

ZTNA Client - Erro de interceptador de rede

Contents

Problema

Usuários com erros de interceptador de rede ao tentar acessar recursos privados por meio do Cisco Secure Access Zero Trust Access (ZTNA). O erro impede a conexão bem-sucedida com qualquer recurso privado configurado no ambiente de acesso com confiança zero, resultando na perda total de acesso a aplicativos e serviços internos.

Ambiente

- Tecnologia: Cisco Secure Access - Acesso de Confiança Zero (ZTNA)
- Versão de software: 5.1.14
- Linha de produtos: SECACCS
- Tipo de erro: Erro do interceptador de rede
- Impacto: Crítico - Perda total de acesso a recursos privados
- Alterações recentes: Nenhum relatado

Resolução

Isso pode ser visto nos registros do Dart:

++ Os seguintes logs foram encontrados:

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() IZtnaApi::SetParameters falhou com o código de erro=BadParameter

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ ZtnaConfigEnforcer.cpp:444 ZtnaConfigEnforcer::applyActiveSteeringPolicy() falhou ao iniciar/atualizar interceptação ZTNA

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] I/ ZtnaConfigEnforcer.cpp:145 ZtnaConfigEnforcer::reportInterceptorConnectivityChange() Relatando acessibilidade KDF: ConfigFailed

na configuração em cache do DART

Um espaço em branco à direita é introduzido - cisco.com - causando esse problema.

- Depois de mais testes, ficou evidente que selecionar a opção de endereço alcançável remotamente para configuração de recursos privados e o campo de endereço acessível remotamente permanece inalterado ou tem os mesmos valores que o endereço acessível

internamente, essa configuração se desabilita automaticamente ao salvar.

- No entanto, parece que quando o campo de endereço acessível remotamente foi verificado, havia um espaço em branco extra no FQDN do endereço acessível remotamente (por exemplo, 'cisco.com' versus 'cisco.com') e a configuração pôde ser salva.
- Como o perfil padrão zero-trust estava em uso, o que significa que qualquer configuração de recurso particular recém-criada ou existente é enviada por push para cada usuário na organização, a configuração com esse espaço em branco foi sincronizada. Esse espaço em branco causou os erros de "Interceptor de Rede" que o cliente estava exibindo.
- Para solucionar esse problema por enquanto, acesse os recursos privados e verifique se não há espaços em branco no FQDN do endereço alcançável remotamente.

Causa

O erro do interceptador de rede no Cisco Secure Access Zero Trust Access é normalmente causado por definições de recursos privados problemáticos ou mal configuradas dentro do ambiente ZTNA. Quando o campo de endereço acessível remotamente foi verificado, havia um espaço em branco extra no FQDN do endereço acessível remotamente (por exemplo, 'cisco.com' versus 'cisco.com').

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

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.