Secure AccessブラウザベースのSAML認証のトラブルシューティングでEnterID付きの空白の白い画面が表示される

内容

問題

Cisco Secure Clientがインストールされていないデバイスで、ブラウザベースのSAML認証を強制するようにCisco Secure Accessを設定すると、認証プロセスは、EntraID認証ページを表示する代わりに、空白の白画面にリダイレクトされます。この問題は、特にMicrosoft Edgeの通常（非InPrivate）モードおよびGoogle Chromeブラウザで発生します。認証は、Edge InPrivateモードを使用している場合に正しく動作します。SAML認証プロファイルでは、復号化とSSO認証の両方が有効になっています。

設定されたポリシー構造には、次のものが含まれます。

- 認証後のユーザにポリシーを許可します。（送信元：any user、宛先：any）
- SAML認証プロファイルでSAML認証ポリシーを許可します。（送信元：エンドポイントIP、宛先：0.0.0.0 TCP 80,443）
- SAML認証プロファイルでSAML認証ヘルパーポリシーを許可します。（送信元：エンドポイントIP、宛先：任意）
- ブロックポリシー。（送信元：エンドポイントIP、宛先：任意）

環境

- Cisco Secure Access（インターネットアクセスモジュール）
- アイデンティティプロバイダー(IdP)としてIDを入力
- Cisco Secure Clientを使用しないデバイス用のブラウザベースのSAML認証

- 復号化とSSO認証が有効なSAML認証プロファイル
- Microsoft EdgeおよびGoogle Chromeブラウザ

解決方法

この問題を解決するには、SAML認証プロファイル設定の復号化除外リストに特定のEntraID関連ドメインを追加します。これにより、SSL/TLS復号化プロセスがEntraID認証フローに干渉しなくなります。

手順1：暗号化解除除外リストにEntraIDドメインを追加する

SAML認証プロファイルの復号化除外リストで、次の4つのEntraIDドメインを設定します。

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

手順2:SAMLポリシーへの設定の適用

復号化の除外設定が両方に適用されていることを確認します。

- Allow SAML authenticationポリシー。（送信元：エンドポイントIP、宛先：0.0.0.0 TCP 80,443）
- Allow SAML authenticationヘルパーポリシー。（送信元：エンドポイントIP、宛先：任意）

ステップ3：解決策の確認

復号化の除外設定を適用した後、認証フローをテストします。

- Microsoft Edge（通常モード）: EntraID認証ページに正常にリダイレクトできます。
- Google Chrome:EntraID認証ページに正常にリダイレクトできます。
- どちらのブラウザでも、EntraID認証入力画面を一貫して表示できます。

原因

空白の白い画面が表示されるのは、SAML認証プロファイルで復号化が有効な場合、Cisco Secure AccessのSSL/TLS復号化プロセスがEntraID認証フローを妨げるためです。復号化プロセスでは、ブラウザとEntraID認証サーバの間のセキュアな通信が切断され、認証ページが適切にロードされなくなります。InPrivateモードは、復号化干渉をバイパスしてSSL/TLSセッションを異なる方法で処理するため、機能します。EntraIDドメインを復号化除外リストに追加すると、認証トラフィックは復号化されずに通過でき、セキュアな認証フローの整合性が維持されます。

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。