

セキュアアクセスエラーのトラブルシューティング"TLSエラー：268435703:SSLルーチン：OPENSSL_internal:WRONG_VERSION_NUMBER"

内容

[はじめに](#)

[問題](#)

[解決方法](#)

[その他の詳細事項](#)

[関連情報](#)

はじめに

このドキュメントでは、セキュアアクセスエラー「TLS error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER」を解決する方法について説明します。

問題

ユーザがブラウザベースのゼロトラストアクセスを使用して、リソースのパブリックURL(たとえば、https://<app-name>.ztna.sse.cisco.io)を使用してプライベートリソースを開こうとすると、アプリケーションがブラウザにロードされず、エラーが表示されます。

アプリケーションに到達できません

管理者にお問い合わせください

ヘッダーの前にアップストリーム接続エラーまたは切断/リセットが発生しました。リセット理由：
：接続エラー、トランスポート障害の理由：TLSエラー：268435703:SSLルーチン
：OPENSSL_internal:WRONG_VERSION_NUMBER

Cisco Secure Access



Application is unreachable

Please contact your administrator

upstream connect error or disconnect/reset before headers. reset reason: connection failure, transport failure reason: TLS error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER

Secure Clientエラー

解決方法

Private ResourceセクションのEndpoint Connection Methodで、適切なプロトコルを設定していることを確認します。

- プライベートアプリケーションをHTTPでのみ使用できる場合は、HTTPを選択する必要があります。
- プライベートアプリケーションがHTTPでのみ使用できる場合は、HTTPを選択する必要があります。
- プライベートアプリケーションがHTTPまたはHTTP経由で使用できる場合、このエラーは発生しません。

Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not

Public URL for this resource ⓘ

https://

Protocol [Server Name Indication \(SNI\) \(optional\)](#) ⓘ

Validate Application Certificate ⓘ

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

プライベートリソースの設定

その他の詳細事項

Secure Accessプロキシエンジンは、ダッシュボードで指定されているプロトコルを使用して、プライベートリソースへの接続を確立しようとします。

(どちらかの側の設定ミスが原因で) プロキシがプライベートアプリケーションとのHTTPSチャンネルを確立できない場合、ブラウザベースの接続を介してプライベートリソースにアクセスしようとすると、ブラウザにOpenSSL関連のエラーが表示される可能性があります。

関連情報

- [セキュアアクセスユーザガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

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。