セキュアクライアントマシンのトンネル認証のポップアップによる信頼できないネットワークでの切断

内容

お問い合わせ内容

Cisco Secure Client(AnyConnect)は、特にユーザが信頼できないネットワークから接続している場合、マシントンネルの接続中にユーザ名とパスワードの入力を繰り返し求めます。認証ポップアップはマシントンネルの接続を中断し、接続を解除するため、ユーザが安定したリモートアクセスを維持する機能に影響を与えます。この問題は、マシントンネルが適切に確立および認証され、予期しないポップアップが表示されてVPNセッションの継続性が中断されるにもかかわらず発生します。

環境

- Cisco Secure Client(AnyConnect)とマシントンネルの設定
- 信頼ネットワーク検出(TND)機能が有効になっているリモートアクセスVPNプロファイル
- マシントンネルに接続されたユーザマシン
- クライアントプロファイルの配布に使用されるグループポリシーオブジェクト(GPO)
- TND設定で設定されたユーザトンネルとマシントンネルの両方のプロファイル

解決策

この問題は、マシントンネルプロファイルとユーザトンネルプロファイルの両方の信頼ネットワーク検出(TND)設定を変更することで解決されました。このソリューションでは、TNDアクションの動作を設定して、信頼できないネットワークで不要な認証プロンプトが表示されるのを防ぎ

ます。

ステップ1：信頼できないネットワークのTND設定

Trust Network Detectionアクションを、マシントンネルプロファイルとユーザトンネルプロファイルの両方で、信頼できないネットワークに対してDo nothingに設定します。この設定により、信頼できないネットワークに接続する際にクライアントが追加のクレデンシャルを求めなくなります。

手順2：信頼できるネットワークのTND設定を構成する

信頼できるネットワークの場合はTrust Network Detection actionをDisconnectに設定し、既知のセキュアなネットワーク環境で意図したセキュリティ動作を維持します。

ステップ3：設定変更の導入

更新されたTND設定をグループポリシーオブジェクト(GPO)プッシュによって展開し、影響を受けるすべてのクライアントマシンに設定変更を配布します。

ステップ4：クライアントマシンの再起動

プロファイルの更新後にクライアントマシンをリブートして、新しいTND設定が正しく反映されるようにします。

ステップ5：検証テスト

複数の信頼できないネットワークを介したマシントンネル接続をテストして、次のことを確認します。

- 認証ポップアップが表示されなくなります

- マシントンネルは一貫して接続されたままです
- クレデンシャルプロンプトがVPNセッションを中断しない
- ユーザは切断することなく安定したリモートアクセスを維持できる

これらの変更を実装した後、ユーザは問題なく解決できることを確認しました。複数のユーザテストを実施し、さまざまなネットワーク条件で安定したVPNセッションの継続性を検証しました。

原因

根本原因は、Cisco Secure Clientプロファイル上の信頼ネットワーク検出(TND)設定の誤設定でした。TND機能は、マシントンネルがすでに適切に認証され確立されていても、信頼できないネットワークから接続されたユーザに対して認証プロンプトをトリガーしていました。ユーザトンネルプロファイルとマシントンネルプロファイルの両方に対するTNDアクションがネットワーク環境に対して最適に設定されていないため、クライアントが不要に追加のクレデンシャルを要求する原因となり、マシントンネル接続が中断されます。

関連コンテンツ

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。