Secure ClientでのSecure Access Domain Bypassの検証

お問い合わせ内容

Cisco Secure Accessを使用している組織では、多くの場合、バイパスドメインを設定して、特定のWebサイト、アプリケーション、またはサービスがSecure Accessに送信されたり、Secure Web Gatewayによって処理されることなく、インターネットに直接接続できるようにしています。 これらのバイパスルールは、Secure Accessダッシュボードで正しく設定されているように見えますが、管理者は、Cisco Secure Clientエンドポイントでバイパスポリシーが実際に適用および適用されているかどうかを確認するという課題に頻繁に直面します。

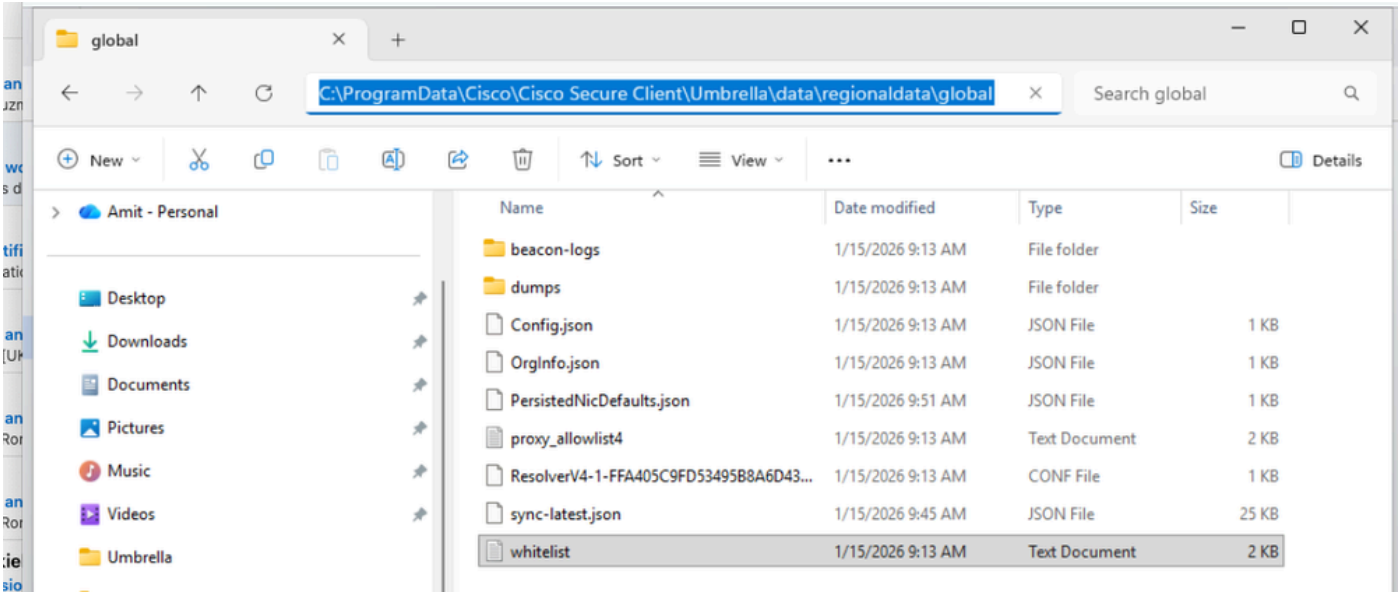
環境

- Cisco Secure Access with Roamingセキュリティモジュールとドメインバイパス

解決策

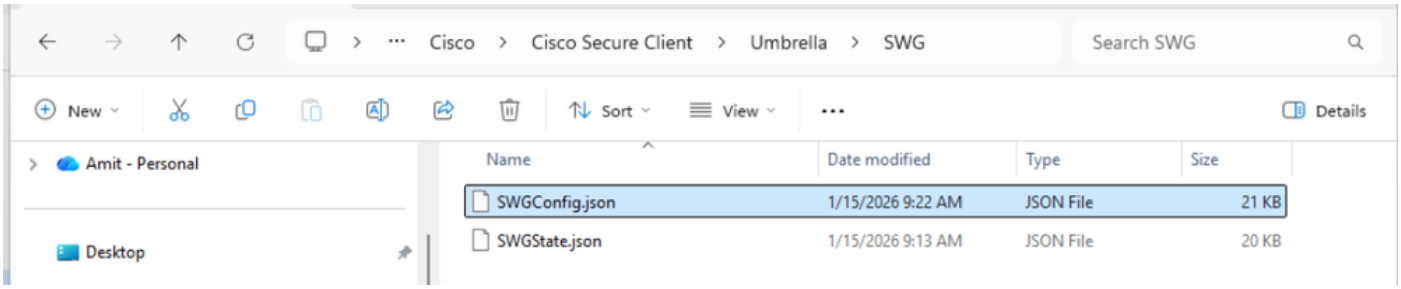
ドメインを次のように設定します。

- セキュアアクセスをバイパスし、設定をallowlist.txtファイルのC: > Program Data > Cisco > Cisco Secure Client > Umbrella > Data > Regional Data > Global Folderの下のクライアントにプッシュします。



inline_image_0.png (インラインイメージ_0.png)

- SWGをバイパスし、設定をSWGConfig.jsonファイルのC: > Program Data > Cisco > Cisco Secure Client > Umbrella > SWGの下のクライアントにプッシュします。



inline_image_1.pngファイル

注：クライアントとクラウド間の同期タイマーは約25分ですが、これを上書きする場合はUmbrellaサービスを再起動できます。

原因

この問題の根本的な原因は、ユーザがSWGバイパスの誤ったファイルをチェックしたことです。

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。