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

この資料は OpenDNS（傘）ローミング モジュールにおけるインストール、設定およびトラブルシューティング の 手順を記述したものです。AnyConnect 4.3.X から始まって、OpenDNS ローミング クライアントは統合されたモジュールとして現在利用できます。 それは別名 Cloud セキュリティモジュールであり、AnyConnect インストーラを使用してエンドポイントに前展開されてできましたり、または ASA から Web 導入によってダウンロード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 クライアント
- OpenDNS/傘ローミング モジュール

- Cisco 適応性があるセキュリティ アプライアンス モデル

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 適応性があるセキュリティ アプライアンス モデル（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 ローミング モジュール 4.3.01095
- Cisco Adaptive Security Device Manager 7.6.2 またはそれ以降
- Windows 8.1

- **注:** OpenDNS 傘モジュールを配置する最小限の要件:
  - AnyConnect VPN クライアント バージョン 4.3.01095 または それ 以降
  - Cisco Adaptive Security Device Manager 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。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークがライブである場合、あらゆるコマンドまたは設定の潜在的影響を理解することを確かめて下さい。

背景説明

Orginfo.json

OpenDNS ローミング モジュールの適切な機能のために、 **Orginfo.json ファイルは** OpenDNS ダッシュボードからダウンロードされるか、または ASA からモジュールを使用する前に押す必要があります。 ファイルが最初にダウンロードされるとき、オペレーティング システムによって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 Windows に関しては、 **Orginfo.json は**「C:\ProgramData\Cisco\Cisco **AnyConnect セキュアな機動性 クライアント\傘**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 はスタティック、各組織のための OpenDNS によってユニーク、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 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、 **Orginfo.json ファイルを**開始するとき傘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、このファイルから情報は傘ディレクトリの下のデータディレクトリの updater.plist に保存されます。 モジュールが正常に Orginfo.jsonfile からの情報を読んだら 、クラウド API を使用して OpenDNS と登録するように試みます。 この登録はマシンにユニークなデバイスID にその試みられた登録を

割り当てる OpenDNS という結果に終ります。 前登録からのデバイスID が既に利用できている場合、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。 デバイスID は同期化オペレーションがはたらくことができるように必要です。 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。 同期化間隔は分数ですそのあとでモジュールは再同期に試みる必要があります。

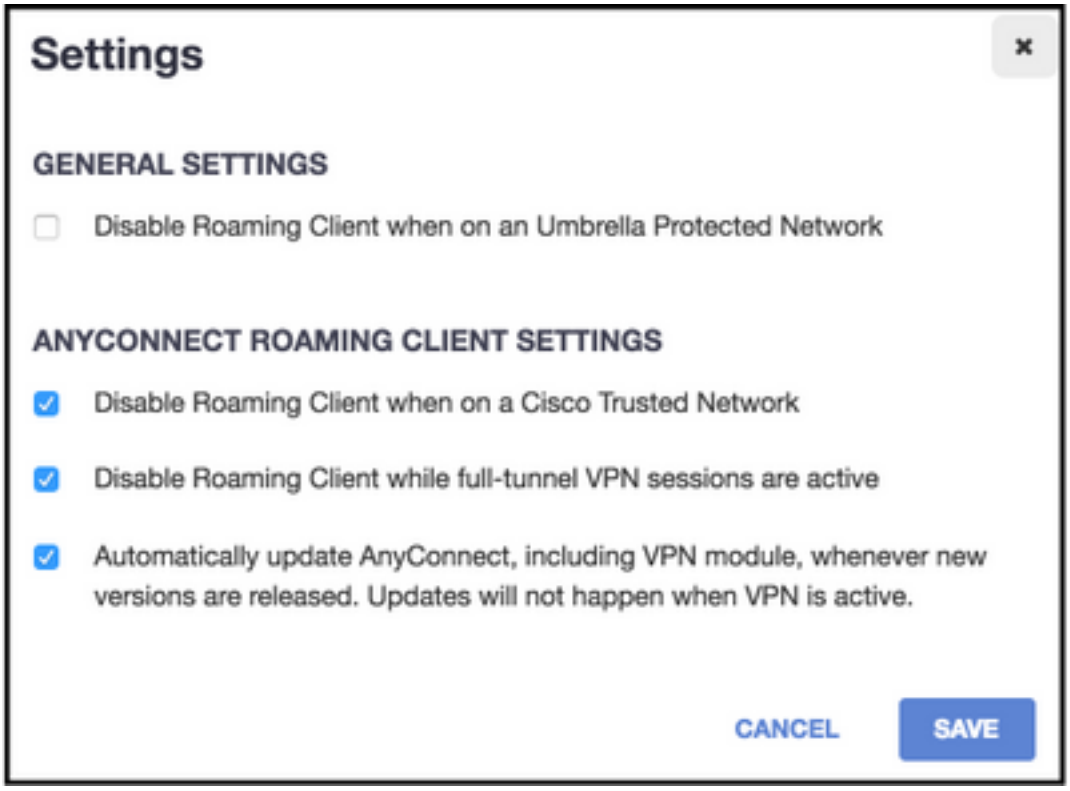
DNS 精査動作

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 DNS プローブ。これらの DNS 要求は debug.opendns.com のための TXT クエリが含まれています。 応答に基づいて、クライアントは確認かどうか OpenDNS 構内 仮想 な アプライアンス (VA ことを) 存在する ネットワークでできました。

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。 クライアントはネットワーク レベルに DNS 適用のための VA に頼ります。
VA がない場合、クライアントは OpenDNS 公共リゾルバに DNS 要求を送信 します（208.67.222.222）UDP/443 を使用して。
肯定応答は DNS 暗号化が可能性のあるであることを示します。 否定応答が受け取られる場合、クライアントは UDP/53 を使用して OpenDNS 公共リゾルバに DNS 要求を送信 します。
このクエリへの肯定応答は DNS 保護が可能性のあるであることを示します。 否定応答が受け取られる場合、クライアントはクエリを数秒間のうちに再試行します。
一定数の否定応答を受け取った上、クライアントの移行故障する開いた状態。 故障する開いた状態は DNS 暗号化や保護が可能性のあるではないことを意味します。 ローミング モジュールが保護されるに正常に移行すれば持っていればおよび/または ローカル検索ドメインおよび whitelist ドメインの外の検索ドメインのための暗号化された状態、すべての DNS クエリが名前解決のための OpenDNS リゾルバに送られれば。 有効に されて暗号化された状態がすべての 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 トンネリング モードでの DNS 動作

1. (有効に なるトンネルすべてまたはトンネルすべて DNS)



注: 示されているように、デフォルトの動作は DNS 保護をディセーブルにするローミング 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 の間にアクティブであるモジュールに関しては全**トンネル VPN セッションが Active オプションの間、トンネル**すべての設定 **クライアントをローミングするディセーブルは** OpenDNS ポータルでチェックを外す必要があります。 この機能を有効に する機能は OpenDNS の高度サブスクリプション レベルを必要とします。 情報は下記のローミング モジュールでの DNS 保護が有効に なると仮定します。

whitelist の問い合わせられたドメイン部:

トンネル アダプタから起きる DNS 要求は VPN トンネルを渡るトンネル DNSサーバに、許可され、送信 されます。 クエリはトンネル DNSサーバによって解決することができない場合未解決に残ります。

問い合わせられたドメイン whitelist のない部品:

トンネル アダプタから起きる DNS 要求はローミング モジュールで OpenDNS 公共リゾルバに許可され、proxied、VPN トンネルを渡って送信 されます。 DNS クライアントに名前解決が VPN DNSサーバによって発生したように見えます。 OpenDNS リゾルバによる名前解決が正常ではない場合、ローミング モジュールは (優先 する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. 分割DNS (ディセーブルにされるトンネルすべて DNS)

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 およびローミング 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。 分割DNS 設定で (とトンネリングを分割含んで下さい) OpenDNS 公共リゾルバが分割含ネットワークに含まれていないようにして下さい。

注: Mac OS X で、分割DNS が両方の IP プロトコル（IPv4 および IPv6）のために有効になればまたはそれは 1 プロトコルのためにだけ有効に なり、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。
分割DNS が 1 プロトコルだけのために有効に なればおよび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れば、分割トンネリングのための DNS フォールバックだけが実施されます。 これは AnyConnect トンネルによって分割DNS ドメインと一致する割り当て DNS 要求だけ（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）意味しますが、パブリックアダプターで、分割DNS ドメインと一致する要求が明白に送信 されないこと実施できません。

whitelist 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 アダプタから起きる DNS 要求は VPN トンネルを渡るトンネル DNSサーバに、許可され、送信 されます。 他のアダプタからのドメインと一致する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）。 従って、非トンネル DNS トラフィックだけローミング モジュールによって保護されます。

whitelist 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:

物理的 な アダプタから起きる DNS 要求は VPN トンネルの外部の公共 DNSサーバに、許可され、送信 されます。 トンネル アダプタからのドメインと一致する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 whitelist または分割DNS ドメインのない部品:

物理的 な アダプタから起きる DNS 要求は OpenDNS 公共リゾルバに許可され、proxied、VPN トンネルの外部で送信 されます。 DNS クライアントに名前解決が公共 DNSサーバによって発生したように見えます。 OpenDNS リゾルバによる名前解決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 アダプタからのドメインと一致するための他の要求はすべてそのような名前無しで 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. トンネリングを分割含むか、または分割除いて下さい（ディセーブルにされる分割DNS およびトンネルすべて DNS 無し）

whitelist 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発注に基づいて DNS 解決を行い VPN がアクティブなとき AnyConnect は優先 する アダプタです。 DNS 要求はトンネル アダプタから最初に起き、VPN トンネルを渡るトンネル DNSサーバに、送信 されます。 クエリがトンネル DNSサーバによって解決することができない場合 OS リゾルバは公共 DNSサーバによってそれを解決するように試みます。

問い合わせられたドメイン whitelist 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発注に基づいて DNS 解決を行い VPN がアクティブなとき AnyConnect は優先 する アダプタです。 DNS 要求はトンネル アダプタから最初に起き、VPN トンネルを渡るトンネル DNSサーバに、送信 されます。 クエリがトンネル DNSサーバによって解決することができない場合 OS リゾルバは公共 DNSサーバによってそれを解決するように試みます。

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 リゾルバによる名前解決が正常ではない場合、ローミング モジュールは (優先 する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。 モジュールのローミングによって (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。

☂ローミング モジュールをインストールし、設定して下さい

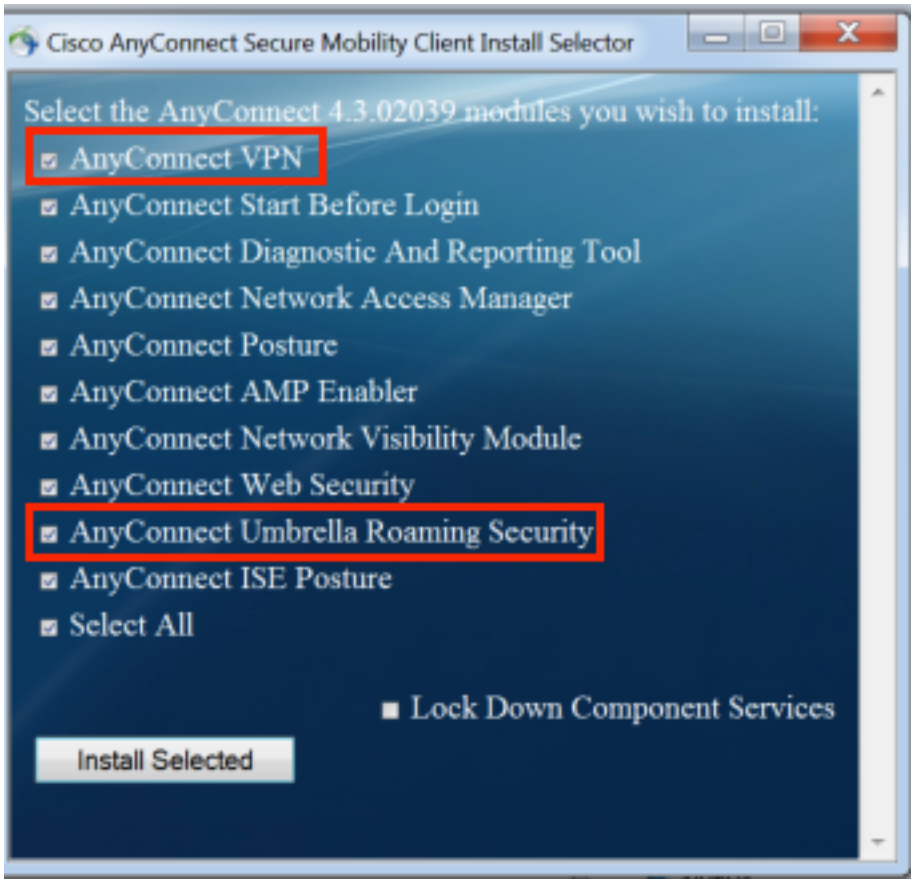
OpenDNS ローミング モジュールを AnyConnect VPN クライアントと統合ために、モジュールは前deploment または Web 展開方法によってインストールされる必要があります:

配置前 (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) を使用して一般的に実現します。

導入 OpenDNS ローミング モジュール

AnyConnect パッケージ インストールの間に Anyconnect VPN および Anyconnect ☂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

OpenDNS ダッシュボードにログイン することおよび設定 > **識別 > ローミング コンピュータ**へのナビゲートによるダウンロード OrgInfo.json ファイルは**および** +sign をクリックします。 スクロールし、AnyconnectUmbrella **ローミング セキュリティモジュール セクションの下で**このイメージに示すように ModuleProfile を選択して下さい:

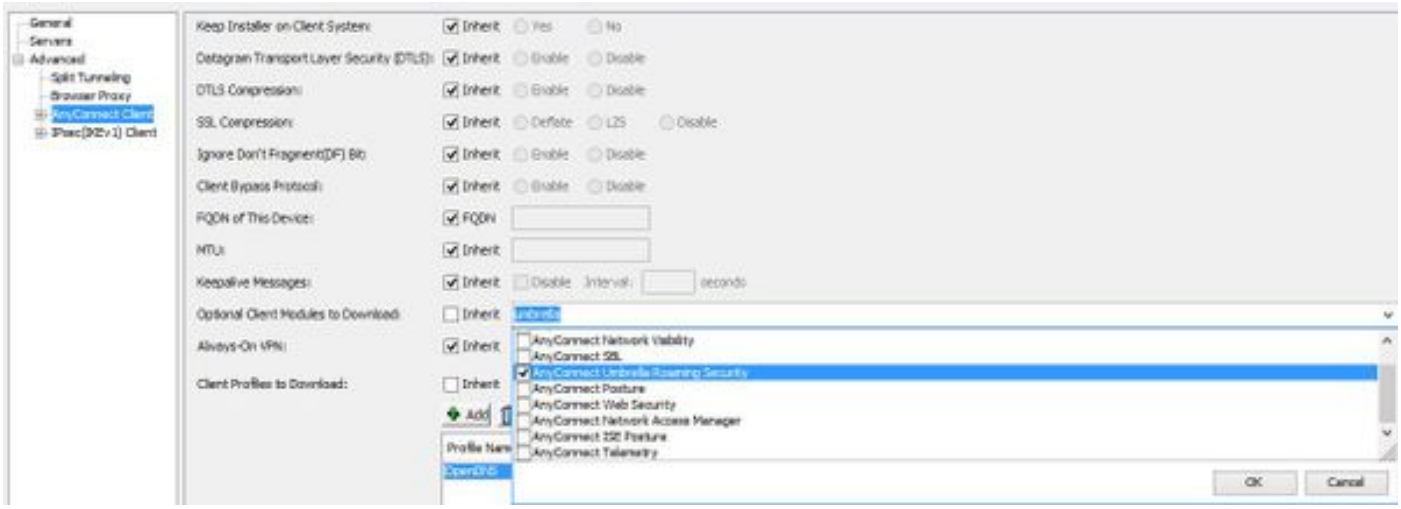
ファイルがダウンロードされれば、オペレーティング システムによってこれらのパスで保存する必要があります。

Mac OS X に関しては: /opt/cisco/anyconnect/Umbrella
Windows の場合： C:\ProgramData\Cisco\Cisco AnyConnect セキュアな機動性 クライアント\傘

Web 配備方式

導入 OpenDNS ローミング モジュール

Anyconnect セキュリティ モビリティ クライアント（ 例えば anyconnect-win-4.3.02039-k9.pkg ）パッケージを Cisco Webサイトからダウンロードし、ASA のフラッシュするにアップロードして下さい。 、ASDM でアップロードされて > **進みました > AnyConnect クライアントは** GroupPolicy に > UmbrellaRoaming **セキュリティをダウンロードし、**選択する**オプションのクライアント モジュール**行きます。

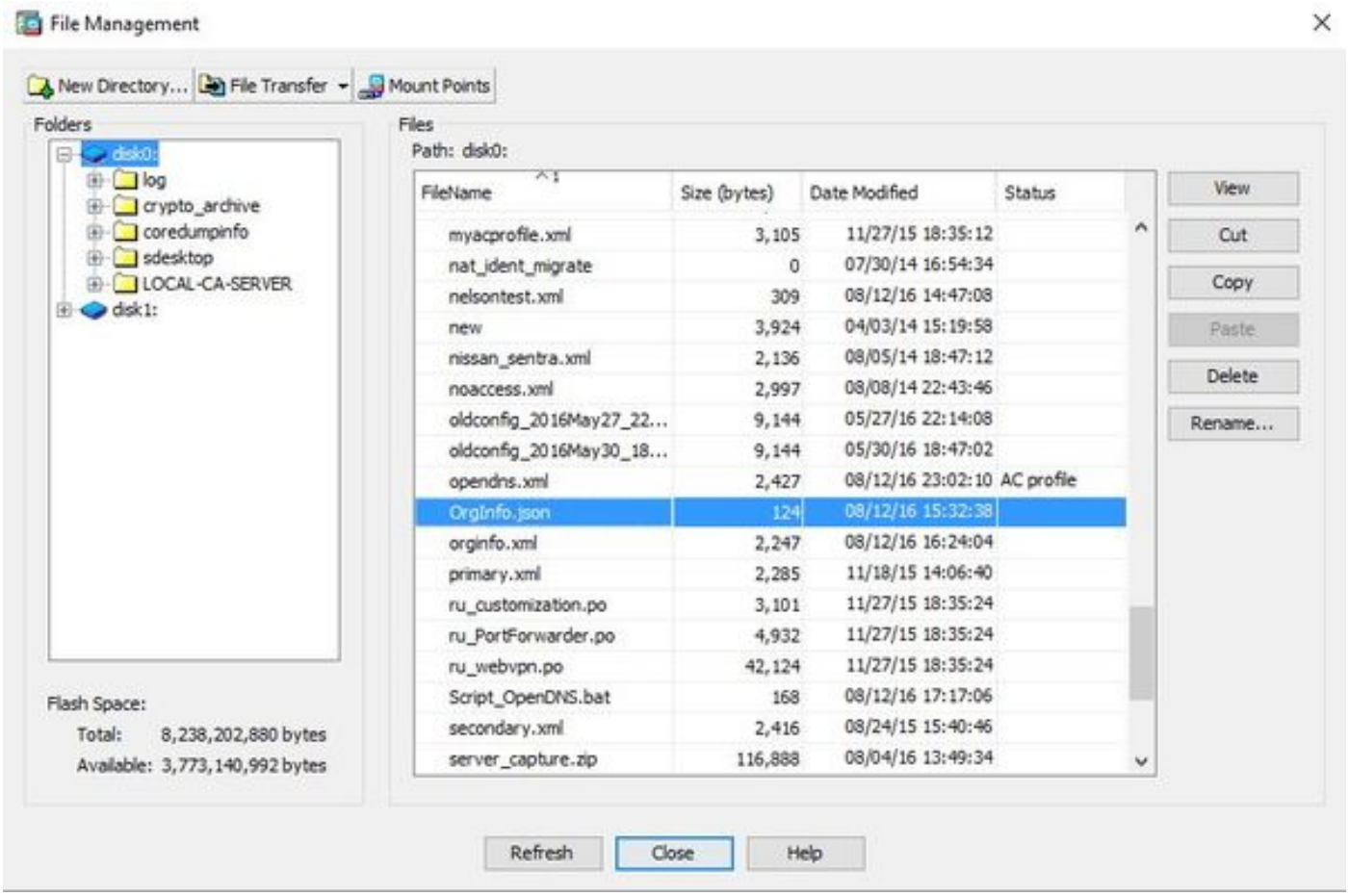


CLI 等量:

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

導入 Orginfo.json

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 のフラッシュするにそれをアップロードして下さい。



2. リモートエンドポイントに **OrgInfo.json ファイルを**押すために ASA を設定して下さい。

```
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。 ASDM をこのタスクの実行に使用するために、ASDM バージョン 7.6.2 または それ 以降は ASA でインストールされる必要があります。

傘ローミング クライアントが説明されているメソッドの 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 が適切な位置のエンドポイントで展開されるまで、傘ローミング モジュールは初期化されません。

設定

セクションは AnyConnect さまざまなトンネリング モードでの OpenDNS ローミング モジュールを操作するのに必要なサンプル CLI コンフィギュレーション の 断片を示します。

```
!--- 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
```

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:

1. 傘ローミング 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てい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オペレーティングである場合、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、傘診断実行し、DNS 失敗の時の下に注意して下さい:

投げ矢の収集: https://supportforums.cisco.com/document/12747756/how-collect-dart-bundle-anyconnect

7. 傘診断 ログを集め、OpenDNS 管理者に生じる URL を送信 して下さい。 だけおよび OpenDNS 管理者はこの情報にアクセスできます。

Windows の場合： 「C:\Program ファイル（x86)\Cisco\Cisco AnyConnect セキュアな機動性 クライアント\ UmbrellaDiagnostic.exe

Mac OSX に関しては: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

関連問題

CSCvb34863: DNS の解決のレイテンシーは AnyConnect がのために設定したときにトンネリングを分割含んでいます