

Dépannage de l'erreur d'accès sécurisé "Erreur TLS: 268435703:Routages SSL:OPENSSL_internal:WRONG_VERSION_NUMB

Table des matières

[Introduction](#)

[Problème](#)

[Solution](#)

[Détails supplémentaires](#)

[Informations connexes](#)

Introduction

Ce document décrit une façon de résoudre l'erreur d'accès sécurisé : "TLS error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER".

Problème

Lorsqu'un utilisateur tente d'ouvrir une ressource privée à l'aide de l'accès sans confiance basé sur un navigateur, à l'aide de l'URL publique de la ressource (par exemple <https://<nom-app>.ztna.sse.cisco.io>), l'application ne se charge pas dans le navigateur et l'erreur s'affiche :

Application inaccessible

Veillez contacter votre administrateur

erreur de connexion en amont ou déconnexion/réinitialisation avant les en-têtes. motif de la réinitialisation : échec de la connexion, motif de l'échec du transport : erreur TLS : 268435703 : routines SSL : 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

Erreur du client sécurisé

Solution

Assurez-vous de configurer un protocole approprié sous la méthode de connexion de point de terminaison dans la section de ressource privée :

- Si l'application privée n'est disponible que sur HTTP, vous devez sélectionner HTTP.
- Si l'application privée est disponible uniquement sur HTTPS, vous devez sélectionner HTTPS.
- Si l'application privée est disponible sur HTTP ou HTTPS, cette erreur ne doit jamais être vue.

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.

Configuration des ressources privées

Détails supplémentaires

Le moteur proxy d'accès sécurisé tente d'établir une connexion à la ressource privée à l'aide du protocole spécifié dans le tableau de bord.

Si le proxy ne parvient pas à établir un canal HTTP avec l'application privée (en raison d'une mauvaise configuration de chaque côté), vous pouvez voir des erreurs liées à OpenSSL dans le navigateur lors de la tentative d'accès aux ressources privées via la connexion basée sur le navigateur.

Informations connexes

- [Guide de l'utilisateur Secure Access](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.