セキュアアクセス証明書のインポート後のMacOSインターネットアクセスの問題

内容

お問い合わせ内容

MacOSユーザは、ポータルからインターネット証明書をインポートした後、Cisco Secure Accessを介してインターネットリソースにアクセスできません。

影響を受けるサービスは次のとおりです。

- Microsoft Outlook（送受信機能）
- Google.com
- AIウェブサイト
- その他のWeb宛先

同じ設定を持つWindowsユーザは影響を受けず、正常に機能し続けます。この問題は、証明書のインポート後にMacOSクライアントが電子メールにアクセスしたり、一般的なインターネットブラウジング機能を使用したりした場合に、特に影響を及ぼします。

環境

- Cisco Secure Access with Unified Policyの設定
- Cisco Secure Accessポータルからインターネット証明書がインポートされたMacOSクライアント
- 同じ構成のWindowsクライアント（影響なし）
- 使用中のインターネットポリシー、プライベートポリシー、DLPポリシー、RBI、およびセキュリティプロファイル

- MacOSとWindowsの動作が異なるオペレーティングシステム混在環境

解決策

この問題を解決するには、特定のMicrosoft Outlookエンドポイントとアプリケーションをを Do Not Decrypt(DND)リストに追加して、これらのサービスのSSLインスペクションをバイパスします。

手順1: Outlookエンドポイントを DNDリストに追加する

Outlookのアクセス問題を解決するには、次のセクションで説明するエンドポイントまたはアプリケーションをDo Not Decrypt (DND)構成に追加します。

```
outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
smtp.office365.com
```

ステップ2：解決の検証

Outlook関連のエンドポイントをDNDリストに追加した後、影響を受けるMacOSクライアントがアクセスできることを確認します。

- Microsoft Outlookの送受信機能
- 以前に影響を受けたその他のインターネットリソース

ユーザは、これらのDNDエントリを実装した後も、Outlookアプリケーションが MacOSデバイスで正常に機能し続けることを確認しました。

原因

この問題は、MacOSクライアントがインターネットリソース（特にMicrosoft Outlookサービス）へのセキュアな接続を確立する機能を妨げるSSL/TLS暗号化インスペクションが原因で発生しました。暗号化インスペクションプロセスによって、特にMacOSプラットフォームでの証明書の検証や接続の確立が適切に行えなくなっているのに対し、Windowsクライアントは同じインスペクションポリシーの影響を受けませんでした。影響を受けるエンドポイントをDo Not Decryptリストに追加すると、これらの特定のサービスのインスペクションがバイパスされ、通常の接続を再開できるようになります。

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。