

Client ZTNA - Errore intercettore di rete

Sommario

Problema

Utenti che riscontrano errori dell'intercettore di rete durante il tentativo di accedere a risorse private tramite Cisco Secure Access Zero Trust Access (ZTNA). L'errore impedisce la corretta connessione alle risorse private configurate nell'ambiente di accesso con attendibilità zero, con conseguente perdita completa dell'accesso alle applicazioni e ai servizi interni.

Ambiente

- Tecnologia: Cisco Secure Access - Zero Trust Access (ZTNA)
- Versione del software: 5.1.14
- Famiglia di prodotti: SECACS
- Tipo di errore: Errore intercettore di rete
- Conseguenze: Critica: perdita completa dell'accesso alle risorse private
- Modifiche recenti: Nessun report

Risoluzione

Questa condizione può essere rilevata nei registri Dart:

++ Sono stati trovati i seguenti log:

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() I/ZtnaApi::SetParameters non riuscito con error code=BadParameter

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ ZtnaConfigEnforcer.cpp:444 ZtnaConfigEnforcer::applyActiveSteeringPolicy() non è riuscito ad avviare/aggiornare l'intercetta ZTNA

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

nella configurazione memorizzata nella cache da DART

Il problema è causato da uno spazio vuoto finale -cisco.com.

- Dopo ulteriori test, è risultato evidente che la selezione dell'opzione relativa all'indirizzo raggiungibile in remoto per la configurazione delle risorse private e del campo dell'indirizzo raggiungibile in remoto non è stata modificata o ha gli stessi valori dell'indirizzo raggiungibile

internamente. Questa impostazione si disattiva al momento del salvataggio.

- Tuttavia, quando è stato controllato il campo dell'indirizzo raggiungibile in remoto, nell'FQDN dell'indirizzo raggiungibile in remoto era presente uno spazio vuoto aggiuntivo (ad esempio, 'cisco.com' anziché 'cisco.com') ed è stato possibile salvare la configurazione.
- Poiché il profilo di attendibilità zero predefinito è in uso, il che significa che qualsiasi configurazione di risorse private appena creata o esistente viene estesa a ogni utente dell'organizzazione, la configurazione con questo spazio vuoto è stata sincronizzata. Questo spazio vuoto ha causato gli errori di "Network Interceptor" che il client stava mostrando.
- Per risolvere il problema, accedere alle risorse private e verificare che gli spazi vuoti non siano presenti nell'FQDN dell'indirizzo raggiungibile in remoto.

Causa

L'errore dell'intercettore di rete in Cisco Secure Access Zero Trust Access è in genere causato da definizioni di risorse private non configurate o problematiche nell'ambiente ZTNA. Quando è stato selezionato il campo dell'indirizzo raggiungibile in remoto, nell'FQDN dell'indirizzo raggiungibile in remoto era presente uno spazio vuoto aggiuntivo (ad esempio, 'cisco.com' anziché 'cisco.com').

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

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).