Anyconnect OpenDNS 漫游安全模块部署指南

目录

简介

本文档介绍对 OpenDNS (Umbrella) 漫游模块进行安装、配置和故障排除的具体步骤。在 AnyConnect 4.3.X 及更高版本中，OpenDNS 漫游客户端可作为集成模块提供。该模块也称为云安全模块，既可以使用 AnyConnect 安装程序预部署到终端，也可以通过网络部署从自适应安全设备 (ASA) 下载。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科 AnyConnect 安全移动
- OpenDNS/Umbrella 漫游模块
- 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：

- 思科 ASA 版本 9.3(3)7
- 思科 AnyConnect 安全移动客户端 4.3.01095
- OpenDNS 漫游模块 4.3.01095
- 思科自适应安全设备管理器 (ASDM) 7.6.2 或更高版本
- Microsoft Windows 8.1
- **注意**：部署 OpenDNS Umbrella 模块的基本要求：
  - AnyConnect VPN 客户端版本 4.3.01095 或更高版本
  - 思科 ASDM 7.6.2 或更高版本
  OpenDNS 漫游模块目前在 Linux 平台上不受支持。

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。如果您的网络处于活动状态，请确保您了解所有命令或配置的潜在影响。

背景信息

Orginfo.json

要使 OpenDNS 漫游模块正常运行，必须从 OpenDNS 控制面板下载 OrgInfo.json 文件，或者在使用模块前从 ASA 推送该文件。在首次下载时，此文件会保存到特定的路径（视操作系统而定）。

对于 Mac OS X，OrgInfo.json 会下载到 /opt/cisco/anyconnect/Umbrella。
对于 Microsoft Windows，OrgInfo.json 会下载到 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella。

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

如图所示，此文件使用 UTF-8 编码格式，包含组织 ID、指纹和用户 ID。组织 ID 显示当前登录 OpenDNS 控制面板的用户所在组织的信息。对于每个组织，组织 ID 是由 OpenDNS 生成的唯一静态标识。指纹用于在设备注册过程中验证 Orginfo.json 文件；用户 ID 显示登录用户的唯一 ID。

当漫游模块启动后，在 Windows 系统中，OrgInfo.json 文件会被复制到 Umbrella 目录下的数据目录，作为工作副本。在 MAC OS X 系统中，此文件中的信息会被保存到 Umbrella 目录下的数据目录中的 updater.plist 文件。漫游模块成功读取 OrgInfo.json 文件的信息后，会尝试使用云 API 注册到 OpenDNS。通过此注册操作，OpenDNS 会为尝试注册的设备分配一个唯一的设备 ID。如果设备已经具有以前注册时分配的设备 ID，则会跳过注册过程。

注册完成后，漫游模块会执行同步操作，以检索终端的策略信息。设备必须拥有设备 ID，才能执行同步操作。同步数据包括syncInterval、内部旁路域和IP地址等。同步间隔是模块再次同步之前所应等待的分钟数。

DNS 探测行为

成功完成注册和同步后，漫游模块会向本地解析器发送域名系统 (DNS) 探测请求。这些 DNS 请求

中包含对 debug.opendns.com 的 TXT 查询。根据响应结果，客户端可以确定网络中是否存在本地 OpenDNS 虚拟设备 (VA)。

如果网络中存在虚拟设备 (VA)，客户端将切换至“VA 优先”模式，终端上不会执行 DNS 强制操作。客户端会通过 VA 在网络级别执行 DNS 强制操作。

如果网络中不存在 VA，客户端会通过 UDP/443 端口向 OpenDNS 公共解析器 (208.67.222.222) 发送 DNS 请求。

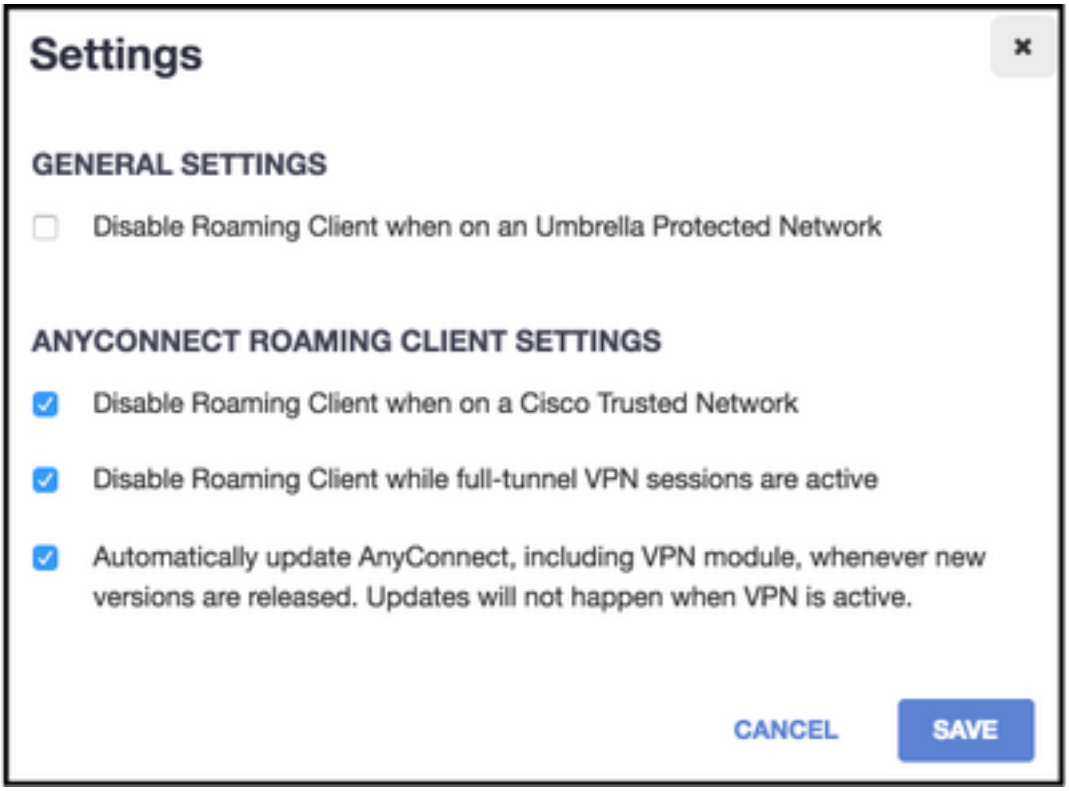
如果得到肯定响应，则表示可以进行 DNS 加密。如果得到否定响应，客户端会通过 UDP/53 端口向 OpenDNS 公共解析器发送 DNS 请求。

如果此查询得到肯定响应，则表示可以获得 DNS 保护。如果得到否定响应，客户端会在几秒后重新尝试发送请求。

如果多次收到否定响应，客户端将切换至“失效开放”状态。“失效开放”状态意味着无法进行 DNS 加密和/或 DNS 保护。漫游模块成功转换到受保护和/或加密状态后，本地搜索域和内部绕行域之外的搜索域的所有DNS查询都将发送到OpenDNS解析器以进行名称解析。在启用加密状态时，所有 DNS 事务都将通过 dnscrypt 进程加密。

启用 AnyConnect 隧道模式时的 DNS 行为

1.全隧道（或启用全隧道DNS）



> **注意**：如图所示，当 VPN 隧道配置为“全部使用隧道”时，漫游模块的默认行为是禁用 DNS 保护。要在 AnyConnect 配置为“全部使用隧道”时启用漫游模块，必须在 OpenDNS 门户上取消选择**禁用“在完全隧道 VPN 会话处于活动状态时漫游客户端”选项。**要启用此功能，必须具有 OpenDNS 的高级订用级别。以下信息假定已启用通过漫游模块的 DNS 保护。

内部旁路列表的查询域部分

允许隧道适配器发起 DNS 请求，这些请求会通过 VPN 隧道发送至隧道 DNS 服务器。如果隧道 DNS 服务器无法解析查询请求，请求将保持未解析状态。

查询域不属于内部旁路列表

允许隧道适配器发起 DNS 请求，这些请求会由漫游模块代理传输至 OpenDNS 公共解析器，并通过 VPN 隧道发送。对于 DNS 客户端，这些请求会表现为已通过 VPN DNS 服务器进行名称解析。如果 OpenDNS 解析器未能成功进行名称解析，漫游模块会故障切换至本地配置的 DNS 服务器，第一个目标是 VPN 适配器（隧道处于正常状态时的首选适配器）。

2.拆分DNS（禁用隧道全DNS）

> **注意：**隧道建立后，所有拆分DNS域都会自动添加到漫游模块内部旁路列表。完成此设置以便在 AnyConnect 和漫游模块之间提供一致的 DNS 处理机制。请确保在分离 DNS 配置下（对分离包括项进行隧道传输），OpenDNS 公共解析器未包括在分离包括项网络中。

> **注意：**在 Mac OS X 系统中，如果对两种 IP 协议（IPv4 和 IPv6）都启用分离 DNS，或者仅对其中一种协议启用分离 DNS，而且没有为另一种协议配置地址池，则会强制执行类似于 Windows 的真正的分离 DNS。
> 如果只对一种 IP 协议启用分离 DNS，并且为另一种 IP 协议分配了客户端地址，则只会强制对分离隧道执行 DNS 回退。这意味着 AnyConnect 仅允许通过隧道来传输与分离 DNS 域匹配的 DNS 请求（其他请求会由 AnyConnect 做出拒绝响应，以强制故障切换至公共 DNS 服务器），但是无法强制规定不允许通过公共适配器发送与分离 DNS 域匹配的明文请求。

查询域内部旁路列表的一部分和拆分DNS域的一部分

允许隧道适配器发起 DNS 请求，这些请求会通过 VPN 隧道发送至隧道 DNS 服务器。来自其他适配器的所有对匹配域的请求会由 AnyConnect 驱动程序做出“无此名称”响应，以实现真正的分离 DNS（阻止 DNS 回退）。 在这种情况下，只有不通过隧道传输的 DNS 流量会受漫游模块保护。

查询域是内部绕行列表的一部分，但不是拆分DNS域的一部分

允许物理适配器发起 DNS 请求，这些请求会从 VPN 隧道外部发送至公共 DNS 服务器。来自隧道适配器的所有对匹配域的请求会由 AnyConnect 驱动程序做出“无此名称”响应，以阻止通过 VPN 隧道发送这些请求。

查询域不属于内部旁路列表或拆分DNS域

允许物理适配器发起 DNS 请求，这些请求会从 VPN 隧道外部代理传输至 DNS 公共解析器。对于 DNS 客户端，这些请求会表现为已通过公共 DNS 服务器进行名称解析。如果 OpenDNS 解析器未能成功进行名称解析，漫游模块会故障切换至本地配置的 DNS 服务器（VPN 适配器上配置的 DNS 服务器除外）。来自隧道适配器的所有对匹配域的请求会由 AnyConnect 驱动程序做出“无此名称”响应，以阻止通过 VPN 隧道发送这些请求。

3.拆分 — 包含或拆分 — 排除隧道（未禁用拆分DNS和隧道全DNS）

内部旁路列表的查询域部分

操作系统原生解析器根据网络适配器的顺序执行 DNS 解析；当启用 VPN 时，AnyConnect 是首选适配器。DNS 请求将首先由隧道适配器发起，并通过 VPN 隧道发送至隧道 DNS 服务器。如果隧

道 DNS 服务器无法解析查询请求，操作系统解析器将尝试通过公共 DNS 服务器来解析请求。

查询域不属于内部旁路列表

操作系统原生解析器根据网络适配器的顺序执行 DNS 解析；当启用 VPN 时，AnyConnect 是首选适配器。DNS 请求将首先由隧道适配器发起，并通过 VPN 隧道发送至隧道 DNS 服务器。如果隧道 DNS 服务器无法解析查询请求，操作系统解析器将尝试通过公共 DNS 服务器来解析请求。

如果 OpenDNS 公共解析器属于分离包括项列表（或不属于分离排除项列表），被代理的请求会通过 VPN 隧道发送。

如果 OpenDNS 公共解析器不属于分离包括项列表（或属于分离排除项列表），被代理的请求会从 VPN 隧道外部发送。

如果 OpenDNS 解析器未能成功进行名称解析，漫游模块会故障切换至本地配置的 DNS 服务器，第一个目标是 VPN 适配器（隧道处于正常状态时的首选适配器）。 如果漫游模块未能成功返回最终响应（并通过代理回退到本地 DNS 客户端），本地客户端将尝试向其他 DNS 服务器（如果有）发送请求。

安装和配置 Umbrella 漫游模块

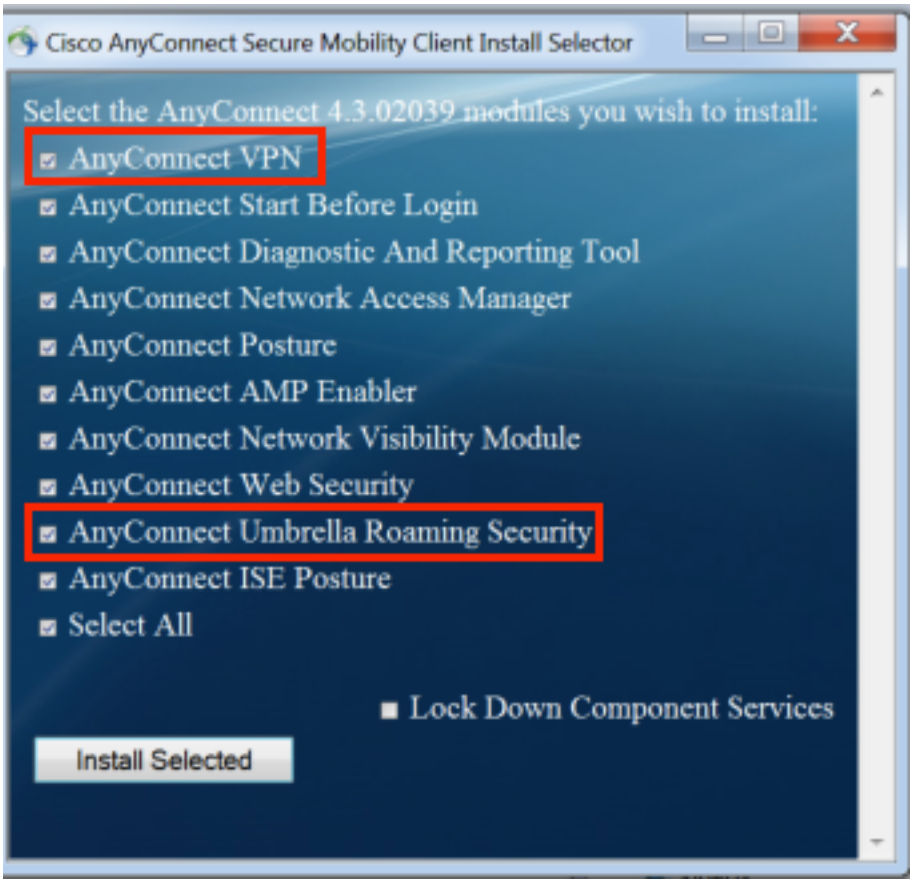
要将 OpenDNS 漫游模块集成到 AnyConnect VPN 客户端，可通过预部署或网络部署两种方式安装漫游模块：

预部署（手动）方法

预部署方法只能以手动方式安装 OpenDNS 漫游模块，并将 OrgInfo.json 文件复制到用户设备。大规模部署通常可以使用企业软件管理系统 (SMS) 来实现。

部署 OpenDNS 漫游模块

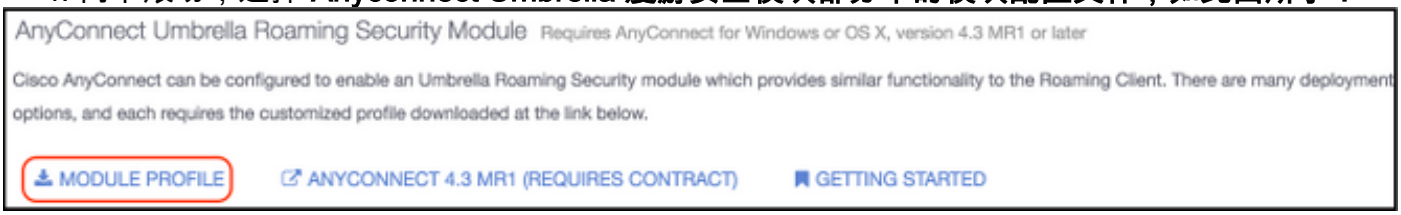
在安装 AnyConnect 软件包的过程中，选择 **AnyConnect VPN 和 AnyConnect Umbrella 漫游安全模块：**



部署 Orginfo.json

要下载 OrgInfo.json 文件，请完成以下步骤：

1. 登录 OpenDNS 控制面板。
2. 依次选择**配置 > 身份 > 漫游计算机。**
3. 点击 + 号。
4. 向下滚动，选择 **Anyconnect Umbrella 漫游安全模块部分中的模块配置文件，如此图所示：**



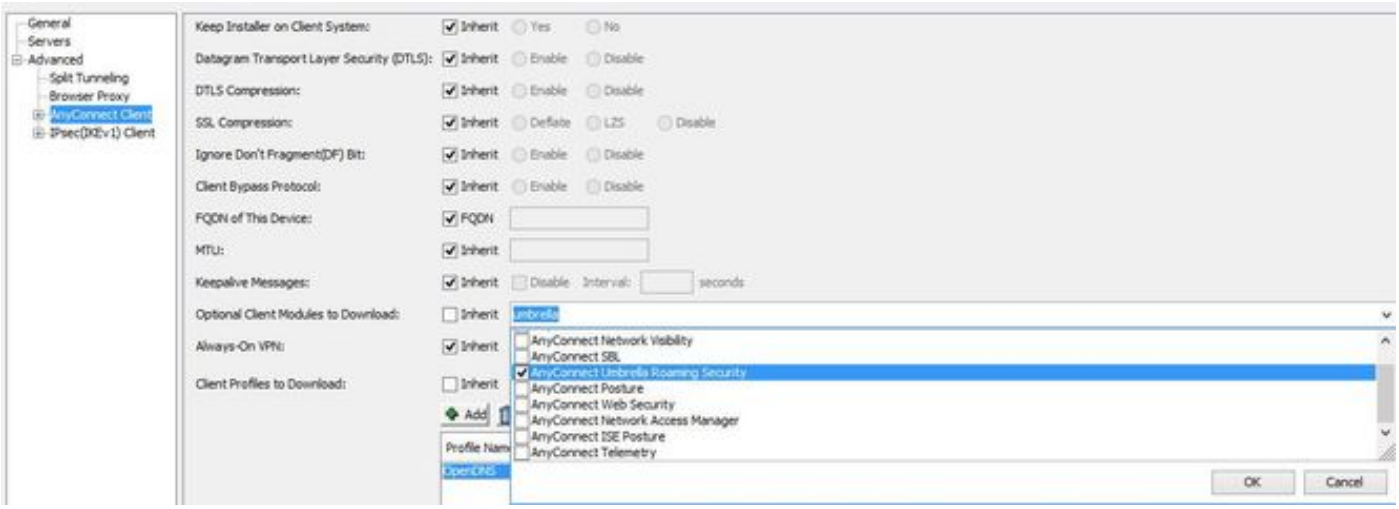
文件下载后，必须将其保存在以下其中一个路径中，具体取决于操作系统。

Mac OS X：/opt/cisco/anyconnect/Umbrella
Windows： C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

网络部署方法

部署 OpenDNS 漫游模块

从思科网站下载 Anyconnect 安全移动客户端 (ASDM) 软件包（即 anyconnect-win-4.3.02039-k9.pkg），然后将其上传到 ASA 的闪存中。上传后，在 ASDM 中，依次选择**组策略 > 高级 > AnyConnect 客户端 > 要下载的可选客户端模块，然后选择 Umbrella 漫游安全。**

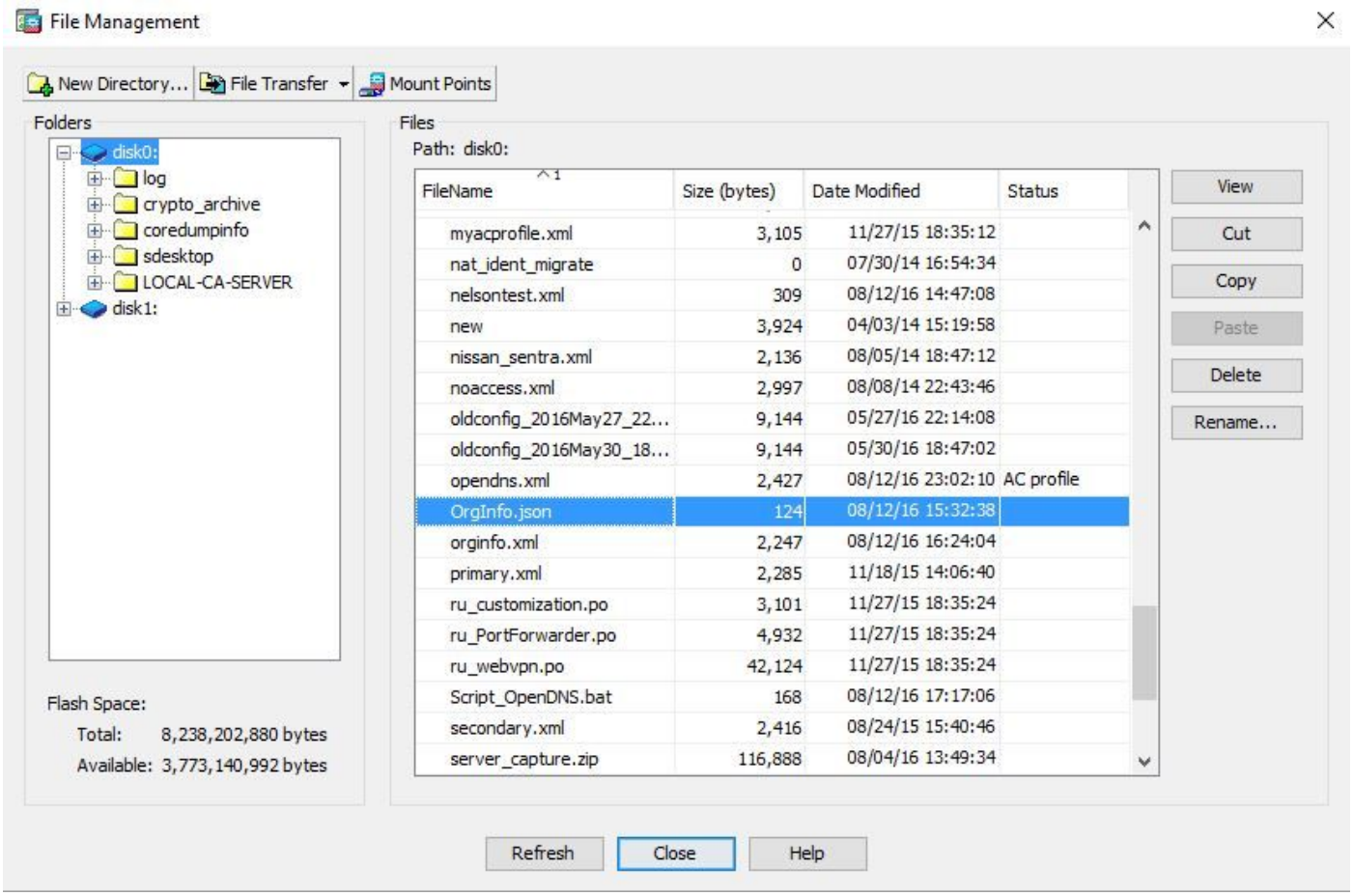


等效的 CLI 命令

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

部署 Orginfo.json

1.从OpenDNS控制面板下载OrgInfo.json文件，并将其上传到ASA的闪存。



2.配置ASA，将OrgInfo.json文件推送到远程终端。

```
webvpn
```

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

> **注意：**此配置只能通过 CLI 执行。要使用 ASDM 来执行此任务，必须在 ASA 上安装 ASDM 版本 7.6.2 或更高版本。

通过上述任何一种方法安装 Umbrella 漫游客户端后，即可看到其作为集成模块显示在 AnyConnect GUI 中（如图所示）：

只有在 Orginfo.json 部署到终端上的正确位置后，Umbrella 漫游模块才会执行初始化。

配置

本节显示在各种 AnyConnect 隧道模式下操作 OpenDNS 漫游模块所需的 CLI 配置代码片段示例。

```
!--- 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
```

验证

当前没有可用于此配置的验证过程。

故障排除

对 AnyConnect OpenDNS 相关问题进行故障排除的步骤如下：

1. 确保设备不仅安装了 Umbrella 漫游安全模块，也安装了 Anyconnect 安全移动客户端。
2. 确保 OrgInfo.json 位于终端上的正确路径之下（注意所使用的操作系统），并且符合本文档中指定的格式。
3. 如果发送至 OpenDNS 解析器的 DNS 查询要通过 AnyConnect VPN 隧道进行传输，请确保在 ASA 上配置发夹，以保证 DNS 查询能够到达 OpenDNS 解析器。
4. 同时收集 AnyConnect 虚拟适配器和物理适配器上的数据包捕获数据（不使用任何过滤器）并记下无法解析的域。
5. 如果漫游模块在加密状态下工作，请在本地阻止 UDP 443 端口后再收集数据包捕获数据（仅出于故障排除目的）。这样可以实现对 DNS 事务的可视性。
6. 运行 Anyconnect DART，进行 Umbrella 诊断，并记下 DNS 发生故障的时间。有关详细信息，请参阅如何收集用于 Anyconnect 的 DART 捆绑包。
7. 收集 Umbrella 诊断日志，并将生成的 URL 发送给您的 OpenDNS 管理员。此信息只有您和 OpenDNS 管理员可以访问。 Windows：C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
   对于Mac OSX:/opt/cisco/anyconnect/bin/UmbrellaDiagnostic

相关信息

- **思科漏洞 ID CSCvb34863：当 AnyConnect 配置为对分离包括项进行隧道传输时，DNS 解析出现延迟**
- **技术支持和文档 - Cisco Systems**