ZTNA-client - Fout netwerkinterceptor

Inhoud

uitgeven

Gebruikers die netwerkonderscheppingsfouten ervaren wanneer ze proberen toegang te krijgen tot privébronnen via Cisco Secure Access Zero Trust Access (ZTNA). De fout voorkomt een succesvolle verbinding met privébronnen die zijn geconfigureerd in de Zero Trust Access-omgeving, waardoor de toegang tot interne toepassingen en services volledig verloren gaat.

milieu

- Cisco Secure Access - Zero Trust Access (ZTNA)
- Softwareversie: 5.1.14
- Productfamilie: SECACS
- Fouttype: netwerkinterceptorfout
- Impact: kritiek - volledig verlies van toegang tot privébronnen
- Recente wijzigingen: geen gemeld

resolutie

Dit is te zien in de Dart-logs:

++ De volgende logs zijn gevonden:

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() IZtnaApi::SetParameters mislukt met foutcode=BadParameter

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ ZtnaConfigEnforcer.cpp:444 ZtnaConfigEnforcer::applyActiveSteeringPolicy() kan ZTNA-interceptie niet starten/bijwerken

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

in de Cached-configuratie van DART

Een achterblijvende witte ruimte wordt geïntroduceerd - cisco.com - waardoor dit probleem wordt veroorzaakt.

- Na verdere tests werd het duidelijk dat het selecteren van de optie voor extern bereikbaar adres voor configuratie van privébronnen en het veld voor extern bereikbaar adres

ongewijzigd is of dezelfde waarden heeft als het intern bereikbare adres, deze instelling schakelt zichzelf uit bij opslaan.
- Het lijkt er echter op dat toen het veld Extern bereikbaar adres werd gecontroleerd, er een extra witruimte was in het Extern bereikbaar adres FQDN (bijvoorbeeld 'cisco.com' versus 'cisco.com'), en de configuratie kon worden opgeslagen.
- Aangezien het standaard zero-trust-profiel in gebruik was, wat betekent dat elke nieuw gemaakte of bestaande configuratie van privébronnen naar beneden wordt geduwd naar elke gebruiker in de organisatie, werd de configuratie met deze witruimte gesynchroniseerd. Deze witruimte veroorzaakte de "Network Interceptor"-fouten die de client vertoonde.
- Om dit probleem voorlopig op te lossen, gaat u naar de privébronnen en zorgt u ervoor dat witruimten niet aanwezig zijn in het op afstand bereikbare adres FQDN.

Oorzaak

De netwerkinterceptorfout in Cisco Secure Access Zero Trust Access wordt meestal veroorzaakt door verkeerd geconfigureerde of problematische definities van privébronnen in de ZTNA-omgeving. Toen het veld Extern bereikbaar adres werd aangevinkt, was er een extra witruimte in het Extern bereikbaar adres FQDN (bijvoorbeeld 'cisco.com' versus 'cisco.com').

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.