SAML認証およびBencodeディクショナリエラーによるCisco Secure Client VPN接続の失敗

内容

お問い合わせ内容

Google IdPでSAML認証を使用すると、Cisco Secure Clientを使用したVPN接続を確立できません。SAML認証はIdP側で成功しますが、認証後の処理でクライアントに障害が発生し、切断状態に移行するため、VPNトンネルの作成ができなくなります。

環境

- Cisco Secure Clientバージョン5.1.13.177
- Google IdPで設定されたSAML認証
- 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)
- Google IdP認証ログにSAML認証の成功が表示される

解決策

この問題は、Cisco Secure Clientを再インストールすることで解決しました。次のトラブルシューティングアプローチが文書化されました。

初期診断ステップ

ステップ1：影響を受けるエンドポイントからDARTログを収集します (https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html

DARTバンドルの抽出> Cisco Secure Client > Anyconnect VPN > Logs > VPN Folder > AnyConnectVPN.txt – 内部設定の読み取り中に次のエラーが表示され、次のエラーが継続的に表示されます。

- Bencodeディクショナリの内部化に失敗しました
- Bencodeディクショナリを作成できませんでした
- PHONEHOMEVPN_ERROR_UNEXPECTED（予期しない電話）
- GLOBAL_ERROR_予期しないエラー

手順2:IdP側でSAML認証のステータスを確認します

問題をクライアント側の認証後処理に切り分けるために、Google IdPログにSAML認証の成功が示されていることを確認します。

解決の実装

ステップ1:Cisco Secure Clientを再インストールする

既存のCisco Secure Clientインストールをアンインストールし、クライアントソフトウェアのクリーンな再インストールを実行します。

ステップ2:VPN接続の復元を確認します。

再インストール後、SAML認証を使用してVPN接続をテストし、接続が正常に確立されてトンネルが適切に作成されたことを確認します。

Cisco Secure Clientを再インストールすると、VPN機能が復元され、SAML認証とトンネル確立が成功しました。

原因

根本原因は、Cisco Secure Clientのインストール内の内部設定データの破損に関連していると考えられます。特に、認証後の処理でBencodeディクショナリ(BID)データを処理するCPhoneHomeVpn/PhoneHomeAgentコンポーネントの機能に影響します。繰り返される「Bencode dictionary interalize failed」および「Failed to create Bencode dictionary」エラーは、SAML認証が成功した後のVPNトンネルの確立に必要な内部設定データを、クライアントが適切に解析または処理できなかったことを示しています。

この問題はクライアントの再インストールによって解決されました。これは、問題がサーバ側の設定やIdP統合の問題ではなく、クライアント側のデータの破損に関連していることを示しています。

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。