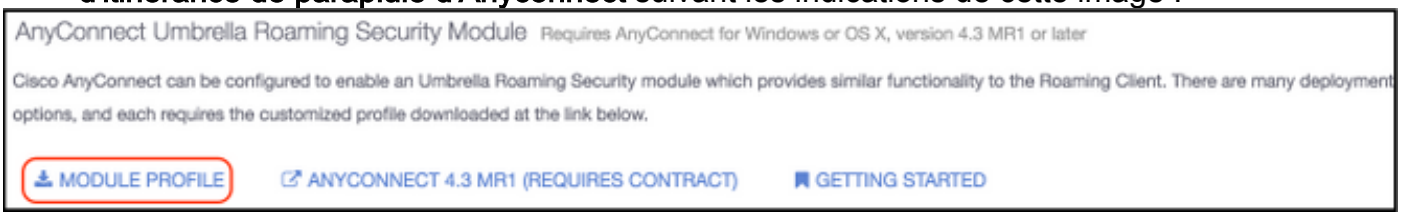
Pendant l'installation de module d'AnyConnect, choisissez l'**AnyConnect VPN** et les modules de **Sécurité d'itinérance de parapluie d'AnyConnect** :



Déployez OrgInfo.json

Afin de télécharger le fichier OrgInfo.json, terminez-vous ces étapes :

1. Connectez-vous dans le tableau de bord d'OpenDNS.
2. Choisissez la **configuration > les identités > les ordinateurs d'itinérance.**
3. Cliquez sur **+** signe.
4. Faites descendre l'écran et choisissez le **profil de module** dans la **section Module de Sécurité d'itinérance de parapluie d'Anyconnect** suivant les indications de cette image :



Une fois le fichier lui est téléchargé doit être enregistré à un de ces chemins, qui dépend du système d'exploitation.

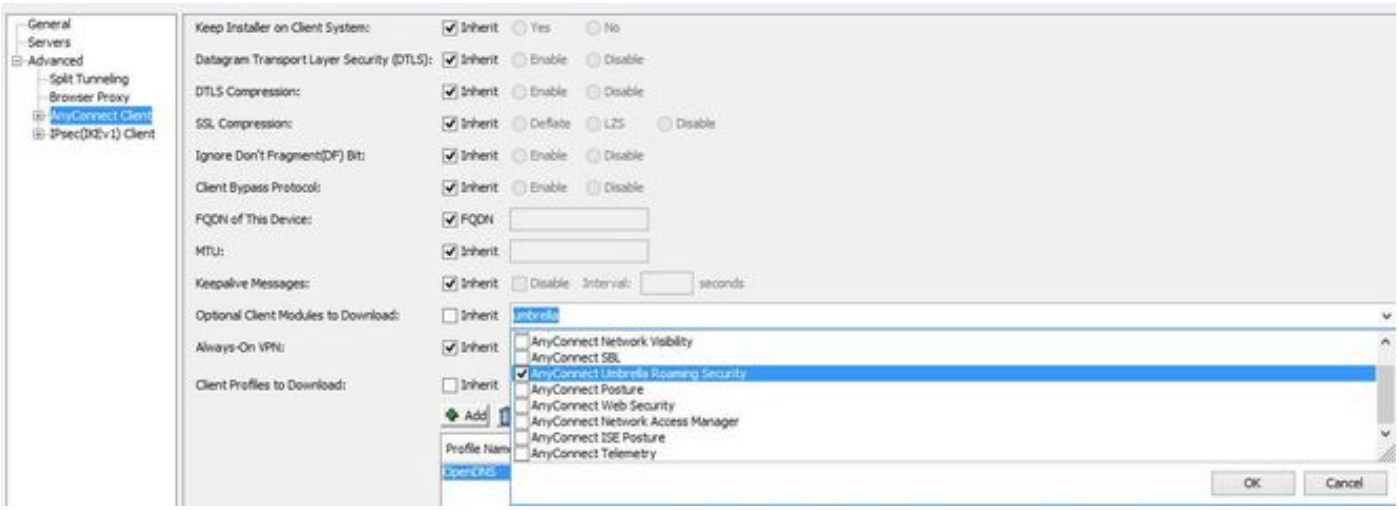
Pour le Mac OS X : /opt/cisco/anyconnect/Umbrella
Pour Windows : Client \ parapluie sécurisés de mobilité de C:\ProgramData\Cisco\Cisco AnyConnect

Méthode de Web-déploiement

Déployez le module d'itinérance d'OpenDNS

Téléchargez le module de client de mobilité de Sécurité d'Anyconnect (c'est-à-dire, anyconnect-

win-4.3.02039-k9.pkg) du site Web Cisco et téléchargez-le à l'éclair de l'ASA. Une fois que téléchargé, dans l'ASDM, choisissez la **stratégie de groupe > a avancé > client d'AnyConnect > les modules facultatifs de client pour télécharger** et puis choisir la **Sécurité d'itinérance de parapluie.**

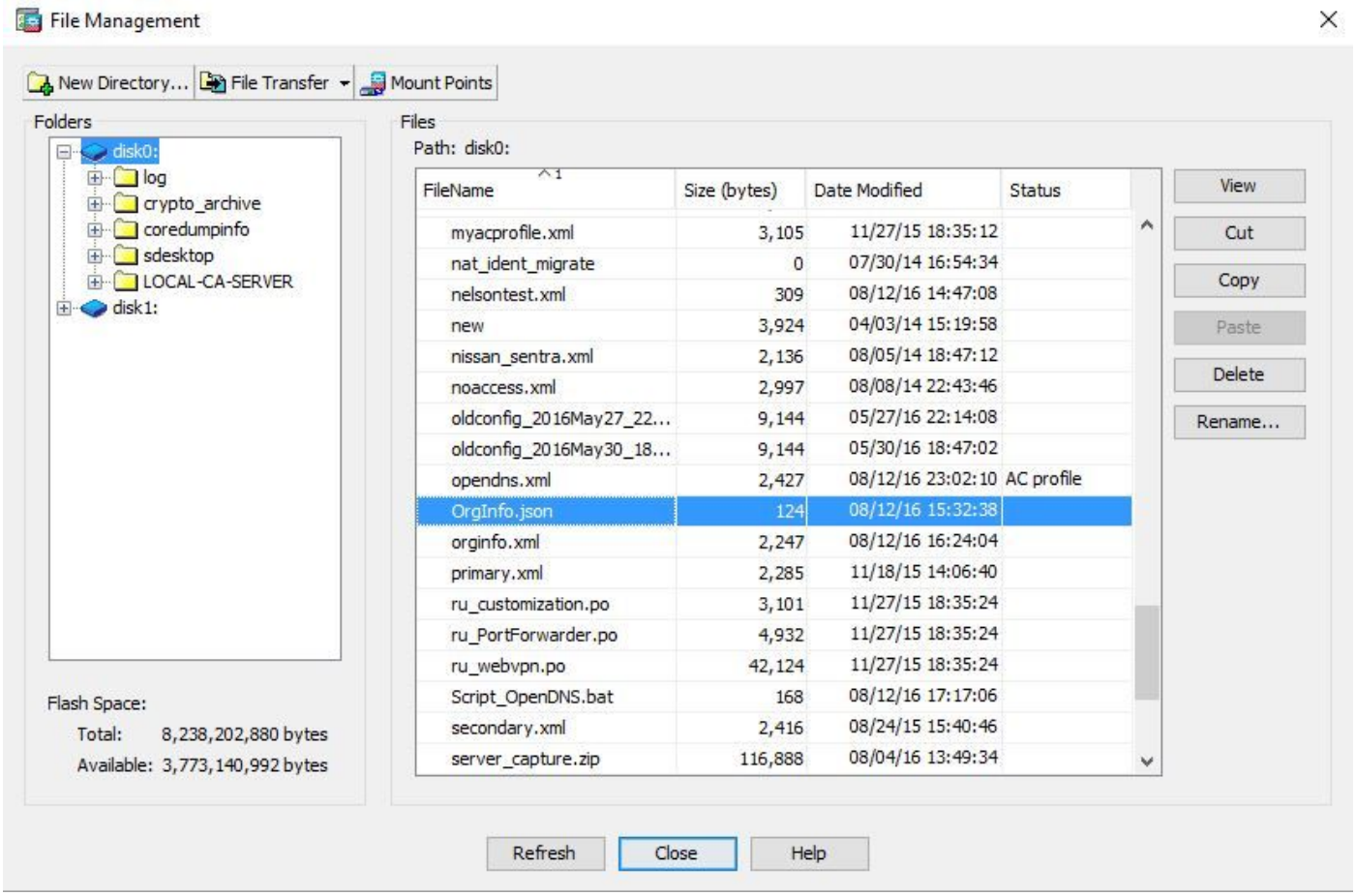


Équivalent CLI

```
group-policy <Group_Policy_Name> attributes
webvpn
anyconnect modules value umbrella
```

Déployez OrgInfo.json

1. Téléchargez le fichier OrgInfo.json du tableau de bord d'OpenDNS et téléchargez-le à l'éclair de l'ASA.



2. Configurez l'ASA pour pousser le fichier OrgInfo.json aux points finaux distants.

```
webvpn
anyconnect profiles OpenDNS disk0:/OrgInfo.json
!
!
group-policy <Group_Policy_Name> attribute
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> **Note**: Cette configuration peut seulement être exécutée par le CLI. Afin d'utiliser l'ASDM pour cette tâche, la version 7.6.2 ou ultérieures ASDM doit être installée sur l'ASA.

Une fois que le client d'itinérance de parapluie est installé par l'intermédiaire d'une des méthodes discutées, elle devrait apparaître comme module intégré dans le GUI d'AnyConnect suivant les indications de cette image :

Jusqu'à ce que l'OrgInfo.json soit déployé sur le point final à l'emplacement approprié, le module d'itinérance de parapluie ne sera pas initialisé.

Configurez

Les expositions de section échantillonnent des extraits de configuration CLI nécessaires pour utiliser le module d'itinérance d'OpenDNS avec les divers modes de Tunnellisation d'AnyConnect.

```
!--- ip local pool for vpn
ip local pool vpn_pool 198.51.100.1-198.51.100.9 mask 255.255.255.224

!--- Optional NAT Hairpin configuration to reach OpenDNS servers through VPN tunnel
object network OpenDNS
subnet 198.51.100.0 255.255.255.0
nat (outside,outside) source dynamic OpenDNS interface
!
same-security-traffic permit intra-interface

!--- Global Webvpn Configuration
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.3.01095-k9.pkg 1
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect profiles OpenDNS disk0:/OrgInfo.json
anyconnect enable
tunnel-group-list enable

!--- split-include Configuration
access-list Split_Include standard permit <host/subnet>

group-policy OpenDNS_Split_Include internal
group-policy OpenDNS_Split_Include attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
```

```
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Include
split-dns value <internal domains> (Optional Split-DNS Configuration)
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Include type remote-access
tunnel-group OpenDNS_Split_Include general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Include
tunnel-group OpenDNS_Split_Include webvpn-attributes
group-alias OpenDNS_Split_Include enable


!--- Split-exclude Configuration
access-list Split_Exclude standard permit <host/subnet>

group-policy OpenDNS_Split_Exclude internal
group-policy OpenDNS_Split_Exclude attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy excludespecified
 split-tunnel-network-list value Split_Exclude
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Exclude type remote-access
tunnel-group OpenDNS_Split_Exclude general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Exclude
tunnel-group OpenDNS_Split_Exclude webvpn-attributes
group-alias OpenDNS_Split_Exclude enable


!--- Tunnelall Configuration
group-policy OpenDNS_Tunnel_All internal
group-policy OpenDNS_Tunnel_All attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelall
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Tunnel_All type remote-access
tunnel-group OpenDNS_Tunnel_All general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Tunnel_All
tunnel-group OpenDNS_Tunnel_All webvpn-attributes
group-alias OpenDNS_Tunnel_All enable
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Les étapes pour dépanner des questions connexes d'AnyConnect OpenDNS sont :

1. Assurez-vous que le module de Sécurité d'itinérance de parapluie est installé avec le client sécurisé de mobilité d'Anyconnect.
2. Assurez qu'OrgInfo.json est présent sur le point final au chemin exact basé sur le système d'exploitation et est dans le format spécifié dans ce document.
3. Si des requêtes DNS aux résolveurs d'OpenDNS sont destinées pour aller au-dessus du tunnel VPN d'AnyConnect, assurez-vous que l'épingle à cheveux est configurée sur l'ASA afin de permettre l'accessibilité aux résolveurs d'OpenDNS.
4. Collectez les captures de paquet (sans tous filtres) sur l'adaptateur virtuel d'AnyConnect et l'adaptateur physique simultanément et les notez en bas des domaines qui ne les résolvent pas.
5. Si le module d'itinérance fonctionne dans un état chiffré, collectez les captures de paquet après avoir bloqué l'UDP 443 localement, pour dépannage des buts seulement. Cette manière là est visibilité dans les transactions de DN.
6. Exécutez le DART d'AnyConnect, des diagnostics de parapluie et le notez en bas de la période de la panne de DN. Voyez comment collecter le paquet de DART pour le pour en savoir plus d'Anyconnect.
7. Collectez les logs diagnostiques de parapluie et envoyez l'URL en résultant à votre administrateur d'OpenDNS. Seulement vous et l'administrateur d'OpenDNS avez accès à ces informations. Pour Windows : C:\Program classe (client sécurisé de mobilité x86)\Cisco\Cisco AnyConnect \ UmbrellaDiagnostic.exe
   Pour le MacOSX : /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Informations connexes

- **ID de bogue Cisco CSCvb34863 : La latence en résolvant des DN quand AnyConnect a configuré pour fractionnement-incluent le Tunnellisation**
- **Support et documentation techniques - Cisco Systems**