# Anyconnect漫游安全模块部署指南的OpenDNS

## 目录



## 简介

本文描述安装、配置和故障排除步骤漫游模块的OpenDNS的(伞)。从AnyConnect 4.3.X开始，漫游客户端的OpenDNS当前是可用的作为一个集成模块。亦称它是Cloud安全模块，并且PRE部署对终端使用AnyConnect安装程序或者可以从ASA下载通过Web部署。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco AnyConnect 安全移动客户端
- 漫游模块的OpenDNS/伞
- Cisco 自适应安全设备

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco可适应安全工具(ASA)版本9.3(3)7
- Cisco AnyConnect安全移动客户端4.3.01095
- 漫游模块4.3.01095的OpenDNS
- Cisco Adaptive Security Device Manager 7.6.2或以上
- Windows 8.1
- **注意**：最低要求部署OpenDNS伞模块：
  - AnyConnect VPN客户端版本4.3.01095或以上
  - Cisco Adaptive Security Device Manager 7.6.2或以上
  Linux平台当前不支持漫游模块的OpenDNS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请确保您了解所有命令或配置潜在影响。

# 背景信息

## Orginfo.json

对于漫游模块的适当作用OpenDNS，必须从OpenDNS控制板下载或从ASA推送 **Orginfo.json文件** 在使用模块之前。当文件首先下载时，在一个特定路径保存根据操作系统。

对于Mac OS X， **Orginfo.json**下载对/opt/cisco/anyconnect/Umbrella
对于Windows， **Orginfo.json**下载到'C:\ProgramData\Cisco\Cisco **AnyConnect安全移动性客户端 \伞**

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

如显示，文件使用编码的UTF-8并且包含organizationId、指纹和userId。组织ID描述当前登录OpenDNS控制板的用户的组织信息。组织ID是静态，唯一和自动生成的由每个组织的OpenDNS。指纹用于在设备已注册时验证 **Orginfo.json文件，**并且用户ID代表登录用户的一唯一的ID。

当漫游模块在Windows启动， **Orginfo.json文件时**复制对在伞目录下的数据目录并且使用作为工作本。在MAC OS X上，信息从此文件保存对在数据目录的updater.plist在伞目录下。一旦模块顺利地读了从Orginfo.jsonfile的信息 **，**使用网云API，尝试向OpenDNS登记。此注册分配一个唯一设备ID到计算机该已尝试注册的OpenDNS导致。如果从前期注册的一个设备ID已经是可用的，设备跳过注册。

在注册完成以后，漫游模块执行一同步操作获取终端的策略信息。设备ID是必要为了同步操作能工作。同步数据尤其包括syncInterval， whitelisted域和IP地址。同步间隔是分钟数量，在后模块应该尝试到再同时。

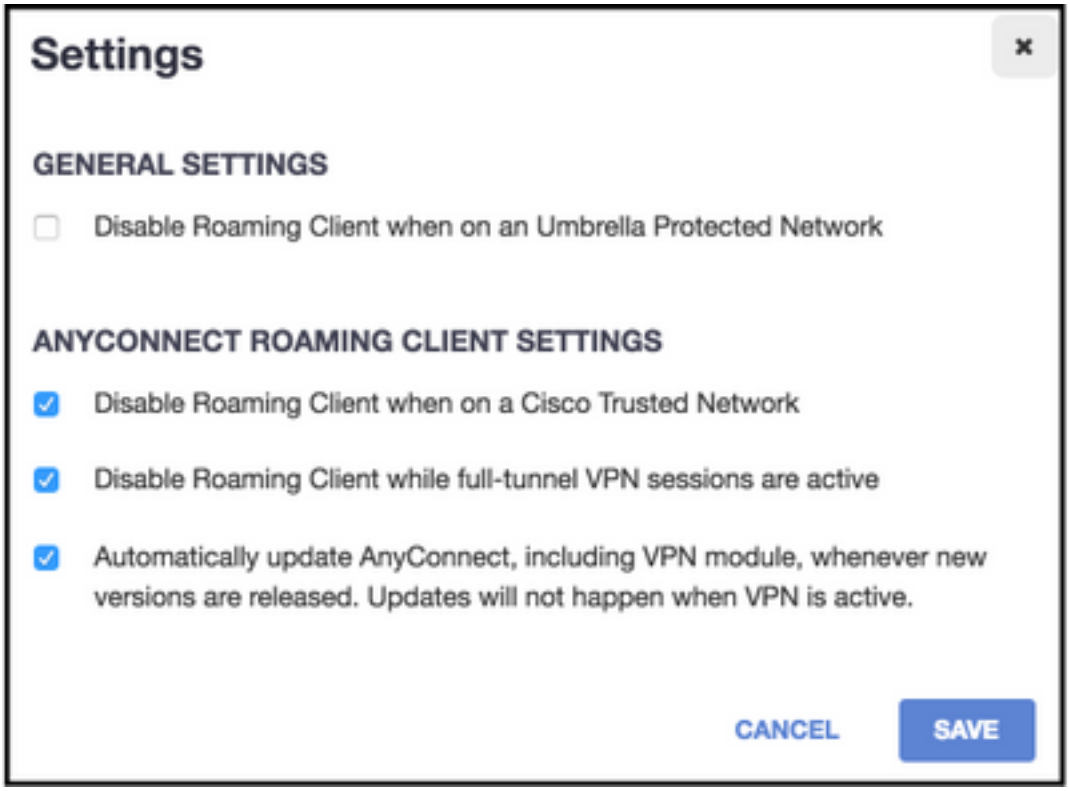
## 探查行为的DNS

在成功的注册和同步，对其本地解析程序的漫游模块发送DNS探测器。这些DNS请求包括debug.opendns.com的TXT查询。凭答复，客户端能确定一个前提OpenDNS虚拟设备(VA)是否在网络存在。

如果VA存在，对‘在后VA’模式的客户端转移和DNS实施在终端没有进行。客户端在DNS实施的VA取决于在网络级。
如果VA不存在，客户端发送DNS请求对OpenDNS公共解析程序(208.67.222.222)使用UDP/443。
肯定答复表明DNS加密是可能的。如果否定答复接收，使用UDP/53，客户端发送DNS请求对OpenDNS公共解析程序。
对此查询的一种肯定答复表明DNS保护是可能的。如果否定答复接收，客户端在几秒钟之内再试查询。
当接收一定量的否定答复后，客户端转移FAIL开放状态。一FAIL开放状态意味着DNS加密和保护不是可能的。一旦漫游模块顺利地有已转换的到一已保护并且/或者已加密状态，搜索域的所有DNS查询在本地搜索域和whitelist域外面被发送对名字解析的OpenDNS解析程序。当已加密状态启用，所有DNS处理由dnscrypt进程加密。

## DNS行为同AnyConnect隧道模式

### 1. 启用的通道所有(或通道所有DNS)




**注意**：如显示，默认行为是为漫游模块禁用DNS保护，当有通道所有配置的一个VPN通道是活跃的时。对于是的模块活跃的在AnyConnect期间通道所有配置，在OpenDNS门户必须不选定**漫游客户端的禁用，当全通道VPN会话是Active选项时**。能力启用此功能要求一先进的订阅级与OpenDNS。下面的信息假设， DNS保护通过漫游模块启用。

**whitelist的被查询的域部份：**

起源于通道适配器的DNS请求允许并且发送到通道DNS服务器，在VPN通道间。如果不可能由通道DNS服务器，解决查询将依然是未解决。

**whitelist的不是被查询的域零件：**

起源于通道适配器的DNS请求允许和是被代理的对OpenDNS公共解析程序通过漫游模块和发送在VPN通道间。对DNS客户端将看起来，好象名字解析通过VPN DNS服务器发生。如果名字解析通过OpenDNS解析程序不是成功的，漫游模块故障切换到本地配置的DNS服务器，从开始是首选的适配器的VPN适配器(当通道是UP)时。

**2. Split-dns (禁用的通道所有DNS)**

**注意**：所有split-dns域自动地被添加到漫游在隧道建立的模块whitelist。这执行提供在AnyConnect和漫游模块之间的一致DNS处理机制。保证在split-dns配置里(与请已分解包括隧道) OpenDNS公共解析程序在已分解包括网络没有包括。

**注意**：在Mac OS X上，如果split-dns为两IP协议(IPv4和IPv6)启用或它为一份协议只启用，并且没有为另一份协议配置的地址池：真的split-dns，类似于Windows，被强制执行。
如果split-dns为一份协议只启用，并且客户端地址为另一份协议分配，只有分割隧道的DNS fallback被强制执行。这意味着AnyConnect只允许匹配split-dns域的DNS请求通过通道(其他请求由AC应答以拒绝的答复强制故障切换到公共DNS服务器)，但是不能通过公共适配器强制执行匹配split-dns域的请求无危险没有发送。

**whitelist的被查询的域部份并且一部分的split-dns域：**

起源于通道适配器的DNS请求允许并且发送到通道DNS服务器，在VPN通道间。匹配的域其他请求从其他适配器将由有'没有这样名称的' AnyConnect驱动程序响应达到真的split-dns (请防止DNS fallback)。所以，非通道仅DNS流量由漫游模块保护。

**whitelist的被查询的不是域部份，但是一部分的split-dns域：**

起源于物理适配器的DNS请求允许并且发送到公共DNS服务器， VPN通道的外部。匹配的域其他请求从通道适配器将由有'没有这样名称的' AnyConnect驱动程序响应防止查询发送在VPN通道间。

**whitelist或split-dns域的不是被查询的域零件：**

起源于物理适配器的DNS请求VPN通道的外部允许和对OpenDNS公共解析程序的被代理的，并且发送。对DNS客户端将看起来，好象名字解析通过公共DNS服务器发生。如果名字解析通过OpenDNS解析程序不成功，漫游模块故障切换到本地配置的DNS服务器，不包括在VPN适配器配置的那个。匹配的域其他请求从通道适配器将由AnyConnect驱动程序响应没有这样名称防止查询发送在VPN通道间。

**3. 已分解包括或已分解排除隧道(没有禁用的split-dns和通道所有DNS)**

**whitelist的被查询的域部份：**

本地OS解析程序执行DNS解析根据大约网络适配器，并且AnyConnect是首选的适配器，当

VPN是活跃的时。DNS请求首先将起源于通道适配器和发送到通道DNS服务器，在VPN通道间。如果查询不可能由通道DNS服务器解决， OS解析程序将尝试通过公共DNS服务器解决它。

**whitelist的不是被查询的域零件：**

本地OS解析程序执行DNS解析根据大约网络适配器，并且AnyConnect是首选的适配器，当VPN是活跃的时。DNS请求首先将起源于通道适配器和发送到通道DNS服务器，在VPN通道间。如果查询不可能由通道DNS服务器解决， OS解析程序将尝试通过公共DNS服务器解决它。

如果OpenDNS公共解析程序是已分解包括列表的已分解排除列表的不是一部分或一部分，被代理的请求在VPN通道间发送
如果OpenDNS公共解析程序不作为已分解包括列表的已分解排除列表的一部分或部分，被代理的请求VPN通道的外部发送

如果名字解析通过OpenDNS解析程序不是成功的，漫游模块故障切换到本地配置的DNS服务器，从开始是首选的适配器的VPN适配器(当通道是UP)时。如果漫游返回的最终答复回到本地DNS客户端的模块(和被代理的)不是成功的，若有本地客户端将尝试其他DNS服务器。

# 安装并且配置漫游模块的伞

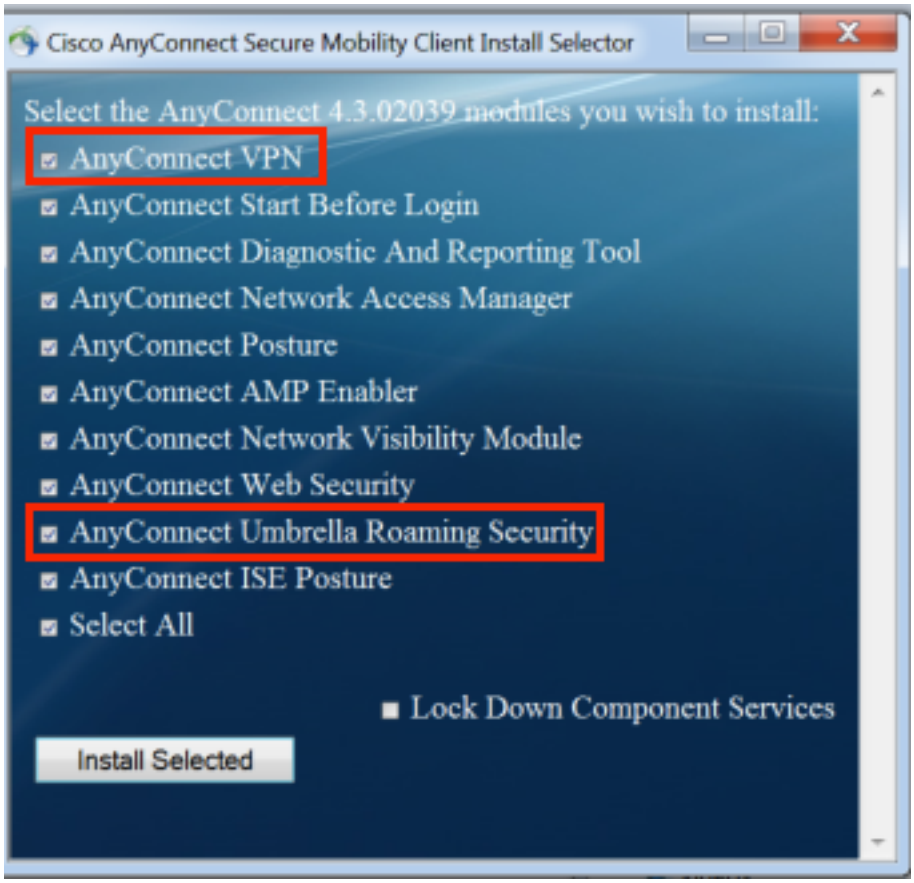
为了集成漫游有AnyConnect VPN客户端的OpenDNS模块，模块需要通过PREdeploment或Web部署方法安装：

## 预部署(手工的)方法

预部署要求漫游模块和复制在用户计算机的OrgInfo.json文件的OpenDNS手工安装。使用企业软件管理系统(SMS)，大规模部署典型地达到。

**部署漫游模块的OpenDNS**

在AnyConnect包安装时请选择Anyconnect VPN和漫游安全模块的Anyconnect伞：




**部署OrgInfo.json**

下载OrgInfo.json文件通过登录OpenDNS控制板和导航对Configuration**>标识>漫游计算机和**点击+sign。把并且选择ModuleProfile移下来**在漫游安全模块部分的**AnyconnectUmbrella下如此镜像所显示：

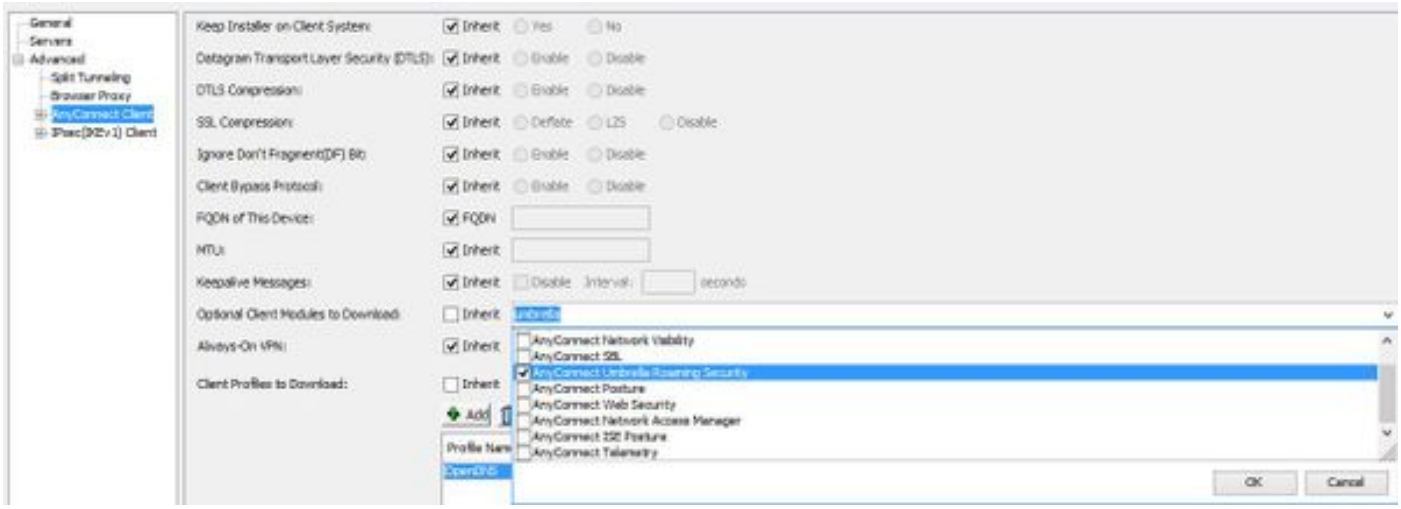

一旦文件下载，必须在这些路径保存根据操作系统。

Mac OS X ：/opt/cisco/anyconnect/Umbrella
Windows ： C:\ProgramData\Cisco\Cisco AnyConnect安全移动性客户端\伞

## Web部署方法

**部署漫游模块的OpenDNS**

下载从Cisco网站的Anyconnect安全移动性客户端(即anyconnect-win-4.3.02039-k9.pkg)包并且上传它对ASA的闪存。一旦上传，在ASDM请去**下载和**选择UmbrellaRoaming**安全的**GroupPolicy **>Advanced > AnyConnect Client>可选客户端模块。**

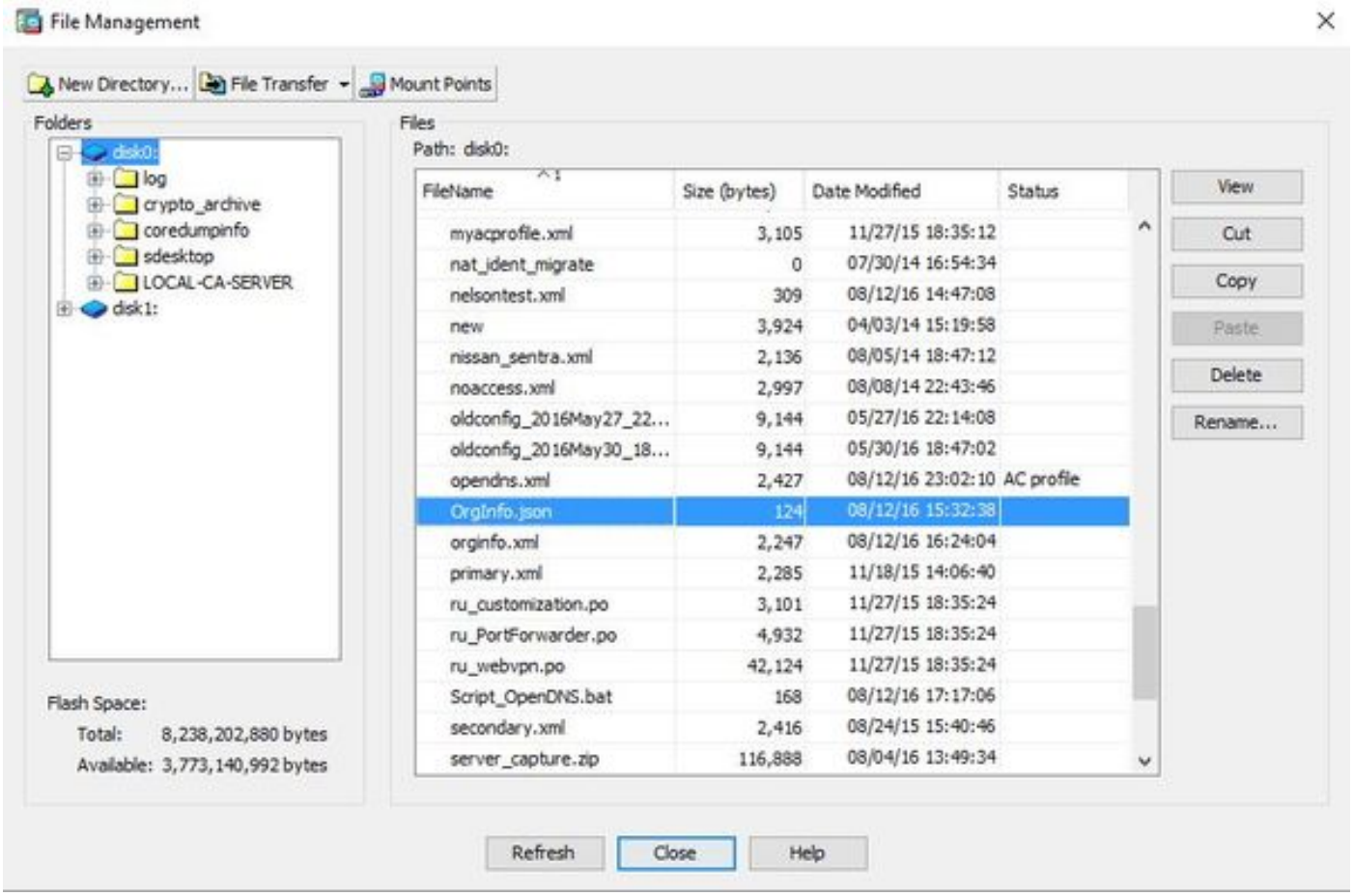



## CLI等同：

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

## 部署Orginfo.json

1. 下载从OpenDNS控制板的Orginfo.json文件并且上传它对ASA的闪存。




2. 配置ASA推送 OrgInfo.json文件到远程终点。

```
webvpn
anyconnect profiles OpenDNS disk0:/orginfo.json
!
!
group-policy <Group_Policy_Name> attribute
```

```
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> **注意**：此配置可能通过CLI只被执行。为了使用ASDM此任务， ASDM版本7.6.2或以上在ASA需要安装。

一旦漫游客户端的伞通过讨论的其中一个方法安装，如此镜像所显示，应该出现作为在AnyConnect GUI内的一个集成模块


直到**Orginfo.json**在正确位置的终端部署，漫游模块的伞不会初始化。

# 配置

部分显示示例必要CLI的配置片断操作漫游模块同多种AnyConnect隧道模式的OpenDNS。

```
!--- 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
```

# 故障排除

排除故障AnyConnect OpenDNS相关问题的步骤：

1.保证漫游安全模块的伞与Anyconnect安全移动性客户端一起安装
2.保证OrgInfo.json是存在终端在根据操作系统的正确路径并且在本文指定的格式
3.如果DNS查询OpenDNS解析程序打算在AnyConnect VPN通道去，请保证发夹在ASA配置允许可接通性到OpenDNS解析程序
4.收集数据包捕获(没有任何过滤器)同时AnyConnect虚拟适配器和物理适配器的并且注释在失败解决的域下
5.如果漫游模块在一已加密状态操作，请在阻塞UDP 443以后收集数据包捕获本地，为了实现故障排除目的只。那里该方式是可见性到DNS处理
6.运行Anyconnect箭，伞诊断并且注释在DNS失败下的时期：

收集箭： https://supportforums.cisco.com/document/12747756/how-collect-dart-bundle-anyconnect

7. 收集伞诊断记录并且发送发生的URL给您的OpenDNS管理员。只有您和OpenDNS管理员访问此信息。

Windows ： ‘C:\Program文件(x86)\Cisco\Cisco AnyConnect安全移动性客户端\UmbrellaDiagnostic.exe

Mac OSX ：/opt/cisco/anyconnect/bin/UmbrellaDiagnostic

# 相关缺陷

CSCvb34863 ：在解决DNS的延迟，当AnyConnect配置为已分解包括隧道