セキュアアクセスにおけるMX75ネットワークトンネルのセキュアクライアントIDの可視性の問題

内容

お問い合わせ内容

セキュアアクセスに接続するMX75ネットワークトンネルの背後にセキュアクライアントを備えたエンドポイントを展開すると、ローミングするクライアントとユーザのIDがシステム内で正しく認識されません。次の特定の動作が確認されました。

- エンドポイントがMX75の背後にある場合、ネットワークトンネル接続よりもセキュアクライアントを優先するように設定されたバックオフ設定が期待どおりに機能しない
- ドメインに基づくトラフィック制御ルールは、トラフィックがローミングクライアントではなく、ネットワークトンネルIDのみに起因するため、適用されません
- アクティビティ検索では、不完全な発信元の口ケーション情報が表示され、ユーザおよび口ーミングクライアントのIDを省略している間、ネットワークトンネルのIDだけが表示されます
- IDベースのトラフィックステアリングルール（Active Directoryユーザまたはローミングクライアントに基づくもの）は、MX75トンネルを通過するトラフィックに適用できません

この動作により、ネットワークトンネルインフラストラクチャを介して接続しているエンドポイントに対して、IDの適切な分離とポリシーの適用が行われなくなります。

環境

- シスコセキュアアクセスの導入
- セキュアアクセスのためのネットワークトンネル設定を備えたMX75アプライアンス
- すべてのエンドポイントにインストールされたSecure Clientエージェント
- ネットワークトンネル接続よりも安全なクライアントを優先するために、ローミングクライアントで無効にされたバックオフ設定
- ドメインベースルーティング用に設定されたトラフィックステアリングルール

- Active Directoryユーザーとローミングクライアント用に構成されたIDベースのポリシー

解決策

この問題は、MX75ネットワークトンネルを介したローミングIDの可視性に依存する代わりに、登録済みネットワークアプローチを使用した回避策の設定を実装することで解決されました。

回避策の実装

ステップ1：登録済みネットワークでRSM(Roaming Security Module)を設定します。

既存のネットワークトンネル設定を、登録済みネットワーク設定と組み合わせたRSM展開に置き換えます。この設定により、IDの帰属とポリシーの適用を適切に行うことができます。

手順2:IDの可視性の検証

登録済みネットワークの設定を実装した後、次の点を確認します。

- アクティビティ検索でユーザIDが正しく表示される
- ローミングクライアントIDが表示され、正しく属性が設定されている
- ユーザおよびクライアントのID機能に基づくトラフィック制御ルール

ステップ3：トラフィックステアリング機能をテストする

新しい設定で、ドメインベースのトラフィックステアリングルールとIDベースのポリシーが正しく適用されることを確認します。

代替アプローチ

プライベートネットワーク上でIDの分離が不要な環境では、RSM（インターネット設定）の実装を検討してください。このアプローチでは、RSMトラフィックがプライベートネットワークのトンネル経由ではなく、インターネットに直接送信されます。これにより、セキュリティ制御を維持しながら、適切なIDの可視性が提供されます。

技術分析

トラブルシューティング中、エンドポイントがMX75トンネルの背後にあるときのID帰属動作を示すために、policy.test.sse.cisco.comを使用して診断出力が収集されました。分析により、ネットワークトンネルを介してローミングIDをルーティングすることは技術的に可能であるものの、この特定の導入シナリオでは推奨またはサポートされる運用フローではないことが確認されました。

原因

根本原因は、トラフィックがネットワークトンネルインフラストラクチャを通過する際に、セキュアアクセスがIDの帰属をどのように処理するかに関連しています。エンドポイントがMX75ネットワークトンネルを介して接続すると、システムは個々のローミングクライアントとユーザのIDを保持するのではなく、すべてのトラフィックをトンネルのIDに関連付けます。この動作はネットワークトンネル接続の設計によるものですが、個々のIDの可視性とポリシーアプリケーションの要件と競合します。

ネットワークトンネルを介してローミングIDをルーティングすることは技術的に可能ですが、前述のID帰属制限のため、この設定は標準運用フローとして推奨されず、サポートもされていません。

関連コンテンツ

- 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。