Palo AltoおよびSecure Access NTG経由のRAVPNaaSからのPR到達可能性のトラブルシューティング

内容

お問い合わせ内容

ユーザはCisco Secure Clientを使用してクラウドVPN接続を正常に確立できましたが、接続後に内部のプライベートリソースにアクセスできませんでした。バックエンドチェック中にVPNトンネルがセキュアアクセス側で接続されているように見えましたが、接続されたユーザは内部ネットワークサービスにアクセスできませんでした。VPN認証とトンネルの確立に成功したにもかかわらず、この接続の問題によりユーザの内部資産へのアクセスに影響が及びました。

環境

- Cisco Secure Client
- セキュアアクセスのネットワークトンネルグループ
- エッジファイアウォールとしてのPalo Alto
- 内部プライベートネットワークリソースの設定
- セキュアアクセスリモートVPN

解決策

接続の問題は、Palo Altoファイアウォール側でコラボレーティブなトラブルシューティングセッションを行い、トンネルをリセットすることで解決しました。

実施されたトラブルシューティング手順

ステップ1：初期接続の検証

現在の接続の状態を検証し、バックエンドチェックでセキュアアクセス側トンネルが接続済みとして表示されていることを確認します。

ステップ2：トンネルのリセットID

トラフィックがPalo Altoを離れて到達しているかどうかを確認するために、Cloud Native Headend(CNHE)のパケットを取得します。

ステップ3:Palo Altoトンネルのリセット

Palo Alto側ではトラフィックは観測されませんでした。

ステップ4:VPN再接続

トンネルリセットを実行することを推奨します。トンネルがリセットされると、ユーザはSecure Clientを使用してVPNに再接続し、リセットインフラストラクチャを介して新しいトンネル接続を確立します。

ステップ5：接続の検証

再接続後、内部リソースアクセスが復元され、ユーザはVPN接続を介して内部ネットワークサービスに正常に到達できることを確認しました。

原因

根本的な原因は、Palo Altoファイアウォール側のトンネル状態の不整合に関連するもので、VPN認証が成功しても内部トラフィックが適切にルーティングされないことにあります。トンネルリセット手順によって、これらの状態の不整合が解消され、内部リソースアクセスの適切な接続パスが復元されました。

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。