AnyConnect OpenDNS漫遊安全模組部署指南

目錄

簡介

本檔案介紹OpenDNS(Umbrella)漫遊模組的安裝、設定和疑難排解步驟。在AnyConnect 4.3.X及更高版本中，OpenDNS漫遊客戶端現在可用作整合模組。它也稱為雲安全模組，可以通過AnyConnect安裝程式預先部署到終端，也可以通過網路部署從自適應安全裝置(ASA)下載。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco AnyConnect Security Mobility
- OpenDNS/Umbrella漫遊模組
- Cisco ASA

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA版本9.3(3)7
- Cisco AnyConnect安全行動化使用者端4.3.01095
- OpenDNS漫遊模組4.3.01095
- 思科自適應安全裝置管理器(ASDM)7.6.2或更高版本
- Microsoft Windows 8.1
- **附註**：部署OpenDNS Umbrella模組的最低要求是：
  - AnyConnect VPN客戶端版本4.3.01095或更高版本
  - Cisco ASDM 7.6.2或更高版本
  Linux平台當前不支援OpenDNS漫遊模組。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您已瞭解任何指令或組態可能造成的影響。

背景資訊

OrgInfo.json

要使OpenDNS漫遊模組正常工作，必須先從OpenDNS控制面板下載OrgInfo.json檔案，或從ASA推送該檔案，然後才能使用模組。首次下載檔案時，檔案會儲存在特定路徑上，該路徑取決於作業系統。

對於Mac OS X，OrgInfo.json將下載到/opt/cisco/anyconnect/Umbrella。
對於Microsoft Windows，OrgInfo.json將下載到C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella。

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

如圖所示，檔案使用UTF-8編碼，並包含organizationId、fingerprint和userId。組織ID代表當前登入到OpenDNS控制面板的使用者的組織資訊。組織ID是靜態的、唯一的，並且由OpenDNS為每個組織自動生成。指紋用於在裝置註冊期間驗證OrgInfo.json檔案，使用者ID代表登入使用者的唯一ID。

當漫遊模組在Windows上啟動時，OrgInfo.json檔案將複製到Umbrella目錄下的資料目錄，並用作工作副本。在MAC OS X上，此檔案中的資訊將儲存到Umbrella目錄下資料目錄中的updater.plist。模組成功從OrgInfo.json檔案中讀取資訊後，將嘗試使用雲API向OpenDNS註冊。此註冊導致OpenDNS為嘗試註冊的機器分配唯一的裝置ID。如果之前註冊的裝置ID已經可用，則裝置將跳過註冊。

註冊完成後，漫遊模組會執行同步操作以檢索終端的策略資訊。同步操作需要裝置ID才能正常工作。同步資料包括syncInterval、內部旁路域和IP地址等。同步間隔是模組嘗試重新同步之前的分鐘數。

DNS探測行為

成功註冊和同步後，漫遊模組會將域名系統(DNS)探測傳送到本地解析器。這些DNS請求包括debug.opendns.com的TXT查詢。根據響應，客戶端能夠確定網路中是否存在本地OpenDNS虛擬裝

置(VA)。

如果存在虛擬裝置(VA)，則客戶端將轉換到「VA後」模式，並且不會在終端上執行DNS實施。客戶端在網路級別依靠VA執行DNS。

如果沒有VA，則客戶端使用UDP/443向OpenDNS公共解析器(208.67.222.222)傳送DNS請求。

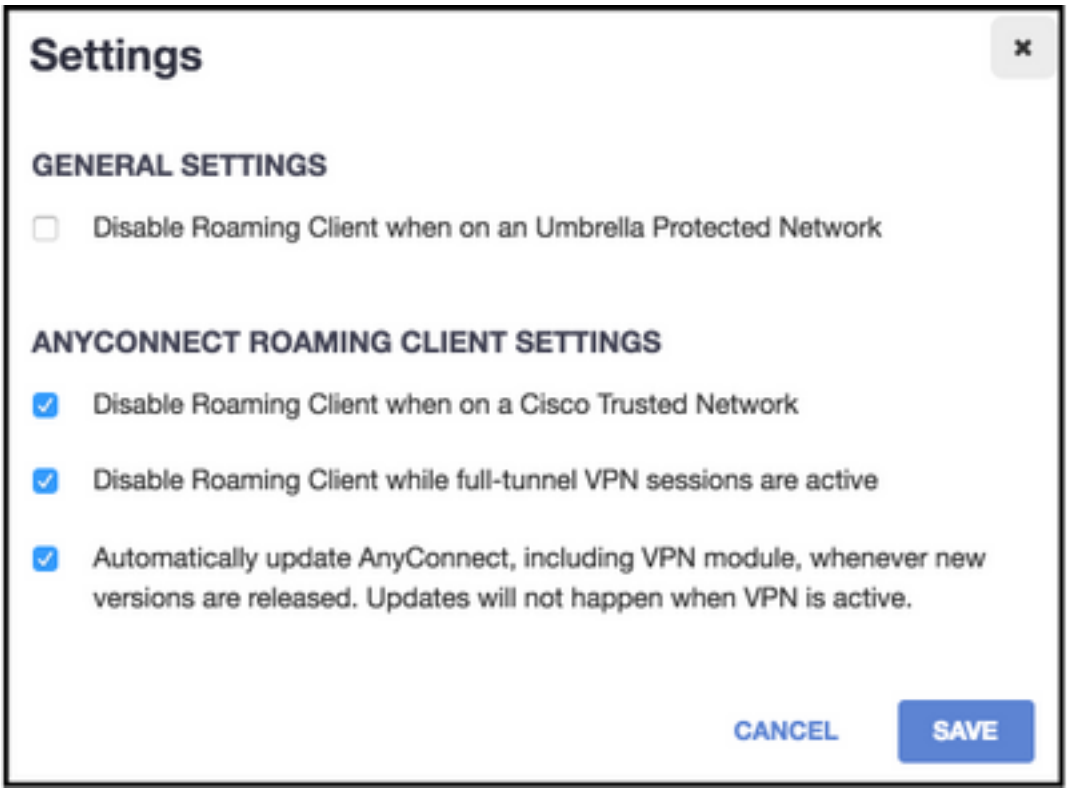
響應為肯定表示可以進行DNS加密。如果收到否定響應，則客戶端使用UDP/53向OpenDNS公共解析器傳送DNS請求。

對此查詢的肯定響應表示可以進行DNS保護。如果收到否定響應，客戶端將在幾秒鐘內重試查詢。

當接收到設定數量的否定響應時，客戶端轉換到失效開放狀態。失效開放狀態表示無法進行DNS加密和/或保護。一旦漫遊模組成功轉換到受保護和/或加密狀態，本地搜尋域和內部旁路域之外的搜尋域的所有DNS查詢都將傳送到OpenDNS解析器進行名稱解析。啟用加密狀態後，所有DNS事務都將由dnscrypt進程加密。

使用AnyConnect隧道模式的DNS行為

1. Tunnel-All（或啟用tunnel-all-DNS）



> **附註**：如圖所示，當具有全隧道配置的VPN隧道處於活動狀態時，漫遊模組會禁用DNS保護。要使模組在AnyConnect全隧道配置期間處於活動狀態，必須在OpenDNS門戶上取消選中**Disable roaming client while full-tunnel VPN sessions is active**選項。啟用此功能需要使用OpenDNS的高級訂閱級別。以下資訊假設已啟用通過漫遊模組的DNS保護。

內部旁路清單的查詢域部分

允許來自隧道介面卡的DNS請求並通過VPN隧道傳送到隧道DNS伺服器。如果隧道DNS伺服器無法解析查詢，則查詢將保持未解析狀態。

查詢的域不是內部旁路清單的一部分

允許來自隧道介面卡的DNS請求，這些請求將通過漫遊模組代理到OpenDNS公共解析器並通過VPN隧道傳送。對於DNS客戶端，它會顯示為通過VPN DNS伺服器進行了名稱解析。如果通過OpenDNS解析器進行的名稱解析不成功，漫遊模組將故障切換到本地配置的DNS伺服器，從VPN介面卡（隧道啟動時首選的介面卡）開始。

2.拆分DNS（禁用隧道所有DNS）

> **附註**：建立隧道後，所有拆分DNS域將自動新增到漫遊模組內部旁路清單中。這樣做是為了在AnyConnect和漫遊模組之間提供一致的DNS處理機制。確保在拆分DNS配置中（使用拆分 — 包含隧道），OpenDNS公共解析器不包括在拆分 — 包含網路中。

> **附註**：在Mac OS X上，如果為兩個IP協定（IPv4和IPv6）都啟用了拆分DNS，或者只為一個協定啟用了拆分DNS，並且沒有為另一個協定配置地址池，則會實施與Windows類似的真正拆分DNS。
> 如果只為一個協定啟用了拆分DNS，而為另一個協定分配了客戶端地址，則只會對拆分隧道實施DNS回退。這意味著AnyConnect僅允許通過隧道與拆分DNS域匹配的DNS請求（其他請求由具有拒絕響應的AC響應，以強制故障切換至公共DNS伺服器），但無法強制通過公共介面卡以明文形式傳送與拆分DNS域匹配的請求。

查詢域是內部旁路清單的一部分，也是拆分DNS域的一部分

允許來自隧道介面卡的DNS請求並通過VPN隧道傳送到隧道DNS伺服器。來自其他介面卡的所有其他匹配域請求將由AnyConnect驅動程式以「無此類名稱」進行響應，以實現真正的拆分DNS（防止DNS回退）。 因此，只有非隧道DNS流量受漫遊模組保護。

查詢的域是內部旁路清單的一部分，但不是拆分DNS域的一部分

允許來自物理介面卡的DNS請求，並將其傳送到VPN隧道之外的公共DNS伺服器。來自隧道介面卡的所有其他匹配域請求將由AnyConnect驅動程式以「無此類名稱」響應，以防止通過VPN隧道傳送查詢。

查詢的域不屬於內部旁路清單或拆分DNS域

允許來自物理介面卡的DNS請求並將其代理到OpenDNS公共解析器，並在VPN隧道外部傳送。對於DNS客戶端，它會顯示為通過公共DNS伺服器進行了名稱解析。如果通過OpenDNS解析器進行的名稱解析失敗，漫遊模組將故障切換到本地配置的DNS伺服器，但不包括VPN介面卡上配置的伺服器。來自隧道介面卡的所有其他匹配域請求將由AnyConnect驅動程式響應（沒有此類名稱），以防止通過VPN隧道傳送查詢。

3.分割 — 包括或分割 — 排除隧道（無分割DNS和隧道全DNS禁用）

內部旁路清單的查詢域部分

本地OS解析程式根據網路介面卡的順序執行DNS解析，當VPN處於活動狀態時，AnyConnect是首選介面卡。DNS請求將首先從隧道介面卡發起，並通過VPN隧道傳送到隧道DNS伺服器。如果隧道DNS伺服器無法解析查詢，作業系統解析程式將嘗試通過公共DNS伺服器解析查詢。

查詢的域不是內部旁路清單的一部分

本地OS解析程式根據網路介面卡的順序執行DNS解析，當VPN處於活動狀態時，AnyConnect是首選介面卡。DNS請求將首先從隧道介面卡發起，並通過VPN隧道傳送到隧道DNS伺服器。如果隧道DNS伺服器無法解析查詢，作業系統解析程式將嘗試通過公共DNS伺服器解析查詢。

如果OpenDNS公共解析器是拆分包括清單的一部分或不是拆分排除清單的一部分，則代理請求通過VPN隧道傳送。

如果OpenDNS公共解析器不是拆分包括清單的一部分或拆分排除清單的一部分，則代理請求會傳送到VPN隧道之外。

如果通過OpenDNS解析器進行的名稱解析不成功，漫遊模組將故障切換到本地配置的DNS伺服器，從VPN介面卡（隧道啟動時首選的介面卡）開始。 如果漫遊模組返回的最終響應（並代理回本機DNS客戶端）不成功，則本機客戶端將嘗試其他DNS伺服器（如果可用）。

安裝和配置Umbrella漫遊模組

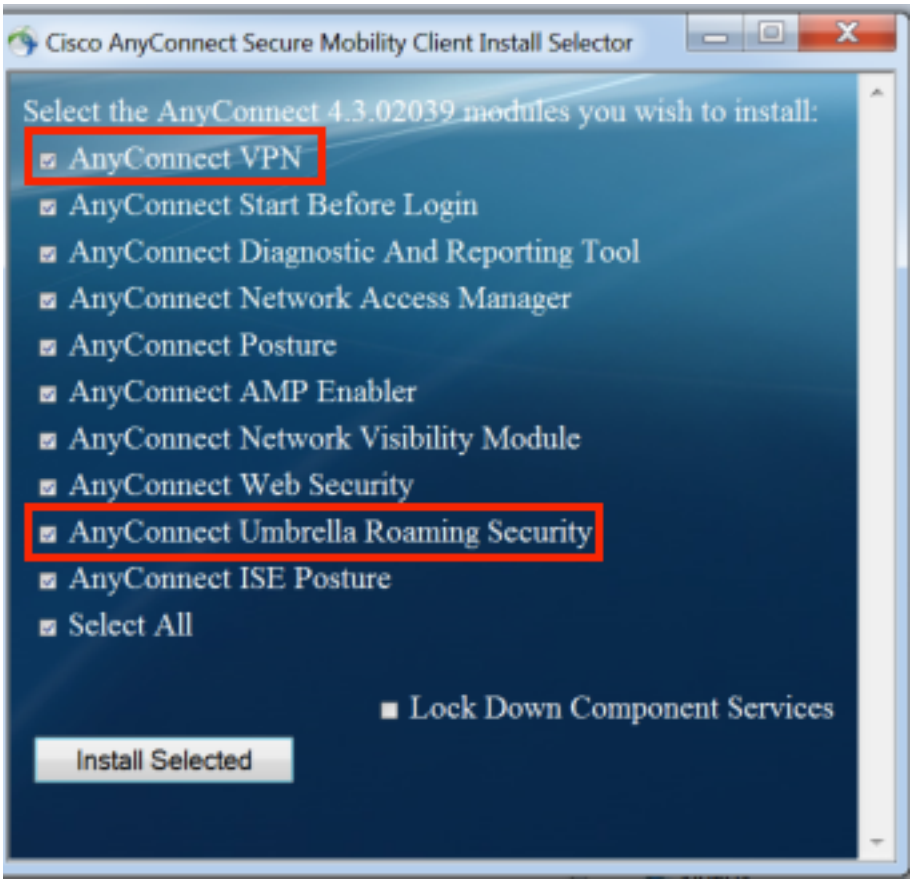
為了將OpenDNS漫遊模組與AnyConnect VPN客戶端整合，需要通過預部署或Web部署方法安裝該模組：

預部署（手動）方法

預部署要求手動安裝OpenDNS漫遊模組並在使用者電腦上複製OrgInfo.json檔案。通常使用企業軟體管理系統(SMS)實現大規模部署。

部署OpenDNS漫遊模組

在AnyConnect軟體包安裝過程中，選擇**AnyConnect VPN**和**AnyConnect Umbrella Roaming Security**模組：



部署OrgInfo.json

要下載OrgInfo.json檔案，請完成以下步驟：

1. 登入到OpenDNS控制面板。
2. 選擇**Configuration > Identities > Roaming Computers。**
3. 按一下**+**符號。
4. 向下滾動並選擇**Anyconnect Umbrella Roaming Security Module**部分中的**Module Profile**，如下圖所示：

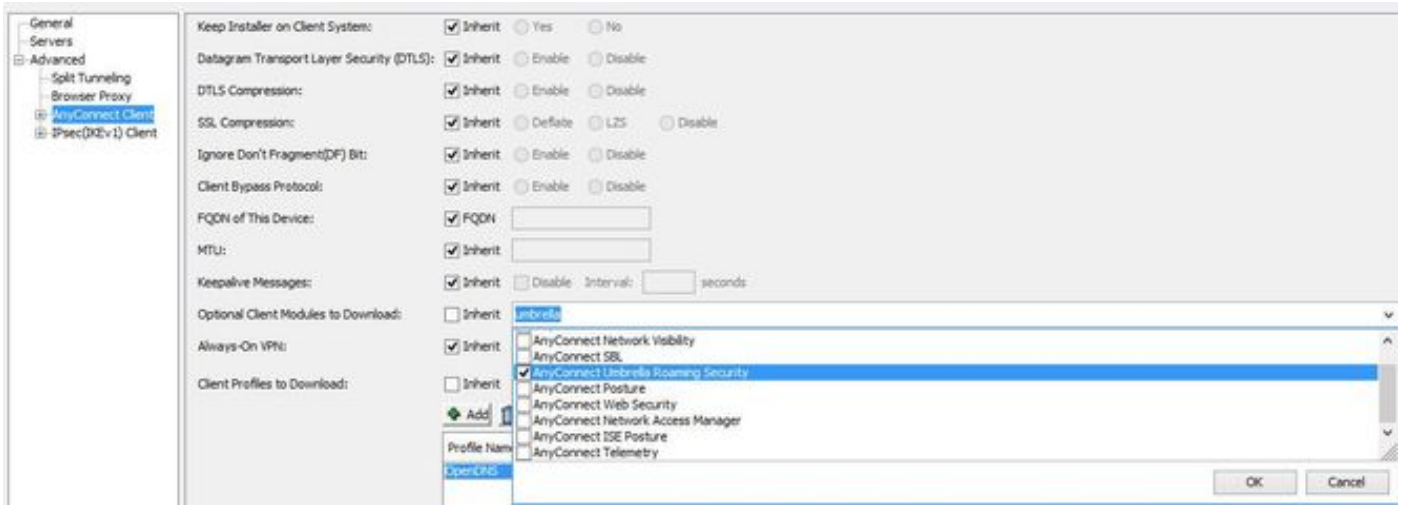
下載檔案後，必須將其儲存在其中一個路徑上，視作業系統而定。

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

Web部署方法

部署OpenDNS漫遊模組

從思科網站下載Anyconnect安全移動客戶端軟體包(即anyconnect-win-4.3.02039-k9.pkg)並將其上傳到ASA的快閃記憶體中。上傳後，在ASDM中選擇**Group Policy > Advanced > AnyConnect Client > Optional Client Modules to Download**，然後選擇**Umbrella Roaming Security。**

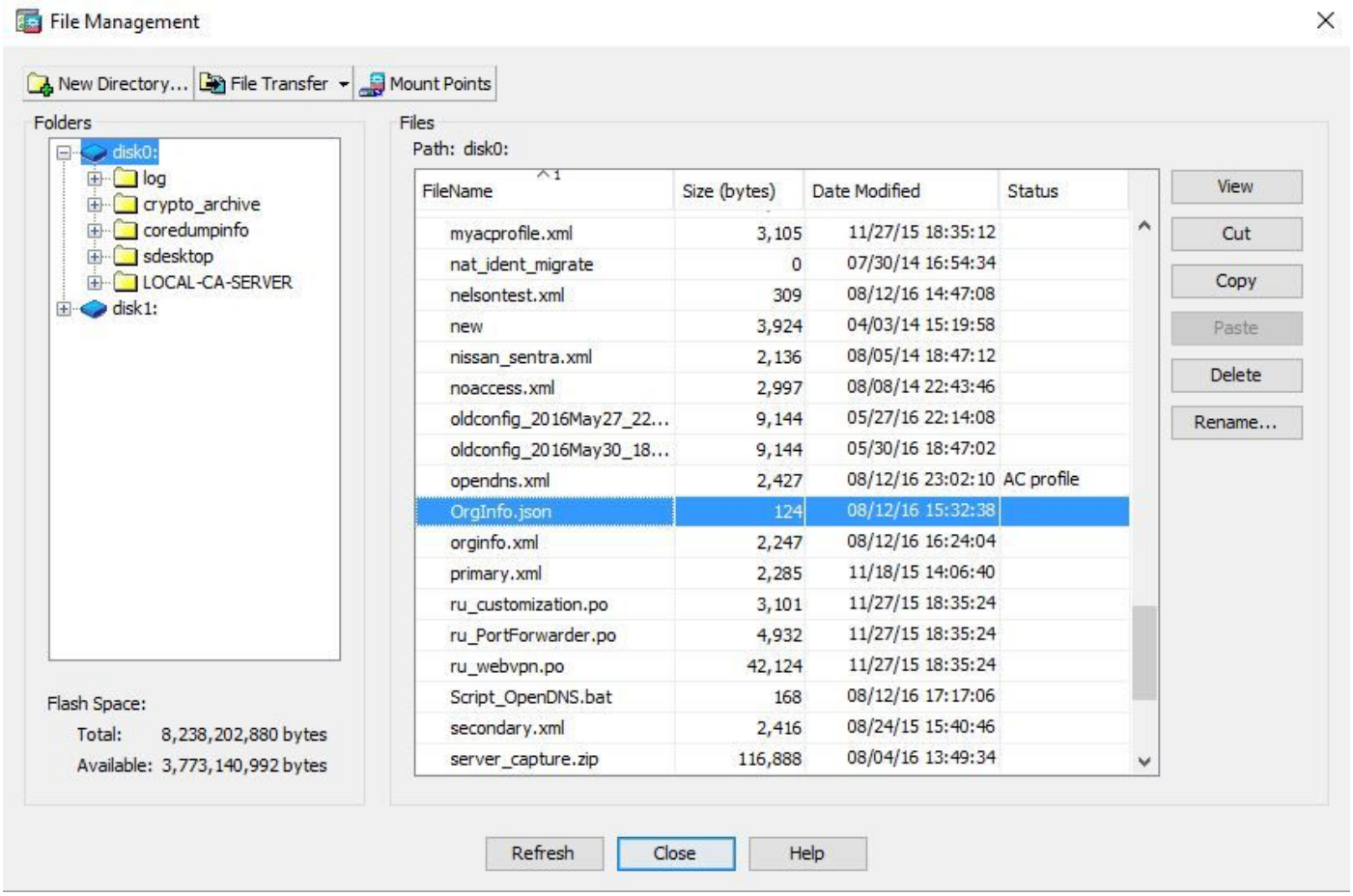


等效的CLI

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

部署OrgInfo.json

1.從OpenDNS儀表板下載OrgInfo.json檔案，並將其上傳到ASA的快閃記憶體。



2.配置ASA以將OrgInfo.json檔案推送到遠端終端。

```
webvpn
```

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

附註：此配置只能通過CLI執行。為了將ASDM用於此任務，需要在ASA上安裝ASDM 7.6.2版或更高版本。

一旦通過所討論的其中一種方法安裝Umbrella漫遊客戶端，它應該會顯示為AnyConnect GUI中的整合模組，如下圖所示：

在終端上正確位置部署OrgInfo.json之前，不會初始化Umbrella漫遊模組。

設定

本節顯示使用各種AnyConnect隧道模式運行OpenDNS漫遊模組所必需的示例CLI配置片段。

```
!--- 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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

排除AnyConnect OpenDNS相關問題的步驟如下：

1. 確保Umbrella漫遊安全模組與Anyconnect安全移動客戶端一起安裝。
2. 確保OrgInfo.json存在於基於作業系統的正確路徑上的終結點上，並且採用本文檔中指定的格式。
3. 如果對OpenDNS解析器的DNS查詢旨在通過AnyConnect VPN隧道，請確保在ASA上配置了髮夾以允許對OpenDNS解析器的可訪問性。
4. 同時收集AnyConnect虛擬介面卡和物理介面卡上的資料包捕獲（沒有任何過濾器），並記下無法解析的域。
5. 如果漫遊模組在加密狀態下運行，請在本地阻止UDP 443後收集資料包捕獲，僅用於故障排除。這樣，就可以看到DNS事務。
6. 運行AnyConnect DART、Umbrella診斷程式，並記下DNS失敗的時間。如需詳細資訊，請參閱如何收集Anyconnect的DART套件。
7. 收集Umbrella診斷日誌並將生成的URL傳送到OpenDNS管理員。只有您和OpenDNS管理員有權訪問此資訊。 對於Windows:C:\Program檔案(x86)\Cisco\Cisco AnyConnect安全移動客戶端\UmbrellaDiagnostic.exe
   對於Mac OSX:/opt/cisco/anyconnect/bin/UmbrellaDiagnostic

相關資訊

- **思科錯誤ID CSCvb34863:為分割包含隧道配置AnyConnect時，解析DNS時的延遲**
- **技術支援與文件 - Cisco Systems**