TLS/DTLSおよびIPsec(IKEv2)デュアル設定でのCisco Secure Access RAVPNプロトコルの動作

内容

お問い合わせ内容

TLS/DTLSとIPsec(IKEv2)の両方のプロトコルがCisco Secure Access RAVPNで有効になっており、プライマリプロトコルがIPsec(IKEv2)に設定されている場合、IPsecトラフィック（UDPポート500/4500）がブロックされているネットワークからVPN接続を確立しようとすると、接続エラーが発生します。Secure Clientでは、クライアントUIのドロップダウンでIPsecオプションがデフォルトで使用され、IPsec接続が失敗してもTLS/DTLSに自動的にフェールオーバーしません。その結果、接続エラーが発生し、制限されたネットワーク環境からRAVPN接続を確立できなくなります。

環境

- デュアルプロトコル設定のCisco Secure Access RAVPN
- TLS/DTLSプロトコルとIPsec(IKEv2)プロトコルの両方が有効
- IPsec(IKEv2)として構成されたプライマリプロトコル設定
- 個別のIPsecおよびTLSオプションを含むプロトコル選択ドロップダウンを使用したセキュアクライアント
- UDPポート500および4500でIPsecトラフィックをブロックするネットワーク環境

解決策

確認された動作は、予期される動作であり、仕様により異なります。Cisco Secure Access RAVPNは、両方のプロトコルが有効になっていて、プライマリプロトコルで接続の問題が発生した場合、IPsec(IKEv2)からTLS/DTLSへの自動プロトコルフェールオーバーを実行しません。

手動でのプロトコル選択が必要

IPSecトラフィックをブロックするネットワークから接続する場合、ユーザはセキュアクライアントで適切なプロトコルを手動で選択する必要があります。

ステップ1:セキュアクライアントアプリケーションを開きます

ステップ2:クライアントインターフェイスでプロトコル選択ドロップダウンメニューを見つけます

ステップ3:選択をIPsecオプションからTLSオプションに手動で変更します

ステップ4:TLS/DTLSプロトコルを使用してVPN接続を開始します。

プロトコル動作の明確化

Cisco Secure Access RAVPNのPrimary protocol設定によって、Secure Clientで提示されるデフォルトプロトコルが決定されますが、自動フェールオーバー機能はイネーブルになりません。TLS/DTLSとIPsec(IKEv2)の両方が有効な場合：

- セキュアクライアントのドロップダウンメニューには、個別のプロトコルオプションが表示されます
- クライアントはデフォルトでプライマリプロトコル設定（この場合はIPsec）に設定されます
- ネットワーク接続の状態に基づくプロトコル間の自動切り替えは行われない
- ユーザは、ネットワーク環境に基づいて適切なプロトコルを手動で選択する必要があります

原因

Cisco Secure Access RAVPNは、自動プロトコルフェールオーバー機能を備えていない設計になっています。TLS/DTLSとIPsec(IKEv2)の両方のプロトコルが有効な場合、システムはセキュアクライアントインターフェイスを介して手動でプロトコルを選択する必要があります。Primary protocol設定では、クライアントのドロップダウン・メニューのデフォルトの選択のみが決定され、プライマリ・プロトコルで接続の問題が発生した場合に自動スイッチング・ロジックは実装されません。

関連コンテンツ

- Cisco Secure Accessのドキュメント
- シスコのテクニカルサポートとダウンロード

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。