

Windows 10ネイティブVPN API (Modern/Metroアプリケーション) のトラブルシューティング

内容

[はじめに](#)

[影響](#)

[根本原因](#)

[解決方法](#)

はじめに

このドキュメントでは、[MicrosoftのUniversal Windows Platform](#)(UWP)上に構築されたVPNアプリケーションの使用率について説明します。これらのアプリケーションは通常、Windows 8以降のMetro/Modern GUIでアプリケーションとして表示されます。デスクトップアプリケーションおよび従来のWindowsスタイルのプログラムは、UWPを使用しないため、影響を受けません。

アプリ以外の形式のWindows VPNまたはAlways on VPNで問題が発生する場合は、『Umbrella Roaming ClientでのWindows VPNに関する注意事項：ソフトウェアとVPNの互換性ガイド』を参照してください。

AnyConnect Umbrellaローミングモジュールでは、同じ相互運用性の問題は発生しません。

影響

ローミングクライアントがアクティブの場合、UWP VPNアプリケーションユーザがVPNセッションを開始しようとする時、「No such host is known」などのエラーメッセージが表示されます。これにより、ユーザがVPNに正常に接続できなくなります。このエラーは、ローミングクライアントが停止している場合、またはVPNクライアントのデスクトップエディションが使用されている場合は表示されません。

たとえば、次のコマンドは機能しません。

- Pulse Secure App +ローミングクライアント
- SonicWall MobileConnect +ローミングクライアント

これらの場合、同じVPNヘッドエンドへの接続は機能します。

- Pulse Secure Desktopアプリケーション+ローミングクライアント
- SonicWall NetExtenderまたはSonicWall Desktopアプリケーション+ roamingクライアント
- Pulse Secure App + AnyConnect Umbrellaローミングモジュール*
- SonicWall MobileConnect + AnyConnect Umbrellaローミングモジュール*

*AnyConnect Umbrellaモジュールは、127.0.0.1 (別のインターフェイス) をDNS設定として設定せず、カーネルドライバを使用してDNSを127.0.0.1にリダイレクトします。UWPアプリは、DNSに別のアダプターを使用していることを認識していないため、この時点では影響を受けません。

根本原因

Microsoftは、よりサンドボックス化された最新のアプリケーションをWindows 8+で開発しました。VPNアプリケーションには、次の制限のいずれかが適用されます。UWP (アプリケーション) 上に構築されたVPNは、クエリを生成するインターフェイスを使用するように制限されます。Umbrellaのローミングクライアントは127.0.0.1 (異なるインターフェイスI0) でリスニングしているため、クエリはローミングクライアント (または127.0.0.1で実行されているその他のDNS転送) にヒットしません。

次のコールでは、ソケットの作成を1つのインターフェイスに制限できます。これは、DNSをインターフェイスに制限する既知のUWP VPNアプリケーションの場合です。

ConnectAsync (ホスト名, 文字列, SocketProtectionLevel, ネットワークアダプター)

"ConnectAsync(Hostname, String, SocketProtectionLevel, NetworkAdapter)メソッドによって使用される名前解決メカニズムは、ドメインネームシステム(DNS)名前空間の指定されたインターフェイスに制限されています。" <https://learn.microsoft.com/en-us/uwp/api/windows.networking.sockets.streamsocket>

Windows VPN APIは、この接続メカニズムまたは同様の接続メカニズムを利用すると考えられています。その結果、DNS用に127.0.0.1を使用するため、UWP「アプリ」形式のVPNはローミングクライアントで機能しなくなります。その結果、DNSが127.0.0.1に送信されるため、VPN接続は失敗します。ただし、コールの制限のため、ローミングクライアントでは受信も応答もされません。その結果、DNSの障害が原因でVPN接続が失敗します。

根本原因は、Windows NCSI接続インジケータの設計上の制限と同様です。このインジケータでは、DNS接続を確認するために127.0.0.1が照会されることはありません (Microsoftによって解決されます)。

解決方法

現時点では、スタンドアロンのローミングクライアントに対しては、127.0.0.1がローカルDNSサーバとして設定されているため、このWindowsの動作を変更できるローミングクライアントへの更新はありません。これはコアです
ローミングクライアントが機能するための要件。MicrosoftがUWP VPNアプリケーションによるDNSへの127.0.0.1の使用を許可するまでは、VPNクライアントのデスクトップエディションに切り替えるか、DNSを指示するためにカーネルドライバを使用するAnyConnectローミングモジュールを使用する唯一のオプションです。

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。