AnyConnect OpenDNS ローミング セキュリティ モジュール導入ガイド

内容

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あることが推奨されます。

- 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いています。

- 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 以降
- Microsoft Windows 8.1
- **注：**OpenDNS Umbrella モジュールを実装する最小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 以降
  OpenDNS Roaming モジュールは、現在 Linux プラットフォームでサポートされていません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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

OpenDNS Roaming モジュールを適切に機能させるには、モジュールを使用する前に OrgInfo.json ファイルを OpenDNS ダッシュボードからダウンロードするか、ASA からプッシュする必要があります。ファイルが最初にダウンロードされるときに、オペレーティング システムに応じて特定のパスに保存されます。

Mac OS X の場合、OrgInfo.json は /opt/cisco/anyconnect/Umbrella にダウンロードされます。Microsoft Windows の場合、OrgInfo.json は C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\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 エンコーディングを使用し、organizationId、fingerprint、および userId が含まれています。組織 ID は、OpenDNS ダッシュボードに現在ログインしているユーザの組織の情報を表します。組織 ID は静的および一意であり、組織ごとに OpenDNS によって自動生成されます。指紋は、デバイスの登録中に OrgInfo.json ファイルを検証するために使用され、ユーザ ID はログインしたユーザの一意の ID を表します。

Windows では、Roaming モジュールが起動されると、OrgInfo.json ファイルが Umbrella ディレクトリの下の data ディレクトリにコピーされ、作業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 OrgInfo.json ファイルから情報を正常に読み取ると、クラウド API を使用して OpenDNS への登録を試行します。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。

登録が完了すると、Roaming モジュールはエンドポイントのポリシー情報を取得するために同期操作を実行します。同期操作を実行するにはデバイス ID が必要です。同期データには、syncInterval、内部バイパスドメイン、およびIPアドレスなどが含まれます。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

登録と同期が正常に実行されると、Roaming モジュールはドメイン ネーム システム（DNS）プローブをそのローカル リゾルバに送信します。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。

仮想アプライアンス（VA）が存在する場合、クライアントは「behind-VA」モードに遷移し、DNS の適用はエンドポイントで実行されません。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。

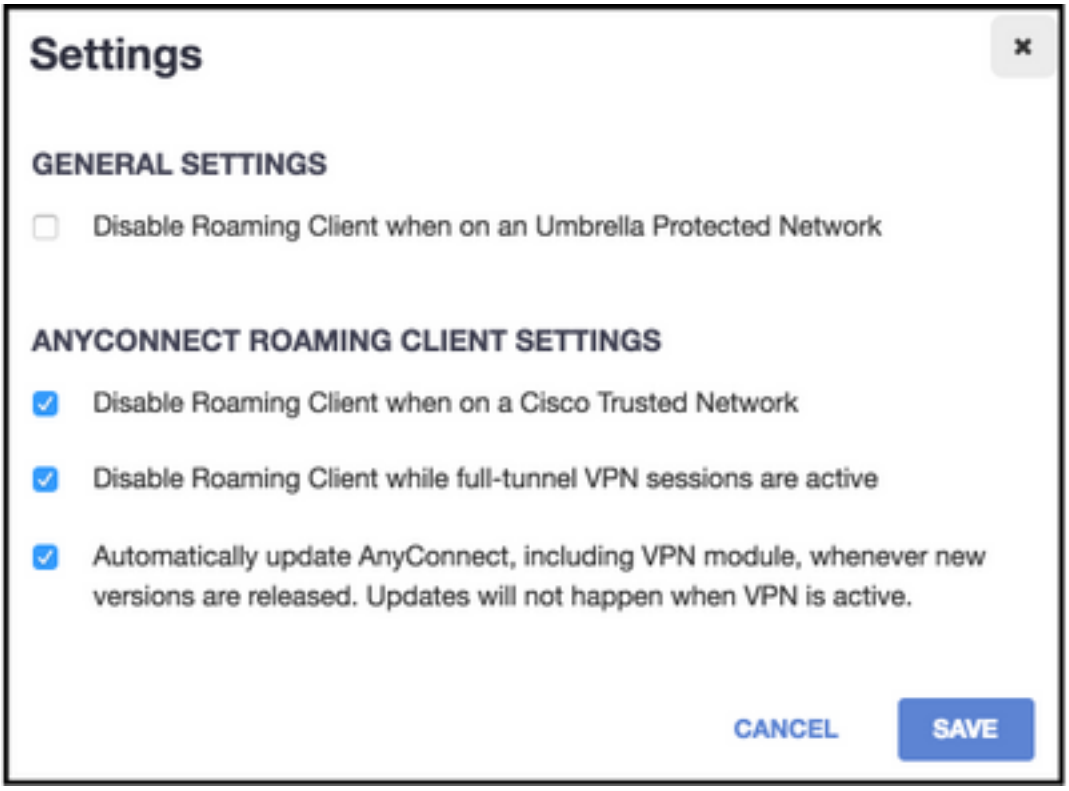
肯定応答は、DNS の暗号化が可能であることを示します。否定応答を受信する場合、クライアントは UDP/53 を使用して、OpenDNS パブリック リゾルバに DNS 要求を送信します。

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。

一定数の否定応答を受信すると、クライアントはフェイルオープン状態に遷移します。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モジュールが保護および/または暗号化された状態に正常に移行すると、ローカル検索ドメインおよび内部バイパスドメイン以外の検索ドメインのすべてのDNSクエリが、名前解決のためにOpenDNSリゾルバに送信されます。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、Roaming モジュールのデフォルト動作では、tunnel-all 設定の VPN トンネルがアクティブのときに DNS 保護が無効にされます。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。以下の情報は、Roaming モジュールを介した DNS 保護が有効であることを想定しています。

内部バイパスリストのクエリ済みドメイン部分

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。

内部バイパスリストに含まれないクエリ済みドメイン

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 リゾルバを介した名前解決が失敗する場合、Roaming モジュールは VPN アダプタ（トンネル確立中の優先アダプタ）をはじめとして、ローカルに設定された DNS サーバにフェールオーバーします。

2.スプリットDNS(tunnel-all-DNS Disabled)

注：すべてのスプリットDNSドメインは、トンネルが確立されると、Roamingモジュールの内部バイパスリストに自動的に追加されます。これは、AnyConnect と Roaming モジュールの間で一貫性のある DNS 処理方法を提供するために実行されます。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 では、split-DNS が両方の IP プロトコル（IPv4 および IPv6）に対して有効になっている場合、または split-DNS が一方のプロトコルに対してのみ有効になっており、他方のプロトコル用に設定されたアドレス プールがない場合、Windows と同様の true split-DNS が適用されます。
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。つまり、AnyConnect はトンネル経由の split-DNS ドメインに適合する DNS 要求のみ許可します（他の要求に対しては AC によって拒否応答が出され、パブリック DNS サーバに強制的にフェールオーバーします）が、split-DNS ドメインに適合するその要求を、暗号化しない状態でパブリック アダプタ経由で送信されないように強制することはできません。

内部バイパスリストのクエリ済みドメインの一部およびスプリットDNSドメインの一部

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、一致するドメインへのその他すべての要求に対しては、AnyConnect ドライバによって「no such name（名前が見つかりません）」という応答が出され、true split-DNS が実行されます（DNS フォールバックを防ぐ）。 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。

内部バイパスリストのクエリ済みドメインの一部であるが、スプリットDNSドメインの一部ではない

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、一致するドメインへのその他すべての要求に対しては、AnyConnect ドライバによって「no such name（名前が見つかりません）」という応答が出され、クエリが VPN トンネル経由で送信されないようにします。

内部バイパスリストまたはスプリットDNSドメインに含まれないクエリ済みドメイン

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 リゾルバを経由した名前解決に失敗した場合、Roaming モジュールは、VPN アダプタで構成されているものを除き、ローカルで構成された DNS サーバにフェールオーバーします。トンネル アダプタからの、一致するドメインへのその他すべての要求に対しては、AnyConnect ドライバによって「no such name（名前が見つかりません）」という応答が出され、クエリが VPN トンネル経由で送信されないようにします。

3. Split-IncludeまたはSplit-Excludeトンネリング（split-DNSおよびtunnel-all-DNSが無効でない）

内部バイパスリストのクエリ済みドメイン部分

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。

内部バイパスリストに含まれないクエリ済みドメイン

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 パブリック リゾルバが split-include リストに含まれる場合、または split-exclude リストに含まれない場合、プロキシされた要求は VPN トンネル経由で送信されます。

OpenDNS パブリック リゾルバが split-include リストに含まれない場合、または split-exclude リストに含まれる場合、プロキシされた要求は VPN トンネルの外部で送信されます。

OpenDNS リゾルバを介した名前解決が失敗する場合、Roaming モジュールは VPN アダプタ（トンネル確立中の優先アダプタ）をはじめとして、ローカルに設定された DNS サーバにフェールオーバーします。 Roaming モジュールによって返された（さらにネイティブの DNS クライアントにプロキシされた）最終的な応答が失敗した場合、ネイティブ クライアントは可能であれば他の DNS サーバを試みます。

Umbrella Roaming モジュールのインストールおよび設定

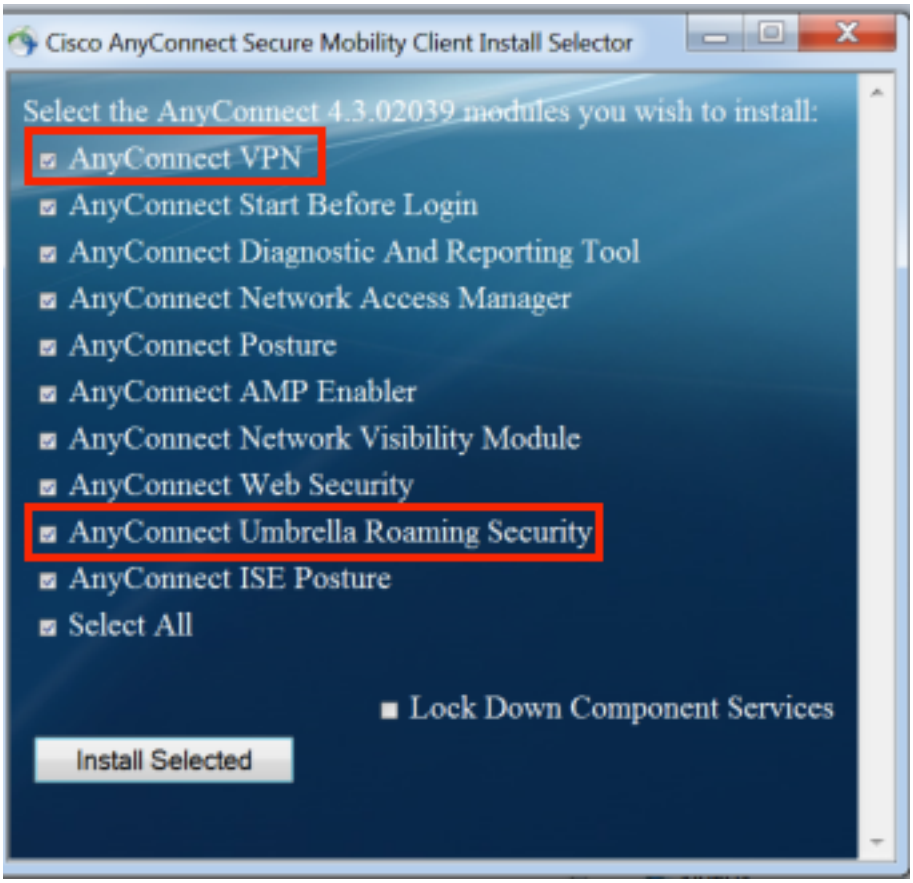
OpenDNS Roaming モジュールを AnyConnect VPN クライアントと統合するには、モジュールを事前展開方式または Web 展開方式のいずれかでインストールする必要があります。

事前展開（手動）方式

事前展開では、OpenDNS Roaming モジュールを手動でインストールし、ユーザのマシンに OrgInfo.json ファイルをコピーする必要があります。大規模な展開は通常、エンタープライズ ソフトウェア管理システム（SMS）を使用して実行されます。

OpenDNS Roaming モジュールの展開

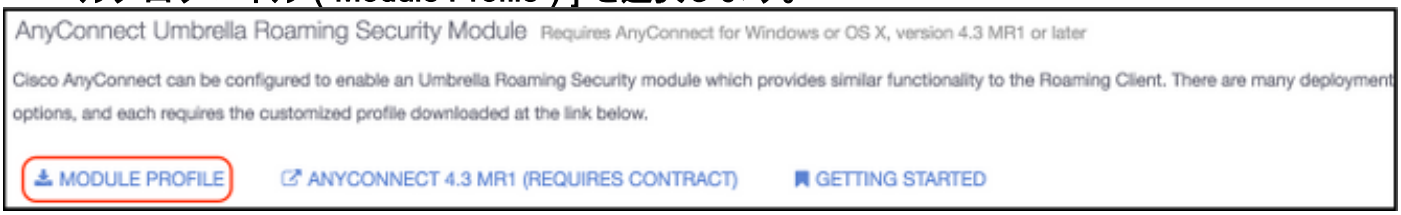
AnyConnect パッケージのインストール中に、[AnyConnect VPN] **モジュールと [Anyconnect Umbrella Roamingセキュリティ（AnyConnect Umbrella Roaming Security）] モジュールを選択します。**



Orginfo.json の展開

OrgInfo.json ファイルをダウンロードするには、次の手順を実行します。

1. OpenDNS ダッシュボードにログインします。
2. [設定（Configuration）] > [ID（Identities）] > [ローミングコンピュータ（Roaming Computers）] の順に選択します。
3. [+] 記号をクリックします。
4. 下方向にスクロールし、次の図に示すように、[Anyconnect Umbrella Roamingセキュリティモジュール（Anyconnect Umbrella Roaming Security Module）] **セクションで [モジュールプロファイル（Module Profile）] を選択します。**



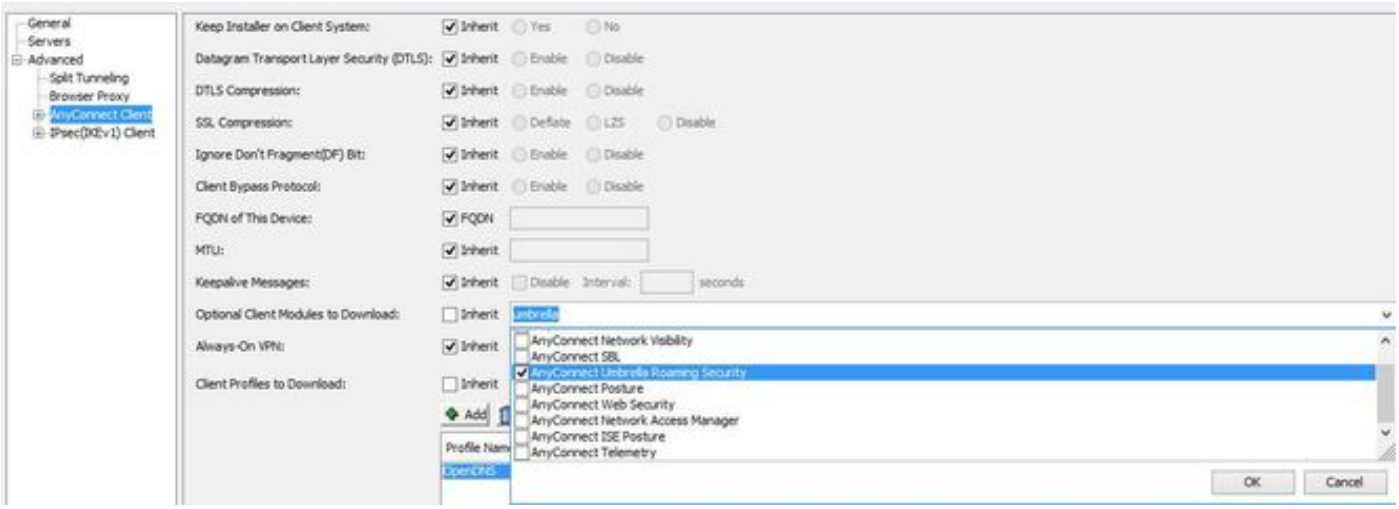
ファイルをダウンロードしたら、オペレーティング システムに応じて次のうちいずれかのパスに保存する必要があります。

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

シスコの Web サイトから Anyconnect セキュリティ モビリティ クライアントのパッケージ（つまり anyconnect-win-4.3.02039-k9.pkg）をダウンロードして、ASA のフラッシュにアップロードします。アップロードしたら、ASDM で、[グループ（Group）] > [ポリシー（Policy）] > [詳細設定（Advanced）] > [AnyConnectクライアント（AnyConnect Client）] > [ダウンロードするオプションクライアントモジュール（Optional Client Modules to Download）] の順に選択してから、[Umbrella Roamingセキュリティ（Umbrella Roaming Security）] **を選択します。**

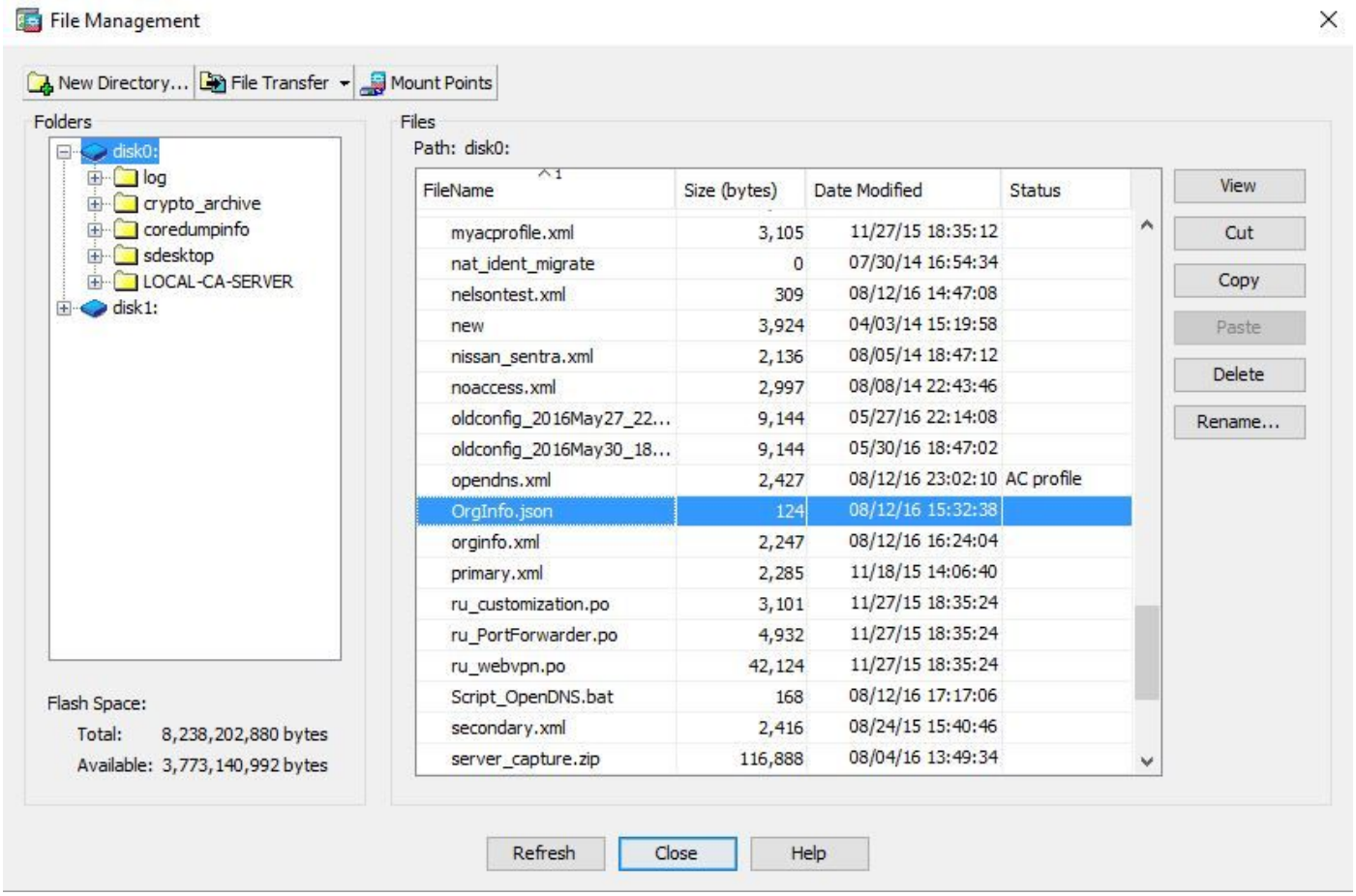


CLI に相当

```
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ます。



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**：この構成は、CLI 経由でのみ実行できます。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。

説明したいずれかの方法によって Umbrella Roaming クライアントがインストールされると、次の図に示すように、AnyConnect GUI で統合モジュールとして表示されます。

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
```

```
        (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。

トラブルシュート

AnyConnect OpenDNS 関連問題をトラブルシューティングする手順は次のとおりです。

1. Umbrella Roaming セキュリティ モジュールが Anyconnect セキュア モビリティ クライアントとともにインストールされていることを確認します。
2. オペレーティング システムに応じて OrgInfo.json が正しいパスのエンドポイントにあり、このドキュメントで指定されたフォーマットであることを確認します。
3. OpenDNS リゾルバに対する DNS クエリが AnyConnect VPN トンネルを経由することになっている場合、そのヘアピンが OpenDNS リゾルバに到達できるように ASA で設定されていることを確認します。
4. AnyConnect の仮想アダプタと物理アダプタでパケット キャプチャを（フィルタなしで）同時に収集し、解決に失敗するドメインを書き留めます。
5. Roaming モジュールが暗号化された状態で機能している場合、UDP 443 をローカルにブロックしてから、トラブルシューティングの目的に限ってパケット キャプチャを収集します。そうすると、DNS トランザクションが可視化されます。
6. AnyConnect DART、Umbrella の診断を実行して、DNS の障害の時刻を書き留めます。詳細については、『How to collect the DART bundle for Anyconnect』を参照してください。
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 Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
   Mac OSXの場合：/opt/cisco/anyconnect/bin/UmbrellaDiagnostic

関連情報

- **Cisco bug 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**