Umbrellaモジュールを使用したセキュアクライアントでのTunnel All DNSの有効化

内容

はじめに

このドキュメントでは、Umbrellaモジュールを使用してCisco Secure Clientのtunnel all DNSを有効にする方法について説明します。

背景説明

シスコは2023年にCisco AnyConnectのサポート終了を、2024年にUmbrellaローミングクライアントを発表しました。Cisco Umbrellaをご利用のお客様の多くは、すでにCisco Secure Clientへの移行のメリットを享受しています。より良いローミング環境を得るために、できるだけ早く移行を開始することをお勧めします。ナレッジベース記事「How do I install Cisco Secure Client with the Umbrella Module?」の詳細を参照してください。

Cisco Secure Client(CSC)とUmbrella（以前のAnyConnect Roaming Security）モジュールは、特別な設定を必要とせずほぼすべてのCSC VPNモードで動作するように設計されています。

ただし、次の条件の両方に当てはまる場合は、さらに考慮が必要です。

- スプリットトンネリングが有効である
- 「Tunnel All DNS」機能が有効になっている

問題と影響

「Tunnel All DNS」を有効にすると、DNSトラフィックはカーネルレベルで代行受信され、正しいVPNインターフェイスから送信されない場合はブロックされます。Cisco Umbrellaリゾルバがスプリットトンネル(Include)設定の一部ではない場合、これによってCSCモジュールに問題が発生します。

デフォルトでは、CSCモジュールは「Tunnel All DNS」によってブロックされていない暗号化DNS（UDPポート443）を使用するため、この問題の影響は最小限です。 したがって、この問題が発生するのは、DNS暗号化を使用できないネットワークだけです。

シナリオは次のとおりです。

- Roamingモジュールは、通常のLANインターフェイスを介してトラフィックをCisco Umbrellaにルーティングしようとします。
- ローカルネットワークはDNS暗号化を許可しないため、標準の暗号化されていないDNSクエリを送信します。
- このトラフィックは、「Tunnel All DNS」機能によってブロックされます。この機能を使用するには、VPNを通過するDNSが必要です。

このシナリオでは、DNSは期待どおりに機能しません。

推奨事項

このような状況が発生しないようにするため、Cisco Umbrellaでは次のいずれかの対策を推奨しています。

- VPNグループポリシーで「Tunnel All DNS」を無効にします。CSCモジュールはDNSのルーティングを処理します。
  または
- 次のCisco Umbrella DNSリゾルバをスプリットトンネル(Include)設定に追加します。
  - 208.67.222.222
  - 208.67.220.220
  - 208.67.222.220
  - 208.67.220.222

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。