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)。在AnyConnect 4.3.X和以后，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，并且可以predeployed到终端用AnyConnect安装程序，或者可以从可适应的安全工具(ASA)下载通过Web配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco AnyConnect安全移动性
- 漫游模块的OpenDNS/伞
- Cisco ASA

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 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 (ASDM) 7.6.2或以上
- Microsoft Windows 8.1

- **Note**:最低要求配置OpenDNS伞模块是：
  - AnyConnect VPN客户端版本4.3.01095或以上
  - Cisco ASDM 7.6.2或以上
  Linux平台目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OpenDNS，在使用前，正常运行，必须从OpenDNS显示板下载或从ASA推进OrgInfo.json文件模块。当首先下载时文件，被保存在取决于操作系统的一条特定路径。

对于Mac OS X， OrgInfo.json下载到/opt/cisco/anyconnect/Umbrella。
对于Microsoft 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描述目前登录OpenDNS显示板的用户组织信息。组织ID是静态，唯一和主动生成由每个组织的OpenDNS。指纹用于在设备已注册时验证OrgInfo.json文件，并且用户ID表示登录用户的一唯一的ID。

当漫游模块在Windows时启动， OrgInfo.json文件被复制到在伞目录下的数据目录并且使用作为工作本。在MAC OS X上，信息从此文件被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信息从OrgInfo.json文件，尝试向与网云API的OpenDNS登记。此注册分配一个唯一设备ID到机器该尝试的注册的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，漫游模块执行同步操作为了检索终端的策略信息。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。同步间隔是分钟的数量，在后模块应该尝试到再同时。

探查工作情况的DNS

在成功的注册和同步，漫游模块发送域名系统(DNS)探测到其本地解析器。这些DNS请求包括

debug.opendns.com的TXT查询。凭回应，客户端能确定一种前提OpenDNS虚拟工具(VA)是否在网络存在。

如果一种虚拟工具(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。客户端取决于DNS实施的VA在网络级。

如果VA不存在，客户端发送一个DNS请求到OpenDNS公共解析器(208.67.222.222)使用UDP/443。

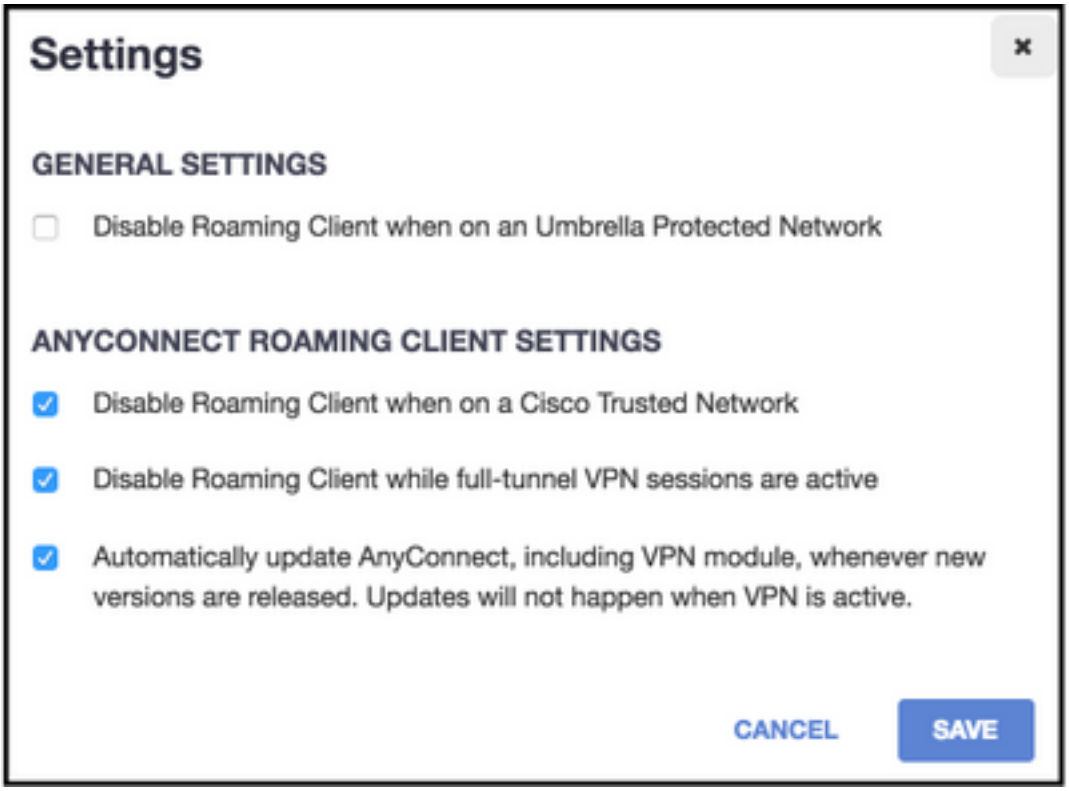
肯定答复表明DNS加密是可能的。如果否定答复接收，使用UDP/53，客户端发送一个DNS请求到OpenDNS公共解析器。

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。

收到一定量的否定答复后，对失败开放状态的客户端转移。一个失败开放状态意味着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对一个保护的并且/或者加密的状态，搜索域的所有DNS查询在本地搜索域和whitelist域外面被发送到名字转换的OpenDNS解析器。有已加密状态功能，所有DNS处理由dnscrypt进程加密。

DNS工作情况同AnyConnect隧道模式

1. 被启用的隧道所有(或隧道所有DNS)



Note:如显示，默认行为是为了漫游模块能禁用DNS保护，当有隧道所有配置的一条VPN隧道是活跃的时。对于是的模块活跃的在AnyConnect期间隧道所有配置，在OpenDNS门户必须不选定**漫游客户端的功能失效，当全通道VPN会话是Active选项时**。能力启用此功能要求与OpenDNS的一个先进的订阅级别。下面的信息假设， DNS保护通过漫游模块是启用的。

Whitelist的被查询的域部份

起源于隧道适配器的DNS请求允许并且被发送到隧道DNS服务器，在VPN隧道间。如果不可能由隧道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

起源于隧道适配器的DNS请求允许和是被代理的对OpenDNS公共解析器通过漫游模块和发送在VPN隧道间。对DNS客户端将看起来，好象名字转换通过VPN DNS服务器发生。如果名字转换通过OpenDNS解析器不是成功的，漫游模块故障切换到本地配置的DNS服务器，从开始是首选适配器的VPN适配器(当隧道是UP)时。

2. Split-dns (被禁用的隧道所有DNS)

> **Note**:所有split-dns域自动地被添加到在隧道建立的漫游模块whitelist。这执行为了提供在AnyConnect和漫游模块之间的一个一致DNS处理机制。保证在split-dns配置(与请已分解包括建立隧道) OpenDNS公共解析器在已分解包括网络没有包括。

> **Note**:在Mac OS X上，如果split-dns为两个IP协议(IPv4和IPv6)是启用的或为一个协议只是启用的，并且没有为另一个协议配置的地址池，真的split-dns类似于Windows被强制执行。如果split-dns为一个协议只是启用的，并且客户端地址为另一个协议分配，只有分割隧道的DNS退路被强制执行。这意味着AnyConnect只允许通过隧道匹配split-dns域的DNS请求(其他请求由AC应答以被拒绝的回应强制故障切换到公共DNS服务器)，但是不能强制执行配比的请求split-dns域没有通过公共适配器无危险被发送。

Whitelist的被查询的域部份并且一部分的Split-dns域

起源于隧道适配器的DNS请求允许并且被发送到隧道DNS服务器，在VPN隧道间。其他要求从其他适配器的配比的域将由有'没有这样名字的' AnyConnect驱动器回应达到真的split-dns (请防止DNS退路)。所以，非隧道仅DNS数据流受漫游模块的保护。

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请求允许并且被发送到公共DNS服务器， VPN隧道的外部。其他要求从隧道适配器的配比的域将由有'没有这样命名的' AnyConnect驱动器回应为了防止查询被发送在VPN隧道间。

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隧道的外部允许和对OpenDNS公共解析器的被代理的，并且被发送。对DNS客户端将看起来，好象名字转换通过公共DNS服务器发生。如果名字转换通过OpenDNS解析器是不成功的，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。其他要求从隧道适配器的配比的域将由AnyConnect驱动器回应没有这样命名为了防止查询被发送在VPN隧道间。

3. 已分解包括或已分解排除建立隧道(没有被禁用的split-dns和隧道所有DNS)

Whitelist的被查询的域部份

本地OS解析器执行DNS解析根据大约网络适配器，并且AnyConnect是首选适配器，当VPN是活跃的时。DNS请求首先将起源于隧道适配器和被发送到隧道DNS服务器，在VPN隧道间。如果查询不可能由隧道DNS服务器解决， OS解析器将尝试通过公共DNS服务器解决它。

Whitelist的不是被查询的域零件

本地OS解析器执行DNS解析根据大约网络适配器，并且AnyConnect是首选适配器，当VPN是活跃的时。DNS请求首先将起源于隧道适配器和被发送到隧道DNS服务器，在VPN隧道间。如果查询不可能由隧道DNS服务器解决， OS解析器将尝试通过公共DNS服务器解决它。

如果OpenDNS公共解析器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隧道间被发送。

如果OpenDNS公共解析器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隧道的外部被发送。

如果名字转换通过OpenDNS解析器不是成功的，漫游模块故障切换到本地配置的DNS服务器，从开始是首选适配器的VPN适配器(当隧道是UP)时。如果漫游回到本地DNS客户端的模块(和被代理的)返回的最终回应不是成功的，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

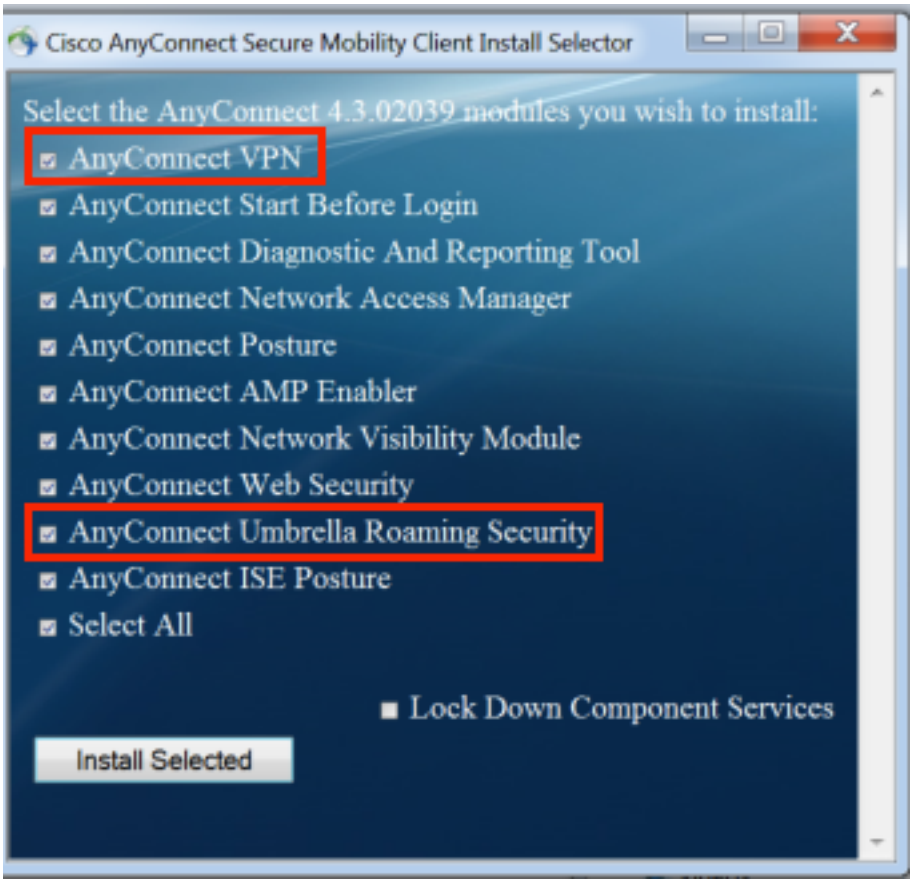
为了集成漫游模块的OpenDNS与AnyConnect VPN客户端，模块需要通过PREdeploment或Web配置方法安装：

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的手工安装。大规模部署用企业软件管理系统(SMS)典型地完成。

配置漫游模块的OpenDNS

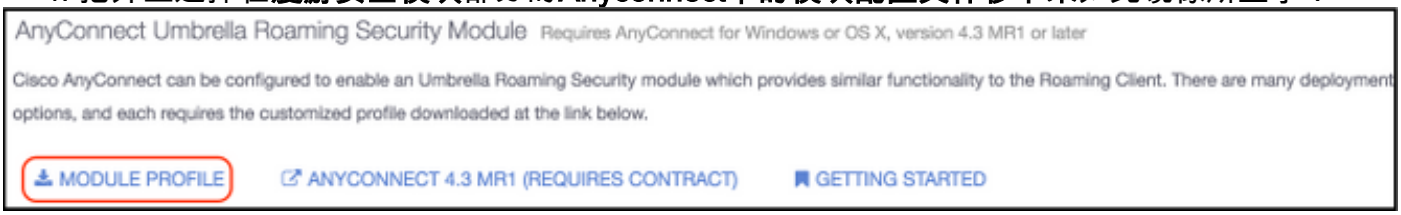
在AnyConnect程序包安装时，请选择**漫游安全模块的AnyConnect VPN**和**AnyConnect伞**：



配置OrgInfo.json

为了下载OrgInfo.json文件，请完成这些步骤：

1. 登录OpenDNS显示板。
2. 选择**Configuration>身份>漫游计算机。**
3. 点击+符号。
4. 把并且选择在**漫游安全模块**部分的**Anyconnect伞的模块配置文件移下来**如此镜像所显示：



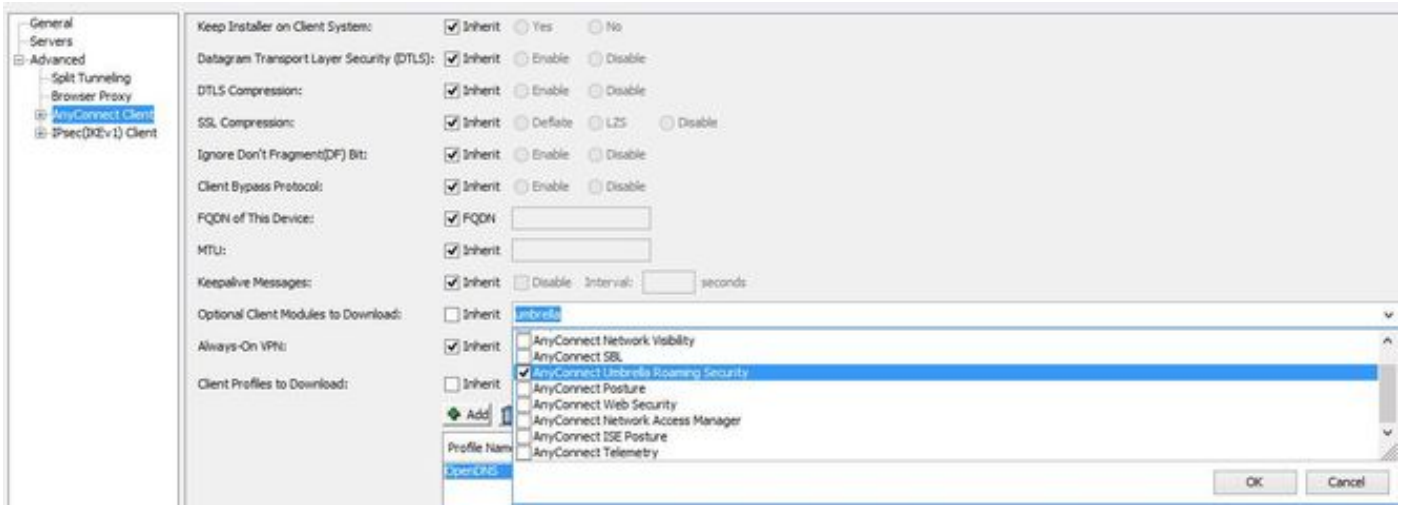
一旦下载文件必须保存一致这些路径，取决于操作系统。

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

Web配置方法

配置漫游模块的OpenDNS

从Cisco网站下载Anyconnect安全移动性客户端程序包(即anyconnect-win-4.3.02039-k9.pkg)并且加载它到ASA的闪存。一旦加载，在ASDM，请选择**组下载**然后选择**伞的策略>Advanced > AnyConnect Client>可选的客户端模块漫游安全。**

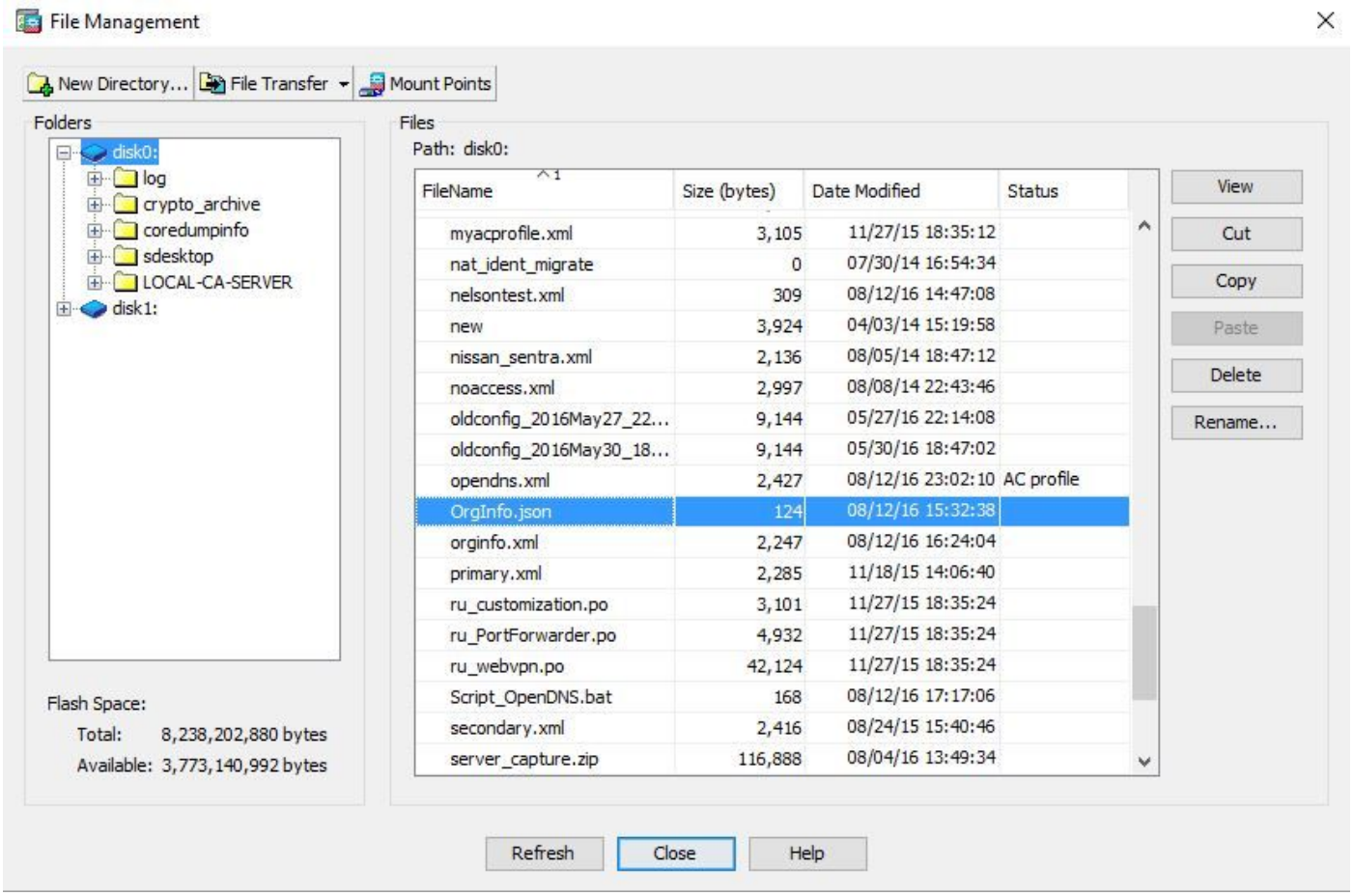


CLI等同

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

配置OrgInfo.json

1. 从OpenDNS显示板下载OrgInfo.json文件并且加载它到ASA的闪存。



2. 配置ASA推进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
```

> **Note**: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或以上需要在ASA上安装。

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在正确的位置的终端配置，漫游模块的伞不会初始化。

配置

部分显示必要示例CLI的配置片断运行漫游模块同多种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
```

验证

当前没有可用于此配置的验证过程。

故障排除

排除AnyConnect OpenDNS相关问题故障的步骤是：

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的路径并且以在本文指定的格式。
3. 如果DNS查询OpenDNS解析器打算在AnyConnect VPN隧道去，请保证两隧道间的本地交换在ASA被配置为了允许可到达性到OpenDNS解析器。
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不能解决的域下。
5. 如果漫游模块在一个已加密状态运行，请在本地阻拦UDP以后收集数据包捕获443，为故障排除的目的只。那里该方式是公开性到DNS处理。
6. 运行AnyConnect箭，伞诊断并且注释在DNS故障下的时期。请参阅如何收集Anyconnect的箭套件欲知更多信息。
7. 收集伞诊断记录并且发送发生的URL到您的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

相关信息

- **Cisco Bug ID CSCvb34863 ：在解决DNS的潜伏期，当AnyConnect配置了为已分解包括建立隧道**
- **技术支持和文档 - Cisco Systems**