AnyConnect OpenDNS ローミング セキュリティモジュール 配置ガイド

目次

概要

このドキュメントでは、OpenDNS（Umbrella）モジュールのインストール、設定、およびトラブルシューティングの手順について説明します。 AnyConnect 4.3.X 以降、OpenDNS Roaming クライアントを統合モジュールとして使用できるようになりました。 これはクラウド セキュリティ モジュールとしても知られ、AnyConnect インストーラを使用してエンドポイントに事前展開したり、Web 展開を使用して ASA（Adaptive Security Appliance）からダウンロードしたりすることができます。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco AnyConnect セキュア モビリティ
- OpenDNS/Umbrella Roaming モジュール
- Cisco ASA

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA バージョン 9.3(3)7
- Cisco AnyConnect セキュア モビリティ クライアント 4.3.01095
- OpenDNS Roaming モジュール 4.3.01095
- Cisco Adaptive Security Device Manager （ ASDM ） 7.6.2 またはそれ以降
- Microsoft Windows 8.1

- **注:** OpenDNS Umbrella モジュールを配置する最小限の要件は次のとおりです:
  - AnyConnect VPN クライアント バージョン 4.3.01095 以降
  - Cisco ASDM 7.6.2 またはそれ以降
  OpenDNS ローミング モジュールは Linux プラットフォームで現在サポートされません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドまたは設定の影響について十分に理解したうえで作業してください。

背景説明

Orginfo.json

適切に機能する OpenDNS ローミング モジュールに関しては OrgInfo.json ファイルは OpenDNS ダッシュボードからモジュールが使用される前にダウンロードされるか、または ASA から押す必要があります。 ファイルは最初にダウンロードされるとき、オペレーティング システムによって決まる特定のパスで保存されます。

Mac OS X に関しては、OrgInfo.json は /opt/cisco/anyconnect/Umbrella にダウンロードされます。
Microsoft Windows に関しては、OrgInfo.json は C:\ProgramData\Cisco\Cisco AnyConnect セキュア モビリティ クライアント\ Umbrella にダウンロードされます。

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

示されているように、ファイルは UTF-8 エンコードを使用し、organizationId、フィンガープリントおよび USERID が含まれています。 組織ID は現在 OpenDNS ダッシュボード ログイン されるユーザ向けの組織情報を示します。 組織ID は静的、ユニーク、および各組織のための OpenDNS によって自動生成されてです。 フィンガープリントがデバイス登録の間に OrgInfo.json ファイルを検証するのに使用され、ユーザー ID はログイン ユーザ向けのユニークな ID を表します。

ローミング モジュールが Windows で開始するとき、OrgInfo.json ファイルは Umbrella ディレク

トリの下のデータディレクトリにコピーされ、作業用コピーとして使用されます。 Mac OS X では、このファイルからの情報は Umbrella ディレクトリの下の data ディレクトリ内の updater.plist に保存されます。 モジュールが正常に OrgInfo.json ファイルからの情報を読んだら、クラウド API との OpenDNS と登録するように試みます。 この登録により、OpenDNS は登録を試行したマシンに一意のデバイス ID を割り当てます。 前の登録のデバイス ID が使用可能な場合、デバイスは登録をスキップします。

登録が完了する後、ローミング モジュールはエンド ポイントのためのポリシー情報を検索するために同期化オペレーションを行います。 同期操作を実行するにはデバイス ID が必要です。 同期化データは syncInterval、whitelisted ドメインおよび IP アドレスがとりわけ含まれています。 同期間隔は、モジュールが再同期を試行した後に経過する分の数です。

DNS プローブの動作

正常な登録および同期化に、ローカル リゾルバへのローミング モジュール送信ドメイン ネーム システム（DNS）プローブ。 このような DNS 要求には、debug.opendns.com の TXT クエリが含まれます。 応答に基づいて、クライアントは、オンプレミスの OpenDNS 仮想アプライアンス（VA）がネットワークに存在するかどうかを判断できます。

バーチャル アプライアンス（VA）がある場合、「の後ろ VA」モードへのクライアントの移行、および DNS 適用はエンド ポイントで実行された。 クライアントがネットワーク レベルで DNS の適用を実行するかどうかは、VA に依存します。

VA が存在しない場合、クライアントは UDP/443 を使用して、OpenDNS パブリック リゾルバ（208.67.222.222）に DNS 要求を送信します。

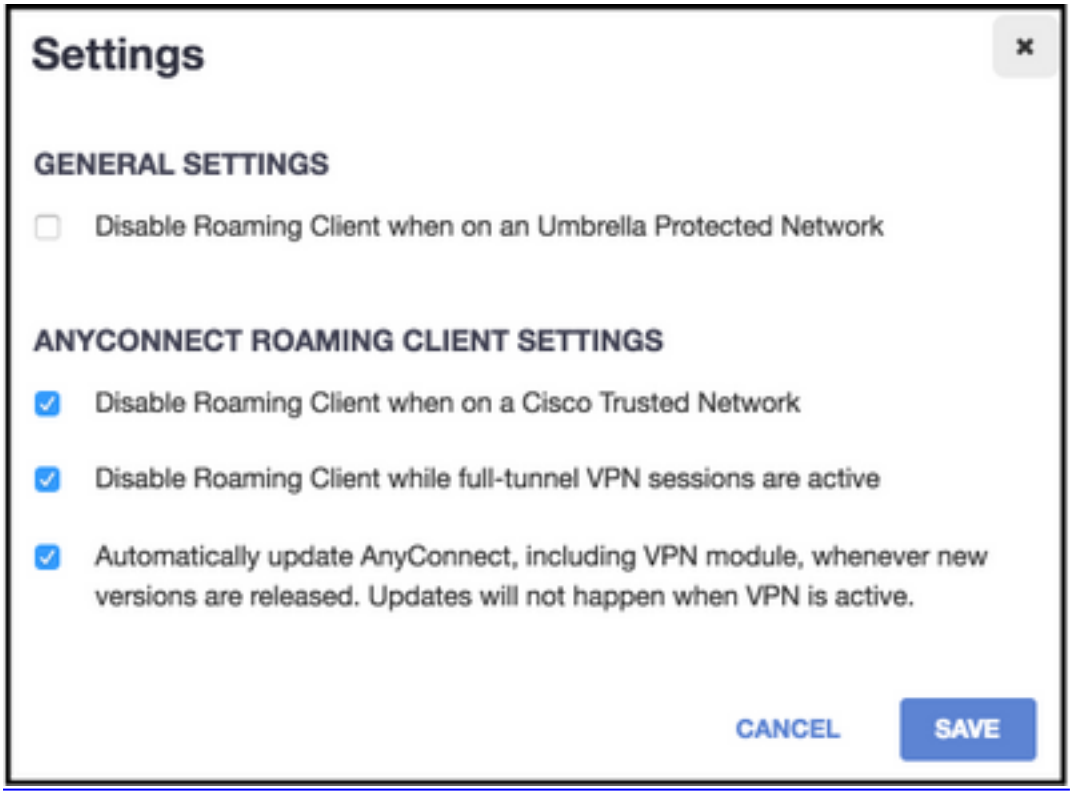
肯定応答は、DNS の暗号化が可能であることを示します。 否定応答を受信する場合、クライアントは UDP/53 を使用して、OpenDNS パブリック リゾルバに DNS 要求を送信します。

このクエリに対する肯定応答は、DNS の保護が可能であることを示します。 否定応答を受信する場合、クライアントは数秒以内にクエリを再試行します。

障害開いた状態への一定数の否定応答を受取り次第、クライアントの移行。 フェイルオープン状態は、DNS の暗号化や保護が不可能であることを意味します。 Roaming モジュールが保護された状態および/または暗号化された状態に遷移すると、ローカル検索ドメインとホワイトリスト ドメイン以外の検索ドメインのすべての DNS クエリが OpenDNS リゾルバに送信され、名前解決が行われます。 暗号化された状態が有効になっているすべての DNS トランザクションは、dnscrypt プロセスによって暗号化されます。

AnyConnect トンネル モードでの DNS の動作

1. Tunnel-All（または tunnel-all-DNS が有効）



注: 示されているように、デフォルトの動作は DNS 保護を無効に するローミング モジュールのためトンネルすべての設定の VPN トンネルがアクティブな間、です。 AnyConnect tunnel-all の設定時にモジュールをアクティブにするには、OpenDNS ポータルで [full-tunnel VPNセッションがアクティブのときにRoamingクライアントを無効にする (Disable roaming client while full-tunnel VPN sessions are active)] オプションをオフにする必要があります。 この機能を有効にするには、OpenDNS で拡張サブスクリプション レベルが設定されていることが必要です。 情報は下記のローミング モジュールでの DNS 保護がイネーブルになっていると仮定します。

ホワイトリストの問い合わせられたドメイン部

トンネル アダプタから発信される DNS 要求が許可され、VPN トンネルを介してトンネルの DNS サーバに送信されます。 トンネルの DNS サーバがクエリを解決できない場合、未解決のままになります。

問い合わせられたドメイン ホワイトリストのない部品

トンネル アダプタから発信される DNS 要求が許可され、Roaming モジュールを介して OpenDNS パブリック リゾルバにプロキシされ、VPN トンネル経由で送信されます。 DNS クライアントには、名前解決が VPN DNS サーバ経由で実行されたかのように見えます。 OpenDNS リゾルバによるネーム・リゾリューションが正常ではない場合、ローミング モジュールは (好まれたにはじまってローカルで設定された DNSサーバにトンネルが稼働している間、) 、アダプタである VPN アダプタ壊れます。

2. Split-DNS (tunnel-all-DNS が無効)

注: すべての分割DNS ドメインはトンネル確立にローミング モジュール whitelist に自動的に追加されます。 これは AnyConnect とローミング モジュール間の一貫した DNS 処理機構を提供するためにされます。 split-DNS 設定 (split-include トンネリングを使用) で、OpenDNS パブリック リゾルバが split-include ネットワークに含まれないようにします。

注: Mac OS X で、分割DNS が両方の IP プロトコル（IPv4 および IPv6）のためにイネーブルになっているか、または 1 つのプロトコルのためだけにイネーブルになって、他のプロトコルのために設定されるアドレス プールがありません Windows と同じような本当分割 DNS は実施されます。
split-DNS が 1 つだけのプロトコルに対して有効になっており、クライアント アドレスが他のプロトコルに割り当てられている場合、split-tunneling 用の DNS フォールバックのみ適用されます。 これは分割DNS ドメイン トンネルで一致する（公共 DNSサーバにフェールオーバーを強制する他の要求は拒否された応答の AC によって答えます）、しかし分割DNS ドメインを一致する要求がパブリックアダプターで明白に送信 されないこと実施できない AnyConnect が割り当てだけ DNS 要求することを意味します。

ホワイトリストの問い合わせられたドメイン部および分割DNS ドメインのまた一部

トンネル アダプタから発信される DNS 要求が許可され、VPN トンネルを介してトンネルの DNS サーバに送信されます。 他のアダプタからの一致するドメインのための他の要求はすべて「そのような名前」の AnyConnect ドライバによって本当分割DNS を実現させるために応答されません（DNS フォールバックを防いで下さい）。 したがって、非トンネル DNS トラフィックのみが Roaming モジュールによって保護されます。

ホワイトリストの問い合わせられたドメイン部、しかし分割DNS ドメインのない一部

物理アダプタから発信される DNS 要求が許可され、VPN トンネルの外部のパブリック DNS サーバに送信されます。 トンネル アダプタからの一致するドメインのための他の要求はすべて「そのようなネーム」の AnyConnect ドライバによってクエリが VPN トンネルを渡って送信 されることを防ぐために応答されません。

問い合わせられたドメイン ホワイトリストまたは分割DNS ドメインのない部品

物理アダプタから発信される DNS 要求が許可され、OpenDNS パブリック リゾルバにプロキシされ、VPN トンネルの外部に送信されます。 DNS クライアントには、名前解決がパブリック DNS サーバ経由で実行されたかのように見えます。 OpenDNS リゾルバによるネーム・リゾリューションが不成功である場合、ローミング モジュールは VPN アダプタで設定される物を除いてローカルで設定された DNSサーバに、壊れます。 トンネル アダプタからの一致するドメインのための他の要求はすべてそのようなネーム無しで AnyConnect ドライバによってクエリが VPN トンネルを渡って送信 されることを防ぐために応答されます。

3. Split-include または Split-exclude トンネリング（split-DNS および tunnel-all-DNS は無効でない）

ホワイトリストの問い合わせられたドメイン部

ネイティブ OS リゾルバは、ネットワーク アダプタの順序に基づいて DNS 解決を実行し、VPN がアクティブのときは AnyConnect が優先アダプタになります。 DNS 要求は最初にトンネル アダプタから発信され、VPN トンネル経由でトンネル DNS サーバに送信されます。 クエリをトンネル DNS サーバで解決できない場合、OS リゾルバはパブリック DNS サーバ経由でそれを解決しようとします。

問い合わせられたドメイン ホワイトリストのない部品

ネイティブ OS リゾルバは、ネットワーク アダプタの順序に基づいて DNS 解決を実行し、VPN がアクティブのときは AnyConnect が優先アダプタになります。 DNS 要求は最初にトンネル ア

ダプタから発信され、VPN トンネル経由でトンネル DNS サーバに送信されます。 クエリをトンネル DNS サーバで解決できない場合、OS リゾルバはパブリック DNS サーバ経由でそれを解決しようとします。

OpenDNS 公共リゾルバが分割含リストの一部分割除リストの一部であるかどうか、proxied 要求は VPN トンネルを渡って送信 されます。

OpenDNS 公共リゾルバが分割含リストの一部または分割除リストの一部ではない場合、proxied 要求は VPN トンネルの外部で送信 されます。

OpenDNS リゾルバによるネーム・リゾリューションが正常ではない場合、ローミング モジュールは（好まれたにはじまってローカルで設定された DNSサーバにトンネルが稼働している間、）、アダプタである VPN アダプタ壊れます。 ローミング モジュールによって（返されるおよびネイティブ DNS クライアントに戻って proxied）最終的な応答が正常ではない場合、ネイティブクライアントは他の DNSサーバを、もし可能であれば試みます。

Umbrella Roaming モジュールのインストールおよび設定

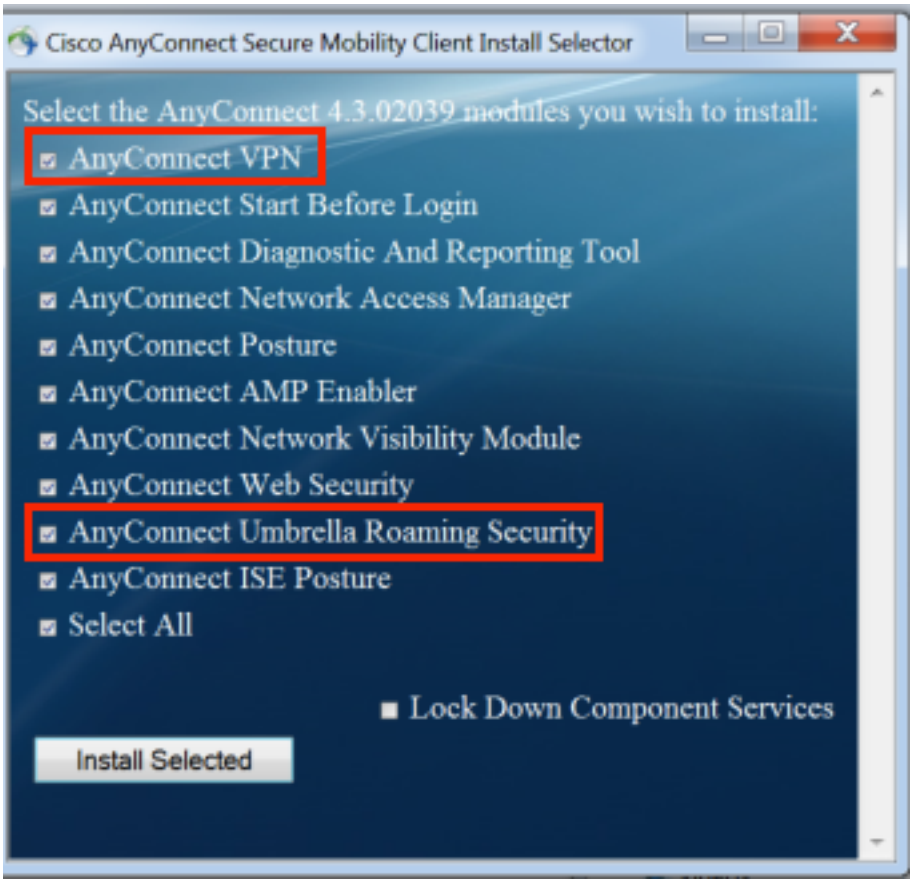
OpenDNS Roaming モジュールを AnyConnect VPN クライアントと統合するには、モジュールを事前展開方式または Web 展開方式のいずれかでインストールする必要があります。

事前展開（手動）方式

配置前はユーザ マシンの OrgInfo.json ファイルの OpenDNS ローミング モジュールおよびコピーの手動インストールを必要とします。 大規模な配置はエンタープライズ ソフトウェア 管理 システム（SMS）によって一般的に実現します。

OpenDNS Roaming モジュールの展開

AnyConnect パッケージ インストールの間に、**AnyConnect VPN** および **AnyConnect Umbrella ローミング セキュリティモジュールを**選択して下さい:



Orginfo.json の展開

OrgInfo.json ファイルをダウンロードするために、これらのステップを完了して下さい:

1. OpenDNS ダッシュボードにログイン して下さい。
2. **> 識別 > ローミング コンピュータ**『Configuration』 を選択 して下さい。
3. **+** サイン クリックして下さい。
4. スクロールし、このイメージに示すように **Anyconnect Umbrella ローミング セキュリティ モジュール** セクションの**モジュール プロファイルを**選択して下さい:

ファイルがダウンロードされればオペレーティング システムによって決まるこれらのパスの 1 つで保存する必要があります。

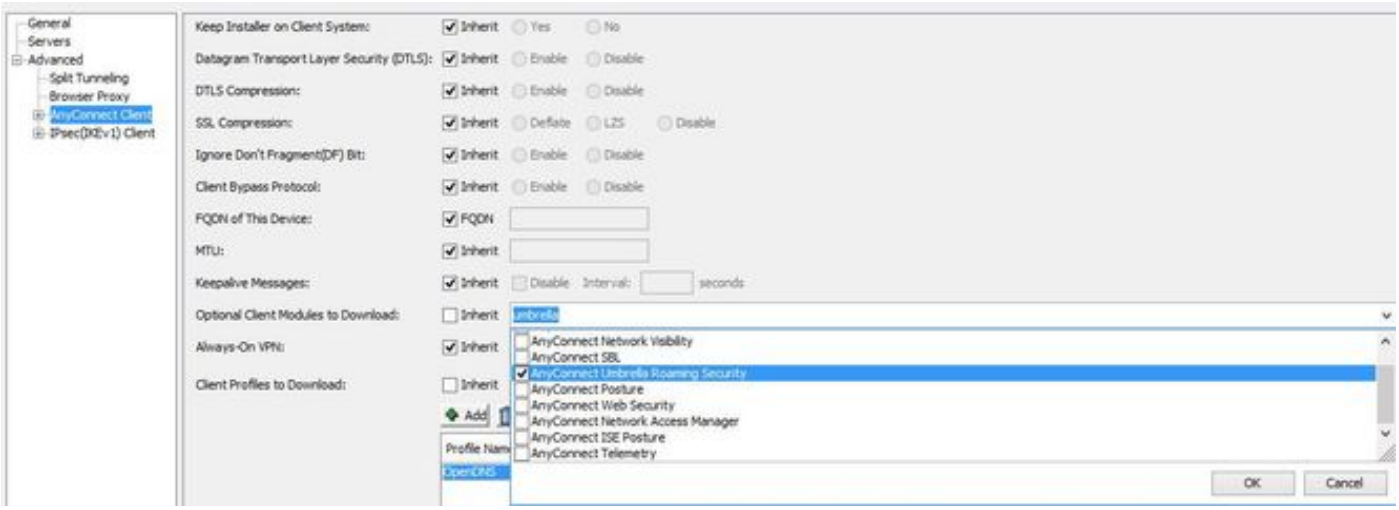
Mac OS X の場合： /opt/cisco/anyconnect/Umbrella
Windows の場合： C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

Web 展開方式

OpenDNS Roaming モジュールの展開

Anyconnect セキュリティ モビリティ クライアント パッケージ（すなわち、anyconnect-win-4.3.02039-k9.pkg）を Cisco Webサイトからダウンロードし、ASA のフラッシュにアップロード

して下さい。 、ASDM でアップロードされて、**ポリシーを > 進みました > AnyConnect クライアント > Umbrella ローミング セキュリティをダウンロードし**、次に選択する**オプションのクライアント モジュール**『Group』 を選択 して下さい。

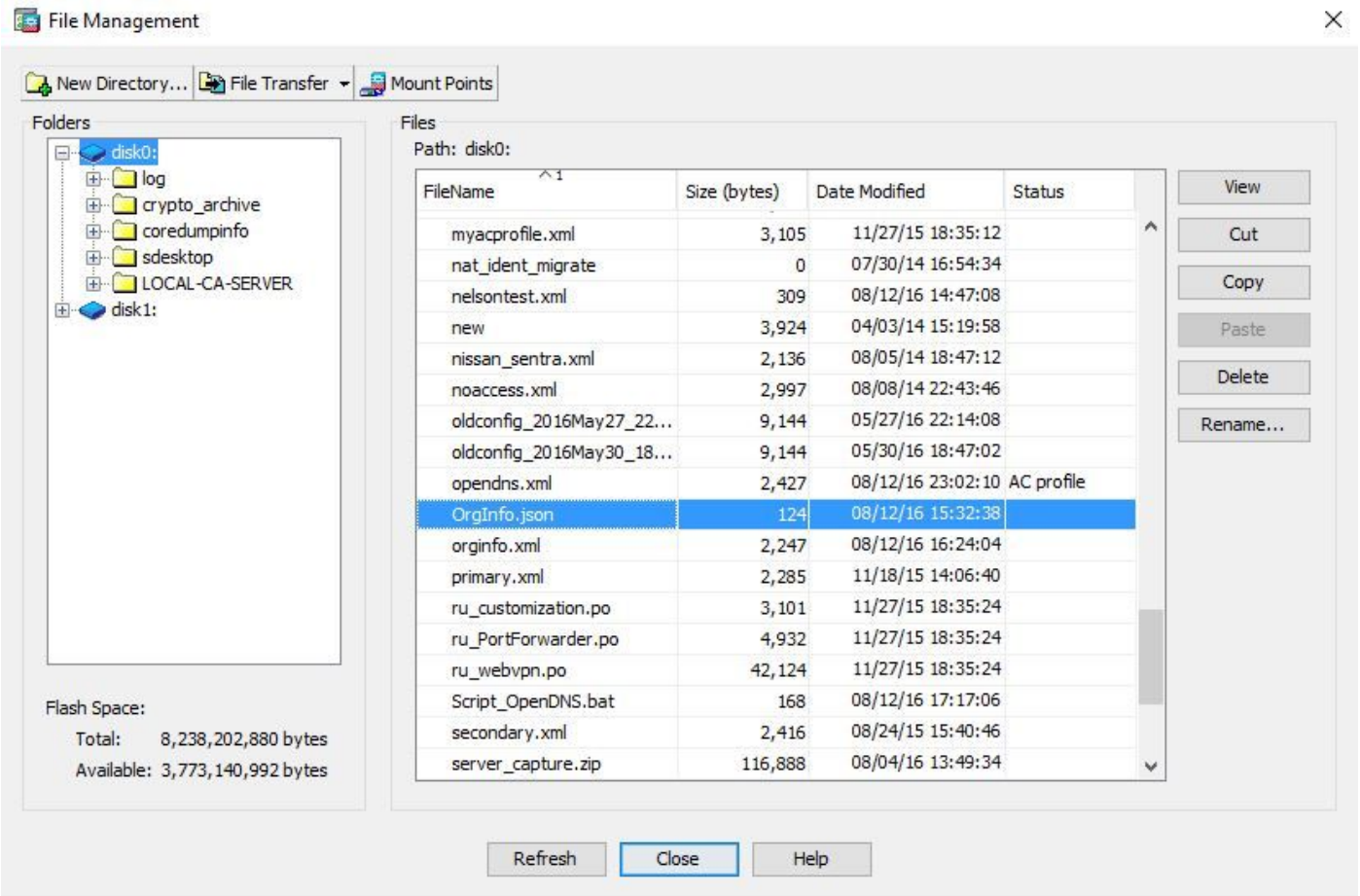


CLI 等量

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

Orginfo.json の展開

1. OrgInfo.json ファイルを OpenDNS ダッシュボードからダウンロードし、ASA のフラッシュにアップロードして下さい。



2. **OrgInfo.json ファイル**をリモート エンドポイントにプッシュするように ASA を設定します。

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

> **注:** この設定は CLI によってしか行うことができません。 このタスクに ASDM を使用するには、ASDM バージョン 7.6.2 以降が ASA にインストールされている必要があります。

Umbrella ローミング クライアントが説明されている方式の 1 つによってインストールされていればこのイメージに示すように AnyConnect GUI 内の統合されたモジュールとして現われる必要があります:

Orginfo.json が正しい場所のエンドポイントに展開されるまで、Umbrella Roaming モジュールは初期化されません。

設定

このセクションでは、OpenDNS Roaming モジュールを各種の AnyConnect トンネル モードで機能させるために必要なサンプルの CLI 設定スニペットを示します。

```
!--- 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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

AnyConnect OpenDNS 関連 問題を解決するステップは次のとおりです:

1. Umbrella ローミング セキュリティモジュールが Anyconnect セキュアな機動性 クライアントと共にインストールされているようにして下さい。
2. OrgInfo.json をで、オペレーティング システムに基づいて正しいパスでエンド ポイントに現在この資料で規定 される 形式にあります確認して下さい。
3. OpenDNS リゾルバへの DNS クエリが AnyConnect VPN トンネルに行くように意図されている場合 OpenDNS リゾルバに到達可能性を可能にするためにヘアピンが ASA で設定されるようにして下さい。
4. 同時の AnyConnect バーチャル アダプタおよび物理的なアダプタのパケットキャプチャを（フィルターなしで）集めて下さいおよび解決しないドメインの下で注意して下さい。
5. ローミング モジュールが暗号化された状態で動作する場合、UDP 443 をローカルでブロックした後パケットキャプチャを、トラブルシューティングを行うのにただ集めて下さい。そこのその方法は DNS トランザクションに表示です。
6. AnyConnect 投げ矢を、Umbrella 診断実行し、DNS 失敗の時の下に注意して下さい。 詳細については Anyconnect のための投げ矢バンドルを集める方法を参照して下さい。
7. Umbrella 診断ログを収集し、表示された URL を OpenDNS 管理者に送信します。 この情報にアクセスできるのは、自分自身と OpenDNS 管理者に限られます。 Windows の場合：
   C:\Program ファイル（x86)\Cisco\Cisco AnyConnect セキュア モビリティ クライアント\UmbrellaDiagnostic.exe
   Mac OS X の場合： /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

関連情報

- **Cisco バグ ID CSCvb34863: AnyConnect が split-include トンネリング用に設定されている場合の DNS の解決の遅延**
- **テクニカル サポートとドキュメント – Cisco Systems**