ローミングクライアントSWGトラフィック用のDuo IdPを使用したCisco Secure Access SSO認証

内容

お問い合わせ内容

ローミングクライアントから発信されたセキュアアクセスSWG (セキュアWebゲートウェイ) トラフィック用にDuo IdPでSSO認証を使用しようとすると、Duo SSO認証の入力が求められず、セキュアアクセスダッシュボードにユーザIDが入力されません。Webトラフィックは、認証が有効で目的のSWGルールに一致し、トラフィックが復号化されますが、認証フローはローミングクライアントトラフィックに対して開始されず、Webアクティビティのユーザレベルの識別を妨げます。

具体的には、次の動作が確認されました。

- SWGのロギングとアクティビティにより、トラフィックが目的のSWGルールに一致し、宛先トラフィックが復号化されたことが示されました
- ログとSecure Accessアクティビティビューには、PCのIDとネットワークIDのみが表示され、Duo/SAML認証チャレンジ、SSOリダイレクト、対話型プロンプトは表示されませんでした
- ポリシーエントリはローミング情報とオリジン情報のみを示し、AD参加前にはユーザIDは存在しませんでした
- トラブルシューティング中にテストVMがActive Directoryに参加すると、Secure Access Activity SearchにユーザIDが表示されるようになりましたが、Duo/SAMLのインタラクティブプロンプトは表示されませんでした

環境

- SWG機能を備えたCisco Secure Access
- Secure Clientバージョン5.1.13.177
- SSO認証用に設定されたDuo IdP

- 組織のサブスクリプション：Secure Access Essentials
- Webプロキシの再認証間隔を日次に設定
- テスト中にPACファイルまたはVPNが使用されていない
- ローミングコンピューター構成を使用して環境をテストする

解決策

包括的な分析とテストの結果、SAMLを使用したSSO認証は、製品の設計上の制限により、セキュアアクセスローミングクライアントトラフィックではサポートされないことが判明しました。この制限を確認するために、次のトラブルシューティング手順を実行しました。

ステップ1：ライブトラブルシューティングと動作の再現

テストでは、SWGポリシーの照合とSSL復号化は正しく行われていることが確認されましたが、ローミングするクライアントトラフィックに対して認証フロー（インタラクティブSAML/Duo SSOリダイレクトおよびチャレンジ）が開始されませんでした。

ステップ2：ルールとソースの変更

SWG規則のソースが、復元試行中にローミングコンピューター名から特定のユーザーIDに変更されました。Secure Clientサービスが再起動され、ポリシーの伝達が確認されました。これらの変更では、認証フローの問題は解決されませんでした。

手順3: Active Directory参加のテスト

テストVMは、ユーザIDの可視性への影響を判断するためにActive Directoryに参加しました。これにより、Secure Access Activity SearchでユーザIDが表示されるようになりましたが、Duo/SAMLのインタラクティブプロンプトはまだ表示されず、問題がユーザIDの可視性のみに関連していないことを確認しています。

ステップ4:DARTバンドルの分析

DARTバンドルが収集され、分析されました。この分析により、SWGポリシーの適用は確認されましたが、ローミングクライアントトラフィックの認証フローの開始は示されておらず、この動作は設計上のものであるという結論に達しました。

ステップ5:Duo IdP構成の検証

Duo IdPのメタデータと設定に対する独立したテストが正常に実行および完了し、Duo設定自体が問題の原因ではないことが確認されました。

ステップ6：内部検証

SAMLを使用したSSO認証は、製品設計上の制限として、セキュアアクセスローミングクライアントトラフィックではサポートされていません。

結論：設定ミスは見つかりませんでした。インタラクティブなSSOプロンプトがないのは、修正可能な設定の問題ではなく、製品サポートの明示的な制限が原因でした。

原因

この問題は、SAMLを使用したSSO認証（Duo IdP統合を含む）がセキュアアクセスローミングクライアントトラフィックでサポートされていない製品設計の制限が原因で発生します。これは、現在のSecure Accessプラットフォームアーキテクチャに固有の制限であり、設定の問題やソフトウェアのバグとは関係ありません。

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。