Umbrella口ーミングクライアントとVPNの互換性の管理

内容

はじめに

概要

Umbrella口ーミングクライアントとVPNクライアントの動作方法

Umbrella口ーミングクライアントの非互換性

VPNクライアントの非互換性の理由

仮想アプライアンスと保護されたネットワーク

スタンドアロンおよびCisco Secure Client + Roamingセキュリティモジュールに関する特別な考慮事項

- Windows 10および11用のDNSバインド順序VPN互換性モード
  - resolv.confs出力例

サードパーティVPNに関する特別な考慮事項

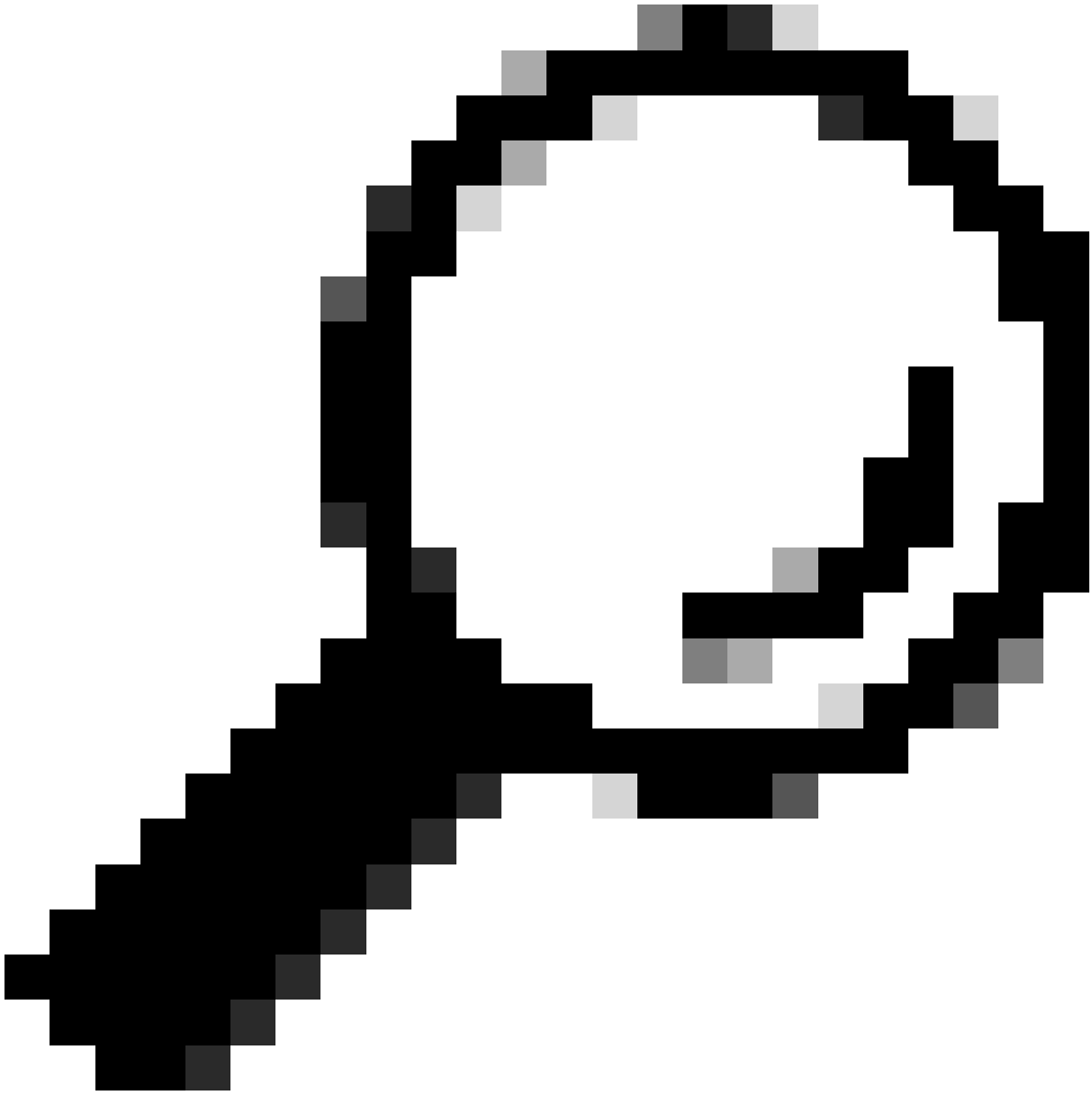
- 常時接続VPN
  - 解決方法
- 粘度VPN
  - 粘性の設定
- トンネルブリック
- Tunnelblick VPNの接続解除の問題
- ライトスピードロケット

はじめに

このドキュメントでは、Cisco Umbrella Roaming Clientとさまざまなソフトウェアとのインタラクションおよび互換性について説明します。

概要

Cisco Umbrella Roaming Clientは、ほとんどのVPNソフトウェアで動作しますが、想定される動作には追加の手順が必要な場合があります。Cisco Umbrellaでは、互換性を最大限に高めるために、Cisco Secure ClientおよびRoamingセキュリティモジュールを導入することを推奨しています。このモジュールは、VPNコンポーネントなしで導入できます。



ヒント：このドキュメントは、一般的なガイダンスとして機能するものであり、サポート対象ソフトウェアの正式なリストではありません。Cisco Umbrellaは、サードパーティ製のソフトウェアやVPNクライアントとの機能のテスト、検証、認定を行いません。

このドキュメントでは、特定のVPNクライアントに関する技術情報と追加のコンテキストについて説明します。これらのクライアントでは、さらに詳細な設定が必要になる場合があります。互換性がないことがわかっているVPNソフトウェアのリストについては、「Umbrella Roamingクライアントの非互換性」セクションを参照してください。SWGクライアントはDNS接続の確立に依存しているため、ローミングクライアントとのDNSの非互換性により、SWGを使用したCisco Secure Client + Roamingセキュリティモジュールで障害が発生する可能性もあります。

Umbrellaローミングクライアントと VPNクライアントの動作方法

Umbrellaローミングクライアントはすべてのネットワークアダプターにバインドされ、コンピューターのDNS設定を127.0.0.1 (localhost)に変更します。 これにより、Umbrella Roaming Clientは、内部ドメイン機能を介したローカルドメインの解決を許可しながら、すべてのDNSクエリをUmbrellaに直接転送できます。VPNサーバへの接続を確立すると、Umbrella Roaming Clientはシステム内の新しいネットワーク接続を検出し、Umbrella Roaming Clientをポイントするように接続DNS設定を変更します。Umbrella Roamingクライアントは、Umbrella AnyCast DNS IPアドレス(208.67.222.222/208.67.220.220)へのDNSルックアップの実行に依存します。

ユーザがVPNに接続する場合、VPNに関連付けられたファイアウォールはUmbrellaへのアクセスを許可する必要があります。

Umbrellaローミングクライアントの非互換性

Umbrella Roamingクライアントは現在、DNSレイヤの適用を提供しています。DNS層はRoaming Clientの主要な機能で、任意のネットワークにDNSベースのセキュリティポリシーを適用します。Roaming Clientのこの機能では、既知のソフトウェアの非互換性が発生する可能性があります。Umbrella RoamingクライアントのDNS層は、サポートチームのテストに基づき、次に示すクライアントと互換性がありません。Cisco Umbrella Engineeringはこれらのクライアントの検証やテストを行いません。すべてのエントリはレビューの対象となります。この記事では、スタンドアロンのUmbrellaローミングクライアントについて説明します。Cisco Secure Client（およびレガシー）用のUmbrella Roamingセキュリティモジュールの関連記事については、関連ドキュメントを参照してください。

VPN クライアント	問題/非互換性	解決方法
パルスセキュア	切断時には、VPN接続中のパルス変更により、保存されたローカルDNSがWiFi/イーサネット値ではなくVPN値のままになる可能性があります。	Umbrellaモジュールで解決 – ほとんどのライセンスに含まれています。
AvayaのVPN	互換性がありません。	Umbrellaモジュールで解決 – ほとんどのライセンスに含まれています。
Windows VPN（特にAlways On VPN）	DNSホスト名が内部ドメインリストにあるにもかかわらず、ローカルDNSが内部応答に解決されない可能性があります。	Umbrellaモジュールで解決 – ほとんどのライセンスに含まれています。
Windowsユニバーサルプラットフォーム上に構築されたVPN「アプリケーション」	これらのアプリケーションは、127.0.0.1ではなく、ローカルNICにDNSを送信する必要があるMicrosoft接続APIを使用する必要があります。そのため、接続できな	Umbrellaモジュールで解決 – ほとんどのライセンスに含まれています。

VPN クライアント	問題/非互換性	解決方法
	いことを示すエラーが表示されます。	
オープンVPN	互換性がありません。	公開済みの修正プログラムはありません.
Palo Alto GlobalProtect VPN（日本での対応時期未定）	3.0.110以降のスタンドアロンローミングクライアントバージョンでは機能しません。	Umbrellaモジュールを使用して修正（ほとんどのライセンスに含まれる）。
F5 VPN	互換性がありません。	Umbrellaモジュールで修正されています。ほとんどのライセンスに含まれています。
チェックポイント VPN	macOSのみ、スプリットトンネルモードのみ。	macOSでスプリットトンネルをディセーブルにします。
SonicWall NetExtender	互換性がありません。	Umbrellaモジュールで修正されています。ほとんどのライセンスに含まれています。
Zscaler VPN（トンネルモード）	互換性がありません。	Umbrellaモジュールで修正されています。ほとんどのライセンスに含まれています。
Akamaiエンドポイント保護(ETPclient)	互換性がありません。	Umbrellaモジュールで修正されています。ほとんどのライセンスに含まれています。
NordVPN	回避策を使用します。	互換性を追加するには、次の2つのオプションがあります。 1. 「OpenVPNを使用してWindowsの手動接続をセットアップする方法」に記載されているように、OpenVPNの接続方法を使用します。 2. Advanced設定でカスタムDNSを

VPN クライアント	問題/非互換性	解決方法
		許可します。DNSを208.67.220.220と208.67.222.222に設定します。
Azure VPN	互換性がありません。	Umbrellaモジュールで修正されています。ほとんどのライセンスに含まれています。
AWS VPN	回避策を使用します。	AWSから手動でダウンロードしたconfigファイルを編集し、pull-filter ignore "block-outside-dns"の2行目を追加します。
VPNのプロビジョニング	互換性がありません。	Umbrellaモジュールで修正されています。ほとんどのライセンスに含まれています。

VPNクライアントの非互換性の理由

一部のVPNクライアントには、Umbrellaローミングクライアントと同様のDNS動作があります。VPN接続のDNSサーバが予期しない値に変更されると、VPNソフトウェアはシステムのDNS設定を、最初の接続時にVPNが設定した値に戻します。Umbrella Roamingクライアントも同じ操作を実行し、DNSサーバを127.0.0.1に戻します。この相互の動作により、VPNとUmbrellaローミングクライアントの間で競合が発生します。この競合により、VPN接続のリセットのためにDNSサーバが無限に繰り返されます。Roaming Clientはこれを検出し、可能であればVPN接続を維持するために自身をディセーブルにします。

仮想アプライアンスと保護されたネットワーク

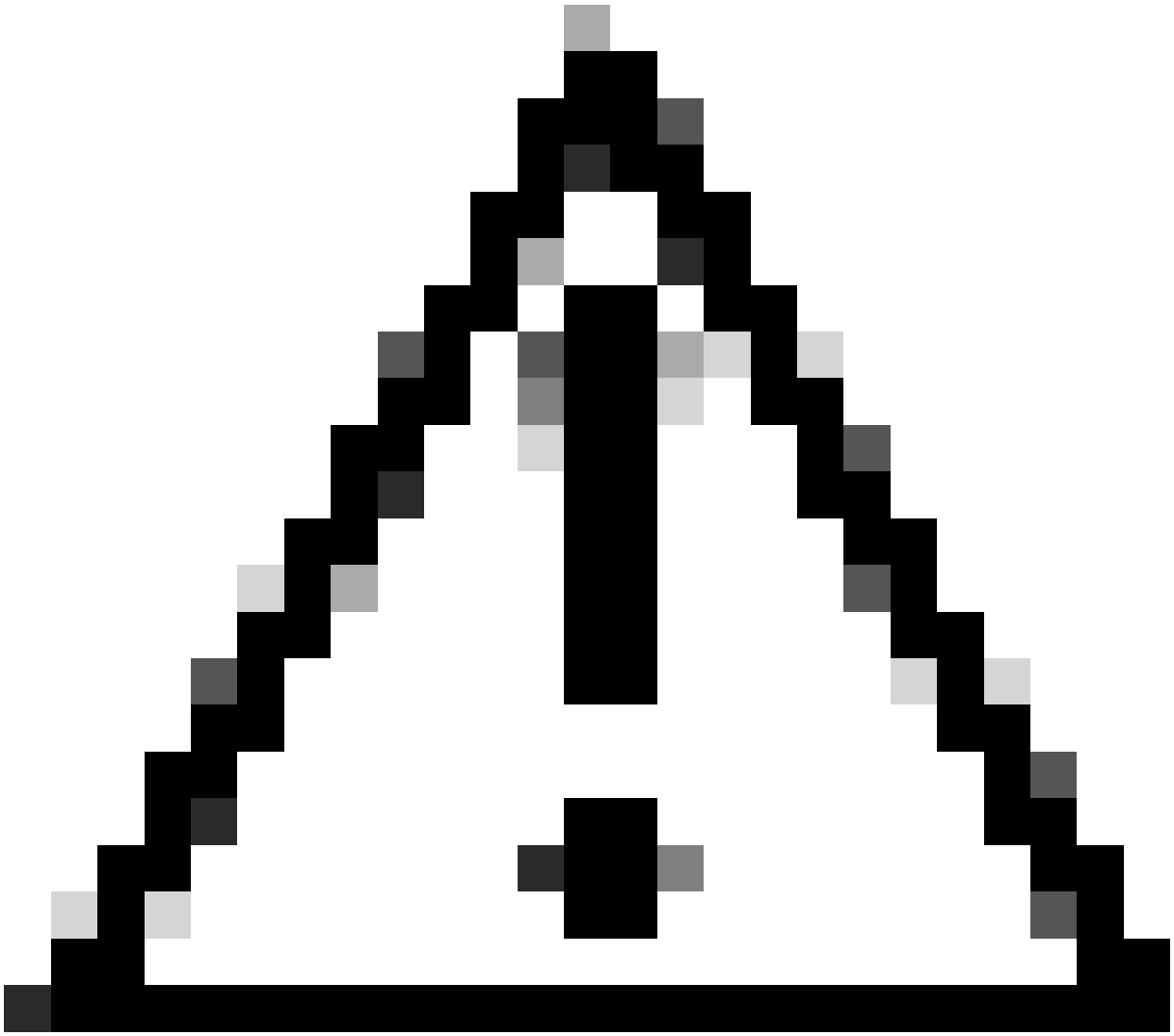
Umbrellaローミングクライアントの動作は、Umbrella仮想アプライアンス(VA)または保護ネットワーク機能を使用するネットワークに接続した場合とは異なります。これは、ユーザがネットワークにローカルに接続するか、VPN経由で接続するかに関係なく適用されます。詳細については、「クライアントと仮想アプライアンスのローミング」または「保護されたネットワーク」のドキュメントを参照してください。

スタンドアロンおよびCisco Secure Client + Roamingセキュリティモジュールに関する特別な考慮事項

ここで提供される情報は、スタンドアロンのUmbrella Roaming Clientに固有のもので、Cisco Secure Client(CSC)+ Roamingセキュリティモジュールには拡張されません。簡単なプラグインのインストールを求めるユーザは、CSCに統合されたUmbrella Roamingを使用できます。Cisco

Secure Client VPNユーザは、VPNの機能上の問題が発生した場合に、CSC + Roamingセキュリティモジュールに移行する必要があります。Cisco Umbrellaでは、CSC + Roamingセキュリティモジュールの検証が必要であり、完全な移行を推奨します。

Cisco Secure Client VPNソフトウェアには、VPN接続の確立時にシステムがDNSを処理する方法に関するオプションが用意されています。詳細については、「DNSクエリと異なるOSでのドメイン名解決に関する動作の違い」を参照してください。この情報は、Cisco Secure ClientおよびUmbrella Roaming Clientを使用した経験に基づいています。内部および外部のDNS解決機能が予想どおりに動作することを確認するために、Cisco Secure Client VPNを有効にしてUmbrellaローミングクライアントをテストすることをお勧めします。



注意:DNSサービスの互換性のためにCisco Secure Clientも使用している場合は、CSC + Roamingセキュリティモジュールを使用する必要があります。ここに示す手順は、必要な場合にのみ統合されていないローミングクライアント用です。これらの手順は、CSC + Roamingセキュリティモジュールには必要ありません。

フルトンネルモードとスプリットトンネルモードの両方で、Cisco Secure Clientが接続されている間にRoaming Clientが動作できるようにするには、特別な指示が必要です。これは、DNSがカーネルドライバによって上書きされるのではなく、ローミングクライアントにフローできるようにするために必要です。フルトンネルの場合、クライアントが強制的にディセーブルにされます。スプリットトンネリングの場合、VPNに接続しているときに内部DNSが失われるという症状が現れます。

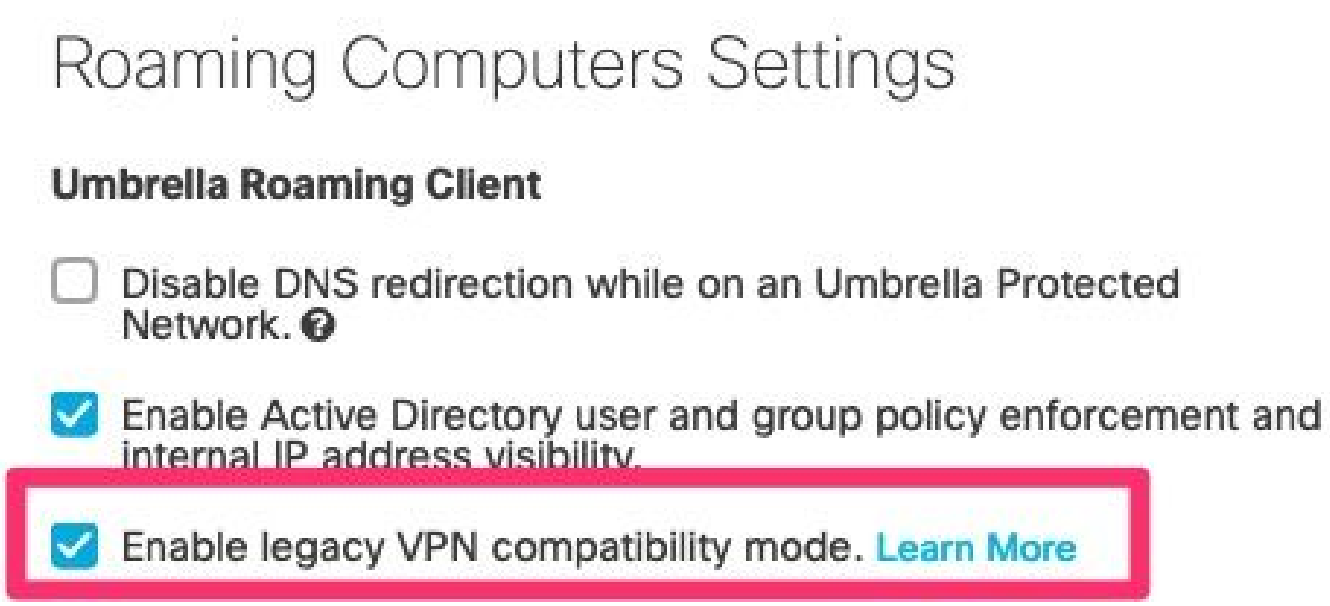
Windows 10および11用のDNSバインド順序VPN互換性モード

Windows 10ユーザの限られたセットで、DNS用のVPN NICではなくローカルLANが優先される特定の問題が発生します。この場合、ローミングクライアントの内部ドメインリストのローカルDNSは解決できませんが、パブリックDNSは問題なく機能します。これは、バージョン2.0.338と2.0.341（デフォルト）およびそれ以降のすべてのバージョンに影響します。バージョン2.0.255では、この問題は発生しませんでした。

以前に影響を受けたVPNクライアントは次のとおりです。

- AnyConnect 3.x
- AnyConnect 4.x（AnyConnect UmbrellaまたはCSC + Roamingモジュールは影響を受けません）
- Sophos VPN（トンネルモード）
- 一部のPalo Alto GlobalProtectの古いバージョンの構成
- WatchGuardモバイルVPN
- ShrewソフトVPN
- バラクーダVPN

解決方法
Roaming Client設定Enable legacy VPN compatibility modeを有効に切り替えます。



360027547111

これが問題であるかどうかを確認するには、診断テストを実行し、resolv.confsの結果をクリックします。VPNアダプタが最初にリストされている場合、この問題はユーザに影響しません。VPNアダプタが2番目にリストされている場合、問題がユーザに影響を与える可能性があります。

resolv.confs出力例

```
Results for: resolv.confs
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Local Area Connection
nameserver 192.168.2.1



C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Cisco AnyConnect Secure Mobility
nameserver 10.1.1.27
nameserver 10.1.1.28
```

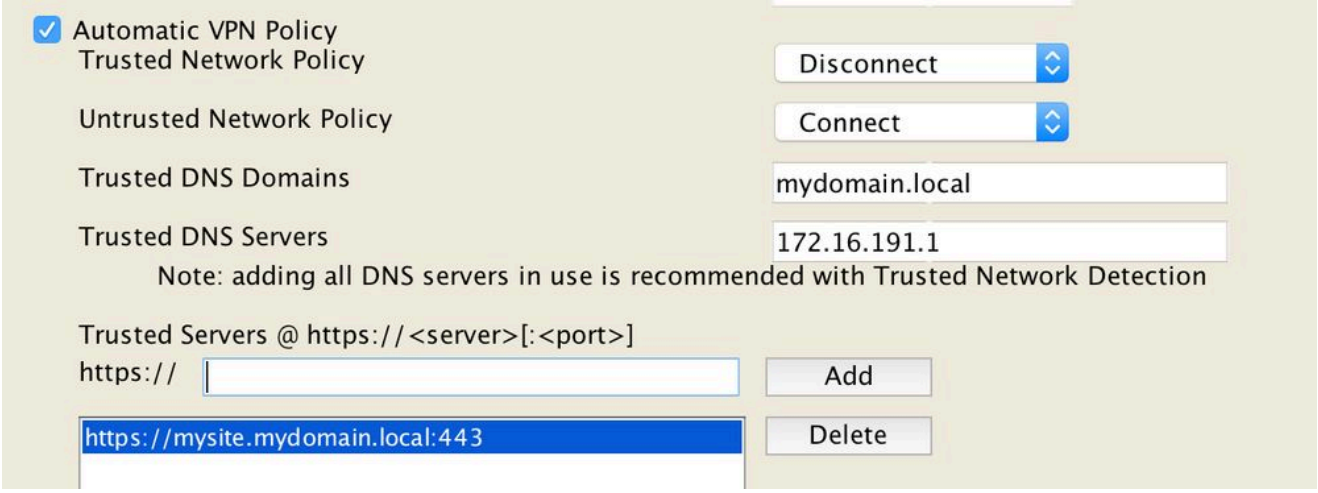
サードパーティVPNに関する特別な考慮事項

常時接続VPN

信頼できるDNSサーバが定義されている場合、スタンドアロンローミングクライアントは、Cisco Secure ClientのAlways On VPN設定と互換性がありません。アクティブの場合、スタンドアロンローミングクライアントは常にDNSを127.0.0.1に設定し、信頼されたすべてのDNSサーバをNIC設定から除外します。DHCP設定を復元するために、ネットワーク上でローミングクライアントを無効にすることができます。ただし、ローミングクライアント関連の保護はすべて構成時に停止します。信頼できるネットワークでクライアントを無効にする方法の詳細については、Umbrellaサポートにお問い合わせください。

解決方法

- CSC + Roamingセキュリティモジュール（Cisco Secure ClientのRoamingクライアント）は影響を受けず、自動VPNポリシーで効果的に機能します。
- 127.0.0.1を信頼できるDNSサーバのリストに追加します。
- すべてのネットワークが信頼できると宣言されないように、信頼できる検出の代替方法（DNS名とサーバー）が定義されていることを確認してください。



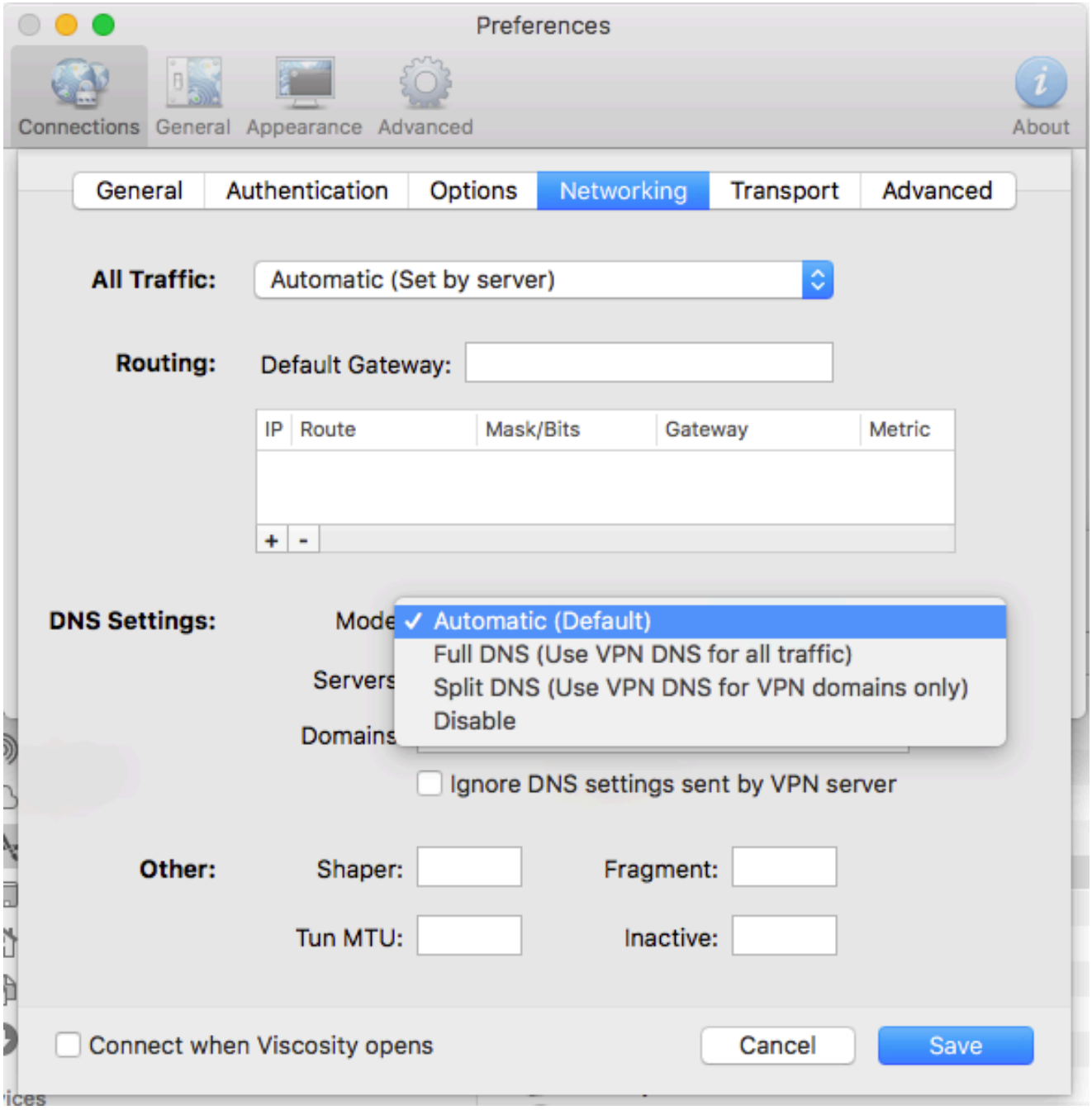
360031250911

粘度VPN

粘性VPNでは、Umbrella口ーミングクライアントで機能するように設定を変更する必要があります。この変更を行わない場合、粘度の既定の動作は、他の互換性のないVPNの動作と同じになります。この変更により、検索ドメイン内のすべてのドメインに対してUmbrellaサーバ経由でプッシュされたDNS設定を使用するようStickityに指示し、その他の要求に対しては引き続き127.0.0.1を使用します。

粘性の設定

1. 粘性で、設定>接続> <接続>（サイト固有）>ネットワーキング> DNS設定に移動します。
2. Automatic (Default)を選択します。



115013433283

OpenVPNサーバを使用する場合は、接続解除または再接続時にネットワークの変更がトリガーされるように、サーバ側でpersist-tunが無効になっていることを確認します。

トンネルブリック

Tunnelblickでは、次の2つの変更が必要です。

- アダプタのDNSサーバの変更を許可します。
- トンネルの確立後にDNS設定を適用します。

Advancedメニューで、指定された設定を確認することにより、TunnelblickはUmbrellaローミングクライアントで機能します。

Connecting and Disconnectingタブで、次の2つの設定を有効にします。

- 接続または切断後にDNSキャッシュをフラッシュする（既定）
- ルート設定前ではなく、ルート設定後にDNSを設定する

While Connectedタブで、この設定をIgnore:

- DNS:Servers > When changes to the pre-VPN value, When changes to anything.（サーバ> VPN前の値が変更されたとき、その他の値が変更されたとき）

OpenVPNサーバを使用する場合は、接続解除または再接続時にネットワークの変更がトリガーされるように、サーバ側でpersist-tunが無効になっていることを確認します。

Tunnelblick VPNの接続解除の問題

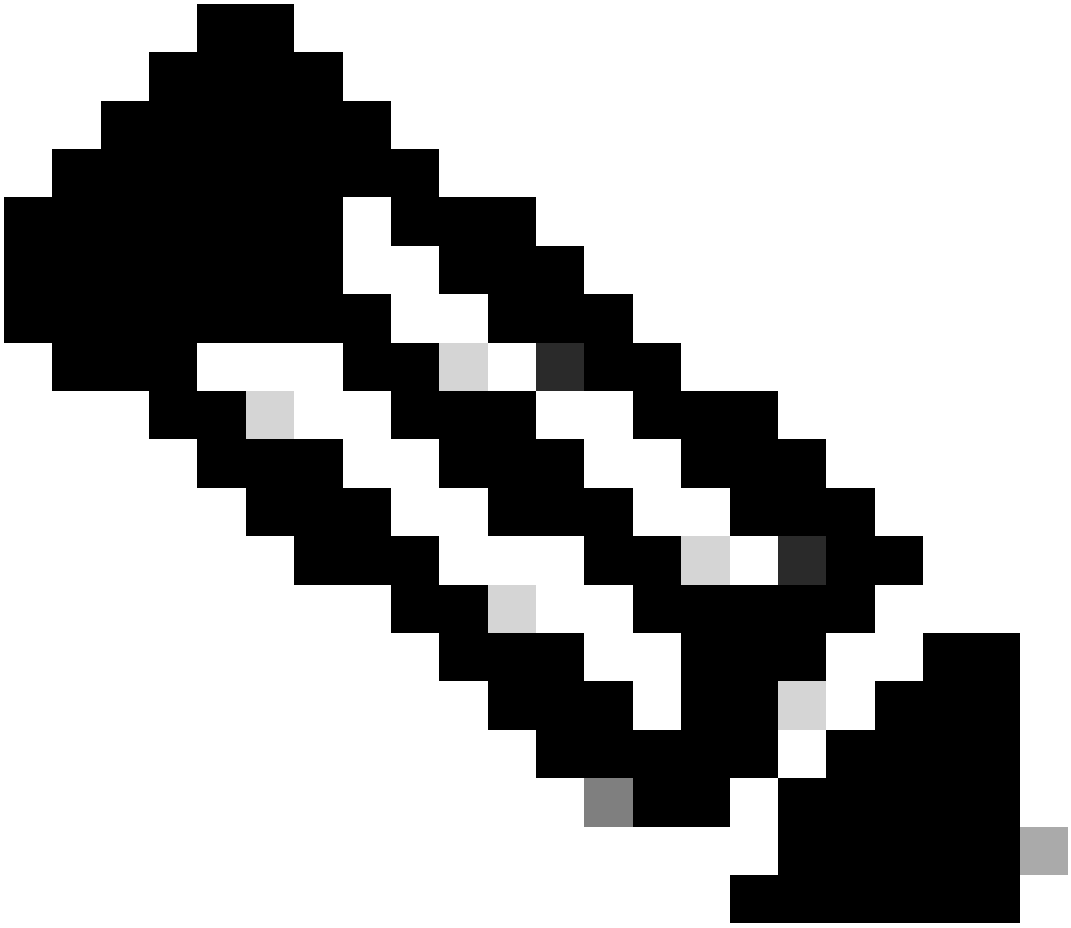
一部のTunnelblickバージョンでは、VPNの切断後にローミングクライアントが正しい内部DNSサーバを正しく識別できません。VPNの接続解除後に内部ドメインに関する問題が発生した場合、Umbrellaは次の手順を推奨します。

この変更により、VPNが接続解除された後、Tunnelblickはプライマリネットワークインターフェイスをダウンおよびアップ状態にします。これは、Tunnelblick設定パネルのSettingsタブで管理します。

- Tunnelblickの古いバージョン（3.7.5beta03より前）では、Reset the primary interface after disconnectチェックボックスを使用します。
- Tunnelblickの新しいバージョン（3.7.5beta03以降）では、On expected disconnectとOn unexpected disconnectの両方の設定をReset Primary Interfaceに設定します。

ライトスピードロケット

Lightspeed Rocketには、Roaming Clientと互換性のない一部の機能があります。特に、www.google.comからnosslsearch.google.comへのNo SSL SearchおよびSafeSearch CNAMEリダイレクションとforceasesearch.comへのDNS変更により、Lightspeed Rocket DNSリダイレクションが有効である限り、すべてのwww.google.com DNS解決が失敗します。



注：この記事では、スタンドアロンのUmbrellaローミングクライアントについて説明します。Cisco Secure Clientおよびレガシーソフトウェア用のUmbrella Roamingセキュリティモジュールに関する関連記事については、関連ドキュメントを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。