

Solucionar problemas de erro de acesso seguro

"Erro TLS: 268435703:rotinas

SSL:OPENSSL_internal:WRONG_VERSION_NUMB

Contents

[Introdução](#)

[Problema](#)

[Solução](#)

[Detalhes adicionais](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve uma forma de resolver o erro de Acesso Seguro: "Erro TLS: 268435703:SSL rotinas:OPENSSL_internal:WRONG_VERSION_NUMBER".

Problema

Quando um usuário tenta abrir um recurso privado usando o acesso de confiança zero baseado em navegador, usando a URL pública do recurso (por exemplo, <https://<nome-do-aplicativo>.ztna.sse.cisco.io>), o aplicativo não é carregado no navegador e o erro é visto:

Aplicativo inacessível

Entre em contato com o administrador

erro de conexão de upstream ou desconexão/redefinição antes dos cabeçalhos. motivo da redefinição: falha de conexão, motivo da falha de transporte: erro TLS: 268435703:rotinas 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

Erro de Cliente Seguro

Solução

Certifique-se de configurar um protocolo apropriado sob o Método de conexão de ponto final na seção Recurso privado:

- Se a aplicação privada estiver disponível somente em HTTP, você deverá selecionar HTTP.
- Se a aplicação privada estiver disponível somente em HTTPs, você deverá selecionar HTTPs.
- Se o aplicativo privado estiver disponível por HTTP ou HTTPs, esse erro nunca deverá ser visto.

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.

Configuração de recurso privado

Detalhes adicionais

O mecanismo de proxy de Acesso Seguro tenta estabelecer uma conexão com o Recurso Privado usando o Protocolo especificado no painel.

Se o proxy não conseguir estabelecer um canal HTTPs com o aplicativo privado (devido a uma configuração incorreta em ambos os lados), você poderá ver erros relacionados ao OpenSSL no navegador ao tentar acessar Recursos Privados através da conexão baseada no Navegador.

Informações Relacionadas

- [Guia do usuário do Secure Access](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.