

# Guide de déploiement du module de sécurité d'itinérance d'Anyconnect OpenDNS

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Orginfo.json](#)

[Étude du comportement grâce à DNS](#)

[Comportement de DNS avec les modes de tunnellation d'AnyConnect](#)

[1. Tunnel-tout \(fonction tunnel-tout-DNS activée\)](#)

[2. DNS divisé \(fonction tunnel-tout-DNS désactivée\)](#)

[3. Tunnel divisé ou non divisé \(aucune fonction DNS divisée et fonction tunnel-tout-DNS désactivée\)](#)

[Installer et configurer le module d'itinérance Umbrella](#)

[Méthode de prédéploiement \(manuel\)](#)

[Déploiement du module d'itinérance OpenDNS](#)

[Déploiement d'OrgInfo.json](#)

[Méthode de déploiement Web](#)

[Déploiement du module d'itinérance OpenDNS](#)

[Déploiement d'OrgInfo.json](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit l'installation, la configuration et le dépannage pour le module d'itinérance OpenDNS (Umbrella). Dans AnyConnect 4.3.X et les versions ultérieures, le client d'itinérance OpenDNS est maintenant offert comme module intégré. Il est également connu comme le module Cloud Security (sécurité cloud) et peut être prédéployé au point d'accès avec l'utilitaire d'installation AnyConnect, ou il peut être téléchargé à partir de l'appareil de sécurité adaptatif (ASA) par l'intermédiaire d'un déploiement Web.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco AnyConnect Secure Mobility
- Module d'itinérance OpenDNS/Umbrella
- Cisco ASA

## Components Used

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 de mobilité sécurisée Cisco AnyConnect 4.3.01095
- Module d'itinérance OpenDNS 4.3.01095
- Cisco Adaptive Security Device Manager (ASDM), versions 7.6.2 ou ultérieure
- Microsoft Windows 8.1
- **Note:** Exigences minimales pour le déploiement du module OpenDNS Umbrella :
  - Client AnyConnect VPN, version 4.3.01095 ou ultérieure
  - Cisco ASDM 7.6.2 ou ultérieure

Le module d'itinérance OpenDNS n'est pas actuellement pris en charge par la plateforme Linux.

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 ou de la configuration.

## Informations générales

### Orginfo.json

Pour que le module d'itinérance OpenDNS fonctionne correctement, un fichier OrgInfo.json doit être téléchargé à partir du tableau de bord OpenDNS ou extrait de l'ASA avant l'utilisation du module. Lorsque le fichier est téléchargé initialement, il est enregistré suivant un chemin précis lequel est en fonction du système d'exploitation.

Pour Mac OS X, le fichier Orginfo.json est téléchargé à /opt/cisco/anyconnect/Umbrella.  
 Pour Microsoft Windows, Orginfo.json est téléchargé à C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella.

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

Comme illustré, le fichier utilise le codage UTF-8 et contient un ID de structure, des empreintes digitales et un ID d'utilisateur. L'ID de structure désigne les renseignements de la structure pour l'utilisateur qui est actuellement connecté au tableau de bord d'OpenDNS. L'ID de structure est statique, unique et créé automatiquement par OpenDNS pour chaque structure. L'empreinte digitale est utilisée pour valider le fichier Orginfo.json pendant l'enregistrement de l'appareil, et l'identifiant de l'utilisateur est un code unique qui représente l'utilisateur connecté.

Lorsque le module d'itinérance démarre dans Windows, le fichier Orginfo.json est copié dans le répertoire de données, sous celui d'Umbrella, et est utilisé comme copie de travail. Sur MAC OS X, les renseignements issus du fichier sont enregistrés dans updater.plist du répertoire de données, sous celui d'Umbrella. Une fois que le module a lu correctement l'information du fichier Orginfo.json, il tente de s'enregistrer avec OpenDNS à l'aide d'une API en nuage. Cet enregistrement se traduit par l'attribution dans OpenDNS d'un identifiant unique pour le périphérique qui a tenté de s'enregistrer. Si l'identifiant d'un périphérique préalable à l'enregistrement est déjà disponible, l'appareil saute l'enregistrement.

Après l'enregistrement, le module d'itinérance effectue une opération de synchronisation afin de récupérer les renseignements de la politique pour le point d'accès. Un identifiant de périphérique est nécessaire pour que l'opération de synchronisation fonctionne. Les données de synchronisation incluent entre autres les domaines syncInterval, les domaines de contournement internes et les adresses IP. L'intervalle de synchronisation désigne le nombre de minutes après lequel le module devrait tenter de se resynchroniser.

## Étude du comportement grâce à DNS

Lorsque l'enregistrement et la synchronisation sont réussis, le module d'itinérance envoie les sondes de système de nom de domaine (DNS) vers ses programmes de résolution locaux. Ces requêtes DNS comprennent les requêtes TXT pour debug.opendns.com. Selon la réponse, le client est en mesure de déterminer si un appareil virtuel (AV) d'OpenDNS existe dans le réseau.

Si une appliance virtuelle (AV) existe, le client passe en mode « derrière l'AV », et l'activation du DNS n'est pas effectuée sur le point d'accès. Le client compte sur l'AV pour activer le DNS sur le réseau.

Si un AV n'existe pas, le client envoie une requête DNS pour les programmes de résolution publics d'OpenDNS (208.67.222.222) au moyen de l'UDP/443.

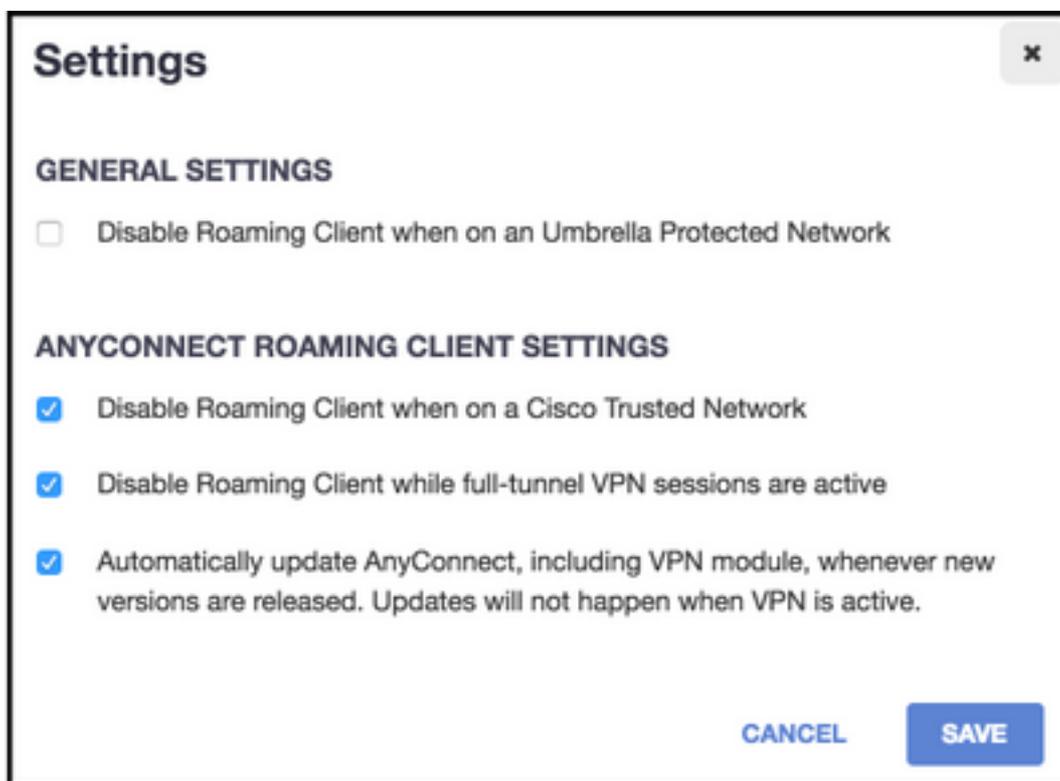
Une réponse positive indique que le chiffrement du DNS est possible. Dans le cas d'une réponse négative, le client envoie une requête DNS pour les programmes de résolutions publics d'OpenDNS au moyen de l'UDP/53.

Si cette requête reçoit une réponse positive, la protection du DNS est donc possible. Dans le cas d'une réponse négative, le client retente la requête en quelques secondes.

Dès réception d'un nombre défini de réponses négatives, le client passe à l'état défaillance-ouvert. Cet état signifie que le chiffrement ou la protection DNS ne sont pas possibles. Une fois que le module d'itinérance est passé à un état protégé et/ou chiffré, toutes les requêtes DNS pour les domaines de recherche en dehors des domaines de recherche locaux et des domaines de contournement internes sont envoyées aux résolveurs OpenDNS pour la résolution de noms. Lorsque l'état chiffré est activé, toutes les transactions du DNS sont chiffrées à l'aide du procédé dnsencrypt.

## Comportement de DNS avec les modes de tunnellation d'AnyConnect

### 1. Tunnel-tout (fonction tunnel-tout-DNS activée)



**Note:** Comme illustré, le comportement par défaut est que le module d'itinérance désactive la protection du DNS, alors qu'un tunnel VPN avec configuration tunnel-tout est activé. Pour que le module soit actif pendant la configuration tunnel-tout d'AnyConnect, l'option **Désactiver le client d'itinérance pendant que les sessions VPN plein tunnel sont actives doit être désactivée sur le portail d'OpenDNS**. La possibilité d'activer cette fonction requiert un niveau d'abonnement avancé dans OpenDNS. Les renseignements ci-dessous supposent que la protection du DNS par l'intermédiaire du module d'itinérance est activée.

### **Domaine interrogé faisant partie de la liste de contournement interne**

Les requêtes DNS qui proviennent de l'adaptateur du tunnel sont autorisées, puis acheminées vers les serveurs DNS du tunnel, à travers le tunnel VPN. La requête restera non résolue si les serveurs DNS du tunnel ne parviennent pas à la résoudre.

### **Domaine interrogé ne faisant pas partie de la liste de contournement interne**

Les requêtes DNS provenant de l'adaptateur du tunnel sont autorisées, puis transmises par proxy vers les programmes de résolution publics d'OpenDNS au moyen du module d'itinérance, pour être ensuite acheminées à travers le tunnel VPN. Pour le client DNS, il apparaîtra comme si la résolution de noms avait eu lieu par le serveur VPN du DNS. Si la résolution de noms par les programmes de résolution d'OpenDNS échoue, le module d'itinérance bascule sur les serveurs DNS configurés localement, en commençant par l'adaptateur VPN (soit l'adaptateur privilégié pendant que le tunnel est configuré).

## **2. DNS divisé (fonction tunnel-tout-DNS désactivée)**

**Note:** Tous les domaines DNS fractionnés sont automatiquement ajoutés à la liste de contournement interne du module d'itinérance lors de l'établissement du tunnel. Cela permet de fournir des mécanismes de traitement DNS cohérents entre AnyConnect et le module d'itinérance. Veiller à ce que dans une configuration DNS divisé (avec tunnellation divisée)

les programmes de résolution publics d'OpenDNS ne figurent pas dans les réseaux divisés.

**Note:** Sur Mac OS X, si le DNS divisé est activé pour les deux protocoles IP (IPv4 et IPv6) ou s'il n'est activé que pour un seul protocole et qu'aucun ensemble d'adresses n'est configuré pour l'autre protocole, le vrai DSN divisé semblable à Windows est appliqué. 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 tunnellation divisée est activée. Cela signifie qu'AnyConnect permet seulement les requêtes DNS qui correspondent à des domaines DNS divisés par le tunnel (les autres requêtes reçoivent leur réponse par AC, et les refus forcent le basculement vers les serveurs DNS publics) et ne peut appliquer les requêtes qui correspondent aux domaines DNS divisés qui ne sont pas acheminées en mode non chiffré via l'adaptateur public.

### **Domaine interrogé faisant partie de la liste de contournement interne et faisant partie des domaines DNS partagés**

Les requêtes DNS qui proviennent de l'adaptateur du tunnel sont autorisées, puis acheminées vers les serveurs DNS du tunnel, à travers le tunnel VPN. Toutes les autres demandes correspondant aux domaines des autres adaptateurs recevront une réponse par le pilote d'AnyConnect, « sans ces noms », pour atteindre un vrai DNS divisé (pour empêcher l'option de rechange du DNS). Par conséquent, seul le trafic DNS hors tunnel est protégé par le module d'itinérance.

### **Domaine interrogé faisant partie de la liste de contournement interne, mais ne faisant pas partie des domaines DNS partagés**

Les requêtes DNS qui proviennent de l'adaptateur physique sont autorisées, puis envoyées vers les serveurs DNS publics, à l'extérieur du tunnel VPN. Toutes les autres requêtes liées aux domaines correspondants de l'adaptateur du tunnel recevront une réponse par le pilote d'AnyConnect « sans ces noms » afin d'empêcher que la requête soit acheminée à travers le tunnel VPN.

### **Domaine interrogé ne faisant pas partie de la liste de contournement interne ou des domaines DNS fractionnés**

Les requêtes DNS qui proviennent de l'adaptateur physique sont autorisées, puis transmises par proxy vers les programmes de résolution publics d'OpenDNS, pour être ensuite acheminées à l'extérieur du tunnel VPN. Pour le client DNS, il apparaîtra comme si la résolution de noms avait eu lieu par le serveur DNS public. Si les programmes de résolution d'OpenDNS échouent la résolution de noms, le module d'itinérance bascule vers les serveurs DNS configurés localement, à l'exclusion de ceux configurés sur l'adaptateur VPN. Toutes les autres requêtes liées aux domaines correspondants de l'adaptateur du tunnel recevront une réponse par le pilote d'AnyConnect sans ces noms afin d'empêcher que la requête soit acheminée à travers le tunnel VPN.

## **3. Tunnel divisé ou non divisé (aucune fonction DNS divisée et fonction tunnel-tout-DNS désactivée)**

### **Domaine interrogé faisant partie de la liste de contournement interne**

Le programme de résolution natif OS effectue la résolution DNS en fonction de l'ordre des

adaptateurs réseau, et AnyConnect est l'adaptateur privilégié si VPN est actif. Les requêtes DNS proviendront d'abord de l'adaptateur du tunnel et seront envoyées vers les serveurs DNS du tunnel, à travers le tunnel VPN. Si la requête ne peut pas être résolue par les serveurs DNS du tunnel, le programme de résolution OS tentera de la résoudre grâce aux serveurs DNS publics.

### **Domaine interrogé ne faisant pas partie de la liste de contournement interne**

Le programme de résolution natif OS effectue la résolution DNS en fonction de l'ordre des adaptateurs réseau, et AnyConnect est l'adaptateur privilégié si VPN est actif. Les requêtes DNS proviendront d'abord de l'adaptateur du tunnel et seront envoyées vers les serveurs DNS du tunnel, à travers le tunnel VPN. Si la requête ne peut pas être résolue par les serveurs DNS du tunnel, le programme de résolution OS tentera de la résoudre grâce aux serveurs DNS publics.

Si les programmes de résolution publics d'OpenDNS font partie de la liste divisée ou ne font pas partie de la liste non divisée, la requête envoyée par proxy est acheminée à travers le tunnel VPN.

Si les programmes de résolution publics d'OpenDNS ne font pas partie de la liste divisée ou font partie de la liste non divisée, la requête envoyée par proxy est acheminée à l'extérieur du tunnel VPN.

Si la résolution de noms par les programmes de résolution d'OpenDNS échoue, le module d'itinérance bascule sur les serveurs DNS configurés localement, en commençant par l'adaptateur VPN (soit l'adaptateur privilégié pendant que le tunnel est configuré). Si la réponse finale retournée par le module d'itinérance (et retransmise par proxy vers le client DNS natif) échoue, le client natif tentera la procédure sur les autres serveurs DNS, s'ils sont accessibles.

## **Installer et configurer le module d'itinérance Umbrella**

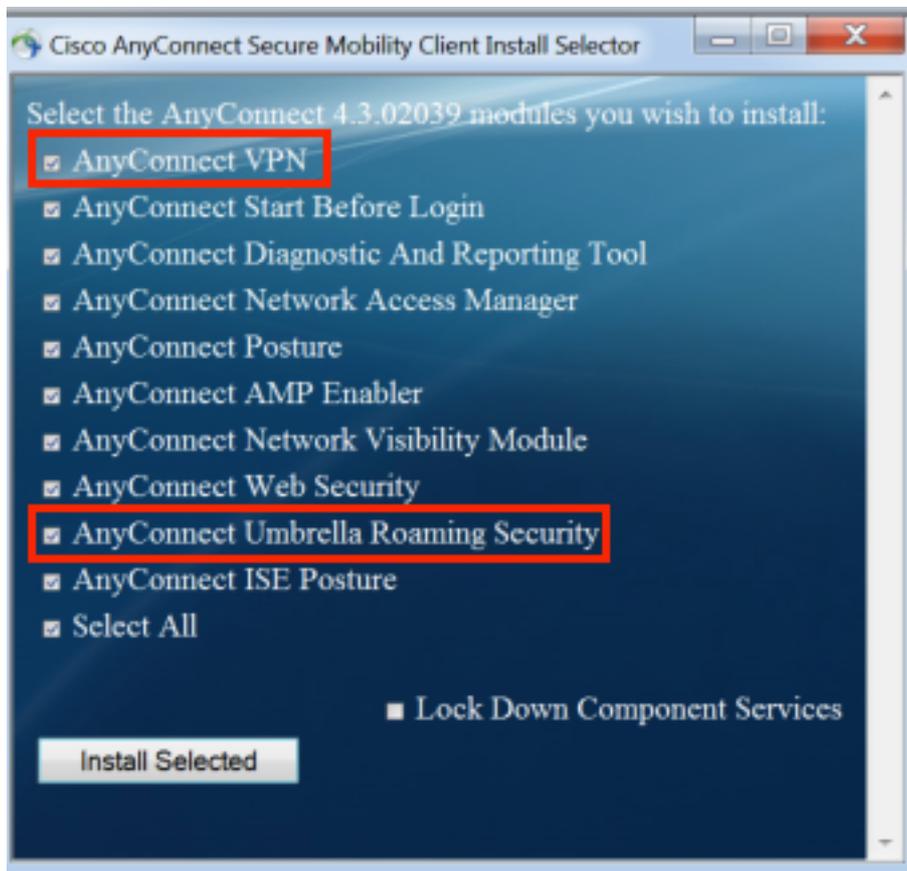
Afin d'intégrer le module d'itinérance OpenDNS au moyen du client VPN d'AnyConnect, le module doit être installé par la méthode de prédéploiement ou de déploiement Web :

### **Méthode de prédéploiement (manuel)**

Le prédéploiement nécessite l'installation manuelle du module d'itinérance OpenDNS et la copie du fichier OrgInfo.json sur l'ordinateur de l'utilisateur. Les déploiements d'envergure sont généralement obtenus avec des systèmes de gestion de logiciel (SMS) des entreprises.

### **Déploiement du module d'itinérance OpenDNS**

Pendant l'installation du paquet AnyConnect, choisissez les modules **VPN AnyConnect** et **AnyConnect Umbrella Roaming Security (sécurité d'itinérance Umbrella Anyconnect)** :



## Déploiement d'OrgInfo.json

Afin de télécharger le fichier OrgInfo.json, effectuez les étapes suivantes :

1. Connectez-vous au tableau de bord OpenDNS.
2. Choisissez **Configuration > Identities > Roaming Computers (configuration > identités > ordinateurs d'itinérance)**.
3. Cliquez sur le signe + .
4. Faites défiler l'écran et sélectionnez **Module Profile (profil du module)** dans la section **Anyconnect Umbrella Roaming Security Module (module de sécurité d'itinérance Umbrella d'Anyconnect)**, comme le montre cette image :



Lorsque le fichier est téléchargé, il doit être enregistré dans l'un de ces chemins, selon le système d'exploitation.

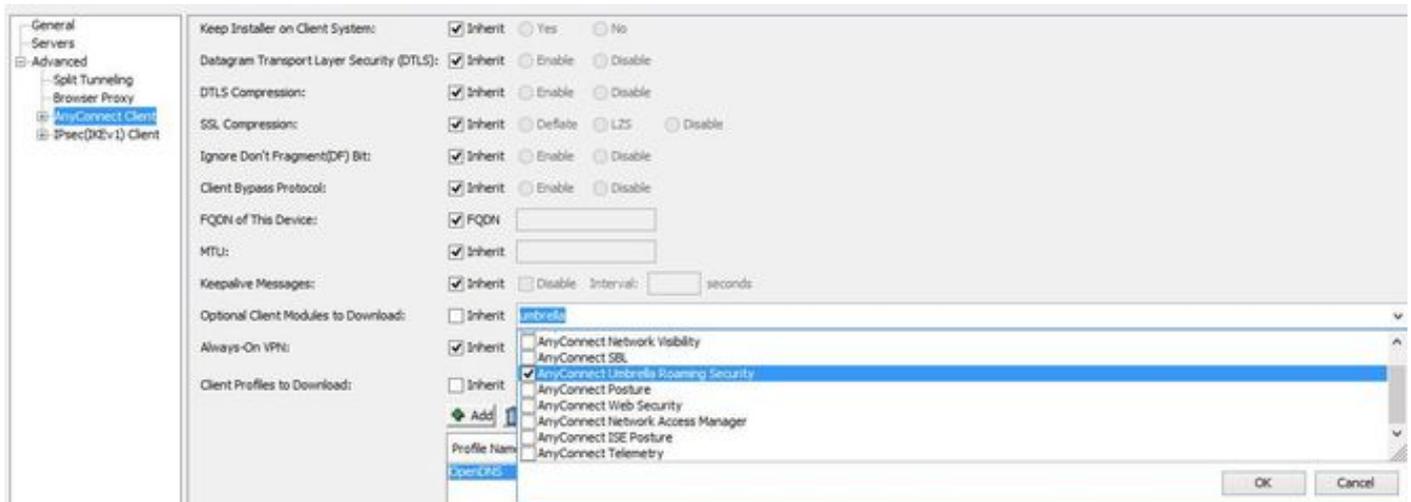
Pour MAC OS X : /opt/Cisco/AnyConnect/Umbrella

Pour Windows : C:\ProgramData\Cisco\Cisco AnyConnect mobilité sécurisée Client\Umbrella

## Méthode de déploiement Web

### Déploiement du module d'itinérance OpenDNS

Téléchargez le paquet du client de mobilité et de sécurité AnyConnect (à savoir, anyconnect-win-4.3.02039-k9.pkg) sur le site Web de Cisco et versez-le dans la mémoire flash de l'ASA. Une fois téléversé, dans ASDM, choisissez **Group Policy > Advanced > AnyConnect Client > Optional Client Modules to Download (politique de groupe > avancé > client AnyConnect > modules facultatifs de client à télécharger)**, puis choisissez **Umbrella Roaming Security (sécurité d'itinérance Umbrella)**.

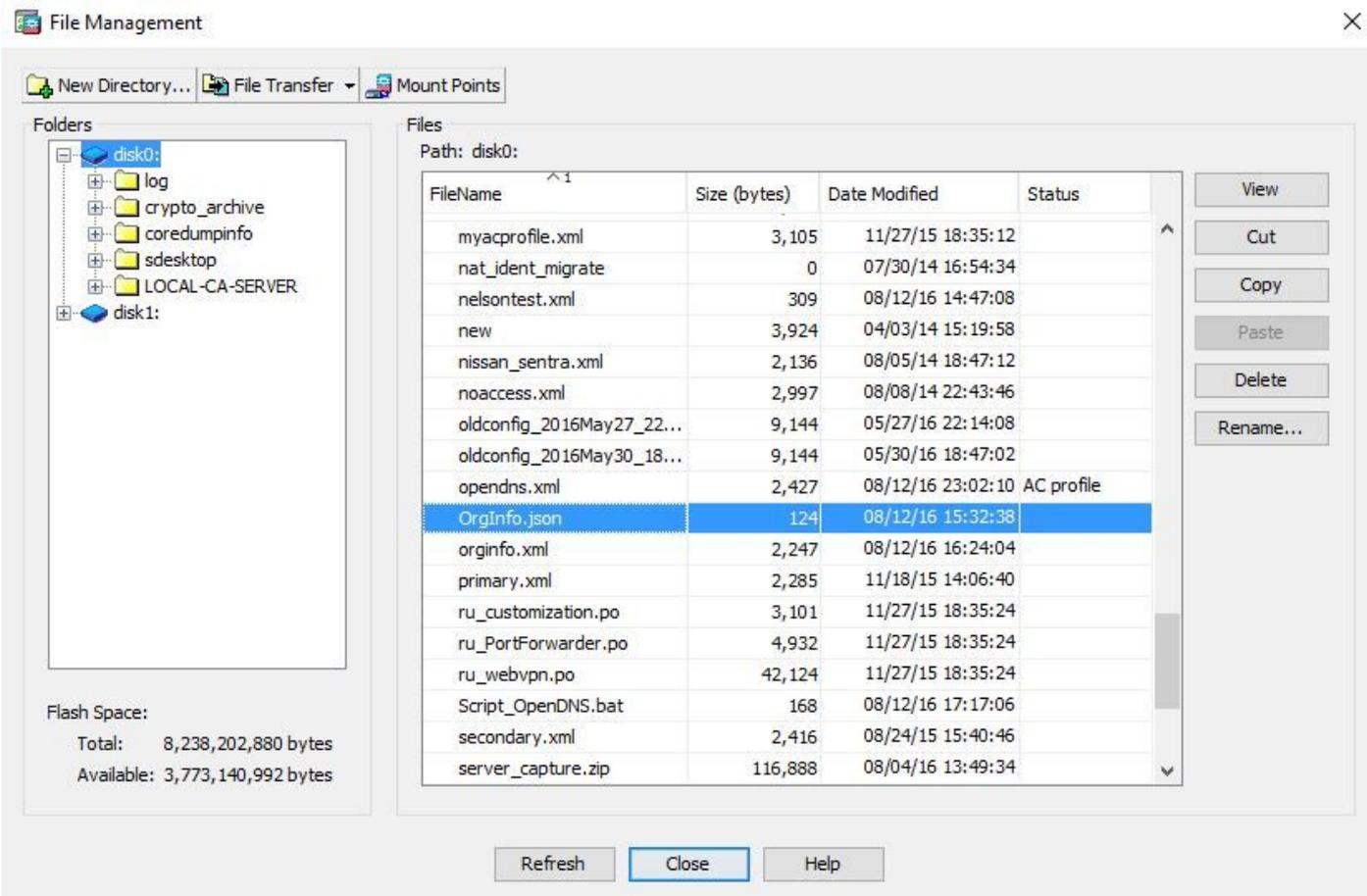


## Équivalent de la CLI

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

## Déploiement d'OrgInfo.json

1. Téléchargez le fichier Orginfo.json sur le tableau de bord d'OpenDNS, puis transférez-le dans la mémoire flash de l'ASA.



2. Configurez l'ASA pour pousser le fichier OrgInfo.json vers des points de terminaison distants.

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

**Note:** Cette configuration ne peut être effectuée que par la CLI. Pour pouvoir utiliser ASDM pour cette tâche, la version 7.6.2 ou une version ultérieure doit être installée sur l'ASA.

Une fois que le client d'itinérance Umbrella est installé à l'aide d'une des méthodes présentées, il doit apparaître comme un module intégré dans l'interface graphique utilisateur (GUI) d'AnyConnect, comme l'illustre l'image suivante :



Jusqu'à ce que le fichier Orginfo.json soit déployé sur le point de terminaison, à l'emplacement approprié, le module d'itinérance Umbrella ne sera pas initialisé.

## Configuration

La section illustre des extraits de la configuration de la CLI nécessaire au fonctionnement du module d'itinérance OpenDNS avec les divers modes de tunnellation 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
```

#### (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
```

## Vérification

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

# Dépannage

Étapes de dépannage pour les problèmes liés à AnyConnect OpenDNS :

1. Assurez-vous que le module de sécurité d'itinérance Umbrella est installé avec le client de mobilité et de sécurité Anyconnect.
2. Assurez-vous que le fichier OrgInfo.json est présent sur le point d'accès, dans le bon chemin d'accès en fonction du système d'exploitation et dans le format précisé dans le présent document.
3. Si les requêtes DNS des programmes de résolution d'OpenDNS sont destinées à franchir le tunnel VPN d'AnyConnect, assurez-vous que ce renvoi d'appel en épingle est configuré sur l'ASA pour permettre l'accessibilité aux programmes de résolution d'OpenDNS.
4. Collectez les données de paquet (sans filtres) à la fois sur l'adaptateur virtuel AnyConnect et sur l'adaptateur physique, puis relevez les noms de domaines qui ne sont pas résolus.
5. Si le module d'itinérance fonctionne en mode chiffré, collectez les données de paquets saisies après blocage local de l'UDP/443, aux fins de dépannage seulement. Ainsi, les transactions du DSN seront visibles.
6. Exécutez DART (demande d'autorisation des écarts) d'Anyconnect, amorcez les diagnostics sur Umbrella, puis notez l'heure des échecs du DNS. Consultez la section [Comment recueillir les groupes DART pour Anyconnect pour en savoir plus.](#)
7. Collectez les journaux de diagnostics d'Umbrella, puis envoyez l'URL obtenue à l'administrateur d'OpenDNS. Seuls vous et l'administrateur d'OpenDNS avez accès à cette information. Pour Windows : C :\Program Files (x86) \Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe  
Pour Mac OS X : /opt/Cisco/AnyConnect/bin/UmbrellaDiagnostic

## Informations connexes

- ID de bogue Cisco [CSCvb34863](#) : Temps d'attente lié à la résolution du DNS quand AnyConnect est configuré pour la tunnellation divisée
- [Support et documentation techniques - Cisco Systems](#)