VPNaaS SAML認証がDuo IdPを使用して"；リレー状態の復号化に失敗"；エラーで失敗する

内容

お問い合わせ内容

SAML認証を使用し、アイデンティティプロバイダー(IdP)としてDuoを使用するセキュアクライアントリモートアクセス(SCA)を使用してVPNaaS接続を確立しようとすると、次のエラーが発生します。

- SSO認証要求を処理できませんでした。システム管理者に問い合わせてください
- Relaystateの復号化に失敗しました

同じIdPおよびDuo設定を使用した認証は、ZTNA(Zero Trust Network Access)では正常に機能しますが、VPN接続では失敗します。 Duoでは、ZTNAおよびVPN用に2つの異なるアプリケーションが設定されており、どちらも同じIdPを使用します。

環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）
- サブテクノロジー：セキュアアクセス – セキュアクライアントリモートアクセス（VPN、ポスチャ、プライベートリソース）
- 認証方法：Duo IdPを使用したSAML
- 2つのDuoアプリケーションを構成：1つはZTNA、もう1つはVPN
- 認証はZTNAで動作し、VPNでは失敗する
- ソフトウェアバージョン：すべて
- 最近のハードウェア/ソフトウェアバージョンの変更は指定されていません

解決策

この問題は、VPN用Duoアプリケーションのエンティティ ID(VID)とアサーションコンシューマサービス(ACS)URLの設定を修正することで解決しました。 正しいメタデータがSecure Accessからダウンロードされ、VPN Duoアプリケーションにアップロードされたため、SAMLリレー状態の復号エラーが解決されました。

1. CSAダッシュボードにログインします。 Connect > Enduser Connectivity -> Virtual Private Networksの順に選択します。 接続しているプロファイルを確認します。
2. そのプロファイルをクリックして、編集します。 Authentication タブに移動します。
3. セキュアアクセス用のSAMLメタデータをダウンロードします。
4. entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml"および <AssertionConsumerService index="0" isDefault="true"

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionC
認します

5. entityIDおよびAssertionConsumerServiceが、VPN SSO認証用に設定されたDuoアプリケーションに一致していることを確認します。

原因

Duo VPNアプリケーションでエンティティIDとACS URLが正しく設定されていないため、SAMLリレー状態の暗号化解除に失敗しました。ZTNA認証が同じIdPで動作しているにもかかわらず、Duo for VPNに正しい設定が存在しませんでした。Secure Accessの正確なメタデータを使用してDuo VPNアプリケーションを更新することで、問題が解決しました。

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。