セキュアアクセスのためのSWG SAML認証Cookie代理問題のトラブルシューティング

内容

問題

Cisco Secure Access経由でWebアプリケーションにアクセスするユーザは、アプリケーションがドメイン間のリダイレクトを実行したり、複数の関連ドメインからリソースを取得したりするときに認証エラーが発生します。この問題は次のように現れます。

- SAML認証後にWebアプリケーションを正しく初期化できない。
- ドメイン間リソースへの要求（CORSエラー）は、既定の拒否ルールによってブロックされています。
- 認証されたユーザーIDではなく、ネットワークまたはトンネルIDに属する要求を示すアクティビティログ。
- リダイレクトされた要求のブラウザコンソールにCORSポリシーエラーが表示される。
- IPサロゲートを使用する場合は物理マシン上でアプリケーションが正しく動作するが、Cookieサロゲートを使用するCitrix仮想デスクトップ環境では失敗する。

この問題は、特に、Cookieサロゲート認証が仮想化環境で使用され、ドメイン間のリソースのフェッチ中にリダイレクトされた要求がユーザからCookieへのマッピングを失う場合に発生します。

環境

- SAML認証が設定されたCisco Secure Access
- Citrix仮想デスクトップ環境でCookie Surrogate認証を有効にする
- 物理マシンで使用されるIPサロゲート認証

- クロスドメインリダイレクトを実行するWebアプリケーション（Web開発者ツールのコンソールログのCORSエラー）
- 物理および仮想デスクトップインフラストラクチャの混在環境

解決方法

この問題は、影響を受けるネットワーク範囲にIPサロゲートバイパスを実装して、ドメイン間のリダイレクト中でも適切なユーザIDの帰属を可能にすることで解決されます。

ステップ1:IPサロゲート設定に移動します。

Cisco Secure Accessダッシュボードにアクセスし、Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogateの順に選択します。

ステップ2：内部ネットワークバイパスの有効化

影響を受けるネットワーク範囲を内部ネットワークバイパス設定に追加します。これにより、システムはこれらのネットワークから発信された要求のユーザID属性を維持できます。

ステップ3：アプリケーションアクセスのテスト

IPサロゲートの実装後、影響を受けるアプリケーションをテストして、次のことを確認します。

- クロスドメインリソース要求は、ユーザーIDに正しく関連付けられます
- アプリケーションはCORSエラーなしで正常に初期化されました
- アクティビティログには、すべての要求について、ネットワークまたはトンネルベースのIDではなく、ユーザIDが表示されます

ステップ5：アクティビティレポートのモニタ

Monitor > Activity Searchを使用して、要求が、ネットワークまたはトンネルベースのIDとして表示されるのではなく、認証されたユーザに正しく帰属していることを確認します。

原因

この動作は、SAML認証の性質と、仮想環境でのCookie Surrogateとの組み合わせにより発生します。Webアプリケーションがクロスドメインのリダイレクトを実行したり、複数の関連ドメインからリソースを取得したりする場合、リダイレクトされた要求では、Cisco Secure Accessが認証済みユーザセッションに関連付けできるようにサロゲートCookieが搬送されない可能性があります。

根本的な原因は次のとおりです。

- クッキーのサロゲートは、リダイレクト全体でのブラウザのクッキーの伝播に依存します。
- ドメイン間セキュリティポリシー(CORS)は、307/リダイレクトのシナリオでCookieを削除できます。
- ブラウザのセキュリティ対策により、異なるドメイン間でのCookieの共有が防止されます。
- 仮想デスクトップ環境では、物理マシンとは異なる方法でクッキーの伝播が処理されます。

ユーザとcookieのマッピングが失われると、セキュアアクセスは認証されたユーザに要求を解決できず、その要求はソースとして登録されたネットワークまたは異なるIDのみに属することになり、デフォルトの拒否ルールによってブロックされます。

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。