Secure Access Network Tunnel Group Internal Server Error Reverting Primary Peer IP（セキュアアクセスネットワークトンネルグループの内部サーバエラー：プライマリピアIPを復帰させる際のエラー）

内容

問題

Cisco Secure Access上のNetwork Tunnel Group(NTG)でリモートピアIPを変更しようとすると、プライマリトンネルIPを以前に設定された値に戻そうとする際に、UIに「Internal Server Error」が表示される場合があります。具体的なシナリオは次のとおりです。

- NTGは最初にプライマリトンネルIPとセカンダリIPで設定され、両方のトンネルが正常に確立されました。
- テスト目的で、プライマリトンネルIPを別のIPアドレスに変更します。これは問題なく受け入れられます。
- プライマリトンネルIPを元の値に戻そうとすると、システムは設定の保存に失敗し、UIに「Internal Server Error」が返されます。
- この動作は常に再現可能であり、以前に設定したIPアドレスを再利用しようとすると表示されます。
- 元のIPは以前は動作しており、セカンダリトンネルIPとの競合はありません。

環境

- Cisco Secure Access（旧称Cisco Umbrella for SSE）
- プライベートアクセス用のネットワークトンネルグループの設定

- プライマリおよびセカンダリピアIPを使用したデュアルトンネル設定
- Webベースの管理インターフェイス

解決方法

この問題は、設定の変更後も元のピアIPがバックエンドシステムで予約されたまま、またはスタックされたままになるという、バックエンドの検証/状態の問題が原因で発生します。次のセクションで説明するトラブルシューティングと解決の手順に従う必要があります。

ステップ1：診断情報の収集

バックエンド検証のために次の情報を収集します。

- セキュアアクセス組織ID
- ネットワークトンネルグループ名
- 該当するプライマリトンネルのトンネルID
- NTG用に選択された地域/データセンター
- 失敗した保存の試みの正確なタイムスタンプ（タイムゾーンを含む）
- 元のIPが他のNTG（現在または以前）に表示されるかどうかを確認します。
- 失敗した保存の試みのブラウザHARキャプチャ

ステップ2：ブラウザのHARファイルをキャプチャする

失敗した保存の試行に関する診断データを収集するには、次の手順を実行します。

- ブラウザー開発者ツールを開く
- Networkタブに移動します。
- ログの保存を有効にする

- 保存の失敗を再現する
- HARファイルをエクスポートし、サポートケースに添付します


注:HARファイルをアップロードする前に、セッショントークンまたはCookieをサニタイズ/削除してください。

ステップ3：バックエンドの検証とクリーンアップ

この問題はバックエンドの介入を必要とし、UIだけで解決することはできません。シスコテクニカルサポートは、次のアクションを実行する必要があります。

- Secure Accessバックエンド/SSEプラットフォームチームとの連携
- 古いピアIP予約の検証
- 孤立したトンネルオブジェクトの確認
- 特定のNTG設定に関連付けられた重複したバックエンドキーを特定します。
- 元のIPに対する古いトンネルピア参照をクリアします
- 必要に応じてNTGオブジェクトのバックエンドの再同期を強制する
- NTG UUIDに関連付けられたリリースピアIP割り当て

ステップ4：別の解決方法

バックエンドクリーンアップがすぐに使用できない場合は、次の手順を実行します。

- Network Tunnel Groupのプライマリ設定を削除する
- 5分間待ちます
- 必要なIPアドレスを使用してNTGを再度追加します


注意：可能です。ここで説明する詳細には、実行すると重大な影響を与える可能性のある

プロシージャまたはコマンドが含まれています。実行または推奨を行う前に、上記の手順またはコマンドがSMEまたは事業部門によって評価されていることを確認してください。

ステップ5：一時的な回避策

NTGが実稼働中で取り外せない場合は、次の手順を実行します。

- 接続には引き続きセカンダリトンネルを使用します
- ベンダー/パートナーから代替パブリックIPを取得する
- 代替IPを使用するようにNTGプライマリを更新します
- バックエンドの問題が解決されるまで、冗長性の低下を確認します。

原因

この問題は、Cisco Secure Accessバックエンドシステムのソフトウェアの不具合が原因で発生します。プライマリピアのIPが変更され、元の値に戻されると、バックエンド検証システムは、元のIPが再利用できる必要がある場合でも、誤って割り当てまたは予約済みとして扱います。この結果、バックエンド検証エラーが発生し、UIによって一般的な「内部サーバエラー」としてマスクされます。 バックエンドシステムが設定変更プロセス中にIP予約を適切にクリーンアップまたは解放できず、永続的な状態の問題が発生して、同じNTGでのIPの再利用が妨げられます。

関連コンテンツ

- Cisco Secure Accessの基本情報のトラブルシューティングと収集
- 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。