Cisco Secure Accessで個人のGoogleアカウントを使用するゲストユーザのZTNA登録の失敗

内容

お問い合わせ内容

ZTNA(Zero Trust Network Access)によるプライベートアクセスの展開中に、Entra IDへの登録とセキュアアクセスでのプロビジョニングが成功した後で、ゲストユーザを個人のGoogleアカウントに登録すると失敗します。発生する具体的な症状には、次のものがあります。

- クライアントベースの登録：登録プロセスがSSO認証に到達し、クレデンシャルが提供されますが、ZTNAに「I/O error」が表示され、登録プロセスがスタックします
- クライアントレスアクセス：エラーメッセージ「Cisco Secure Access Login failure.Check IDP Configuration」とトランザクションIDを確認します。

これらの障害により、プライベートリソースへのアクセスが妨げられ、非企業IDを使用した契約者形式のアクセスに対するZTNA機能のテストに影響が及びます。

環境

- Cisco Secure AccessとZTNAの導入
- Identity ProviderとしてのMicrosoft Entra ID（以前のAzure AD）
- 個人のGoogleアカウント(@gmail.com)がEntra IDにゲストユーザとして登録されている
- ゲストアカウントのプロビジョニングとセキュアアクセスでの表示
- Entra IDとCisco Secure Access間で設定されるSAML認証

解決策

登録エラーは、Microsoft Entra IDのSAML属性マッピング構成を変更することで解決されました。この問題に対処するために、次の手順が実行されました。

ステップ1:DARTバンドルとクライアントの動作を分析する

DARTバンドルをレビューして、Cisco Secure ClientおよびZTAコンポーネントが正常に動作していることを確認します。分析では、登録フローがCisco Secure Accessに正常に到達していること、およびアイデンティティプロバイダーとのSAML認証中に障害が発生していることを確認する必要があります。

手順2:Enter ID認証ログを調べる

Entra ID認証ログを調べて、認証プロセスがアイデンティティプロバイダーの観点から正常に完了することを確認します。ログには認証の成功が表示されますが、属性の不一致によりセキュアアクセスでログインが拒否されます。

手順3:SAML属性マッピングの問題を特定する

Entra IDがSAML要求としてUPN（ユーザプリンシパル名）を発行していることを確認します。このUPNは、セキュアアクセスで想定される個人のGmailアカウントIDと一致しません。アサートされたIdP属性が、予期されたユーザーIDに対応していません。

手順4:SAML属性マッピングを変更する

Microsoft Entra IDのSAML属性マッピングをUPNからEmail Addressに変更します。これにより、電子メールアドレスの請求がGoogleアカウントの個人IDと一致します。

ステップ5：登録の成功の確認

属性マッピングの変更を実装した後、ZTNA登録プロセスを再試行します。これで、Cisco Secure Access ZTAがGmailアドレスを認識し、登録が正常に完了することを許可するようになったはずです。

原因

登録エラーは、Microsoft Entra IDによってアサートされているSAML属性とCisco Secure Accessの予期されるユーザIDの不一致が原因で発生しました。Entra IDは、SAML要求としてUPN（ユーザプリンシパル名）を送信するように設定されていますが、個人用Googleアカウント(@gmail.com)の場合、このUPNは実際の電子メールアドレスIDに対応していませんでした。Cisco Secure Accessは、プロビジョニングされたゲストユーザアカウントと照合するための識別属性として電子メールアドレスを受信する必要があり、IdP認証に成功しても認証が拒否される結果となっていました。

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。