

Risoluzione dei problemi relativi all'errore di accesso sicuro "Errore TLS: 268435703:SSL routine:OPENSSL_internal:WRONG_VERSION_NUM"

Sommario

[Introduzione](#)

[Problema](#)

[Soluzione](#)

[Ulteriori dettagli](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere l'errore Secure Access: "TLS error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER".

Problema

Quando un utente tenta di aprire una risorsa privata utilizzando un accesso con attendibilità totale basato su browser, utilizzando l'URL pubblico per la risorsa (ad esempio <https://<nome-app>.ztna.sse.cisco.io>), l'applicazione non viene caricata nel browser e viene visualizzato l'errore:

Impossibile raggiungere l'applicazione

Contattare l'amministratore

errore di connessione a monte o disconnessione/reimpostazione prima delle intestazioni. motivo reimpostazione: errore di connessione, errore di trasporto. motivo: errore TLS: 268435703: routine 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

Errore client protetto

Soluzione

Verificare di aver configurato un protocollo corretto in Metodo connessione endpoint nella sezione Risorsa privata:

- Se l'applicazione privata è disponibile solo su HTTP, è necessario selezionare HTTP.
- Se l'applicazione privata è disponibile solo su HTTPS, è necessario selezionare HTTPS.
- Se l'applicazione privata è disponibile tramite HTTP o HTTPS, questo errore non deve mai essere visualizzato.

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.

Configurazione risorse private

Ulteriori dettagli

Il motore proxy di accesso sicuro tenta di stabilire una connessione alla risorsa privata utilizzando il protocollo specificato nel dashboard.

Se il proxy non è in grado di stabilire il canale HTTP con l'applicazione privata (a causa di una configurazione errata su entrambi i lati), è possibile visualizzare gli errori relativi a OpenSSL nel browser quando si cerca di accedere alle risorse private tramite la connessione basata su browser.

Informazioni correlate

- [Guida per l'utente di Secure Access](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).