

セキュアクライアントTNDの手動VPN接続動作とURLブロッキングの考慮事項

内容

お問い合わせ内容

信頼できるネットワークの設定が切断に設定されている信頼できるネットワーク検出(TND)機能でVPNプロファイルを使用すると、ユーザがCisco Secure Clientを使用して手動で接続を開始した場合でも、信頼できるネットワーク内にあるエンドポイントは正常にVPN接続を確立できます。

この動作は、信頼できるネットワークでエンドポイントが検出されたときにVPNセッションを切断するようにTND設定が設定されているにもかかわらず発生します。

特定された具体的な懸念事項は次のとおりです。

- 信頼されたネットワークエンドポイントからの手動VPN接続は、標準のTND設定では制御またはブロックできません
- Cisco Secure Access(CSA)の設定が、信頼できるネットワークエンドポイントからの手動VPN接続をブロックできるかどうか不明
- VPNプロファイル接続URL(xxxx.vpn.sse.cisco.com)の安定性に関する質問と、このURLが定期的に変更され、ファイアウォールベースのブロッキング戦略に影響を与えるかどうかについての質問

環境

- Cisco Secure Access(CSA)の導入
- VPNプロファイル設定を使用したCisco Secure Client
- 信頼ネットワーク検出(TND)機能が有効

- Disconnectとして設定されたTND Trusted Network設定
- 設定された信頼ネットワーク内に配置されたエンドポイント
- ネットワークアクセス制御用のファイアウォールインフラストラクチャ

解決策

手動VPN接続でのTNDの動作について

確認された動作は、文書化されているCisco Secure Clientの機能と一致しています。シスコのドキュメントによれば、TNDは信頼ネットワーク上でユーザが手動で開始するVPNセッションを切断したり阻止したりしません。これは、TNDの設定に関係なく、正常な動作です。

主な技術的な事実は次のとおりです。

- TND自動切断機能は、自動的に確立されたVPN接続にのみ適用されます。
- ユーザが開始した手動のVPN接続は、TND接続解除動作をバイパスします。
- 信頼できるネットワークエンドポイントからの手動VPN接続をブロックするCSA構成設定が存在しません。

運用上の軽減戦略

信頼できるネットワークエンドポイントからの手動VPN接続を制御する主な方法は、ネットワークレベルの制御を通じて行われます。

ステップ1：ファイアウォールURLブロッキングの実装：VPNプロファイル接続URL(xxxx.vpn.sse.cisco.com)へのアクセスをブロックするように、信頼できるネットワークファイアウォールを設定します。これにより、信頼ネットワーク上のエンドポイントがVPNサービスエンドポイントに到達しなくなります。

ステップ2:URLの安定性の確認：VPNプロファイルURL識別子(xxxx部分)はテナント固有であり、定期的に変更されるものではありません。これにより、ファイアウォールブロッキングルー

ルの安定したターゲットが提供されます。

検証およびテスト

テストの結果、信頼できるネットワークファイアウォールでVPNプロファイル接続URLをブロックすると、ユーザがCisco Secure Client経由で手動接続を試みても、エンドポイントがVPN接続を確立できないことが確認されました。

原因

この動作は、Cisco Secure Client TNDの実装での設計上の動作です。TND機能は、特にネットワークの信頼ステータスに基づいて自動VPN接続を管理するように設計されていますが、ユーザが開始する手動VPN接続を意図的に妨げることはありません。この設計により、ユーザは必要に応じて自動動作を上書きしながら、一般的なユースケースに対して自動化されたネットワーク検出と接続管理を提供できます。

関連コンテンツ

- [Cisco Secure Client管理者ガイド – TND設定](#)
- [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。