

Cliente ZTNA - Error del interceptor de red

Contenido

Problema

Usuarios que sufren errores de interceptor de red al intentar acceder a recursos privados a través de Cisco Secure Access Zero Trust Access (ZTNA). El error impide una conexión correcta a cualquier recurso privado configurado en el entorno de acceso de confianza cero, lo que provoca una pérdida total del acceso a las aplicaciones y los servicios internos.

Entorno

- Tecnología: Cisco Secure Access: acceso de confianza cero (ZTNA)
- Versión del software: 5.1.14
- Familia de productos: SECACCS
- Tipo de error: Error de interceptor de red
- Impacto: Crítico: completa pérdida de acceso a recursos privados
- Cambios recientes: Ninguno notificado

Resolución

Esto se puede ver en los registros de Dart:

++ Se han encontrado los siguientes registros:

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() I/ZtnaApi::SetParameters failed with error code=BadParameter

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ZtnaConfigEnforcer.cpp:444 ZtnaConfigEnforcer::applyActiveSteeringPolicy() no pudo iniciar/actualizar la intercepción ZTNA

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

en la configuración en caché desde DART

Se introduce un espacio en blanco a la derecha, cisco.com, que causa este problema.

- Después de realizar pruebas adicionales, se hizo evidente que al seleccionar la opción de dirección de acceso remoto para la configuración de recursos privados y el campo de dirección de acceso remoto no se modifica o tiene los mismos valores que la dirección de

acceso interno, esta configuración se deshabilita al guardar.

- Sin embargo, parece que cuando se verificó el campo de dirección alcanzable remotamente, había un espacio en blanco adicional en el FQDN de la dirección alcanzable remotamente (por ejemplo, 'cisco.com' frente a 'cisco.com '), y la configuración se pudo guardar.
- Como el perfil predeterminado de confianza cero estaba en uso, lo que significa que cualquier configuración de recursos privados nueva o existente se envía a todos los usuarios de la organización, se sincronizó la configuración con este espacio en blanco. Este espacio en blanco causó los errores de "interceptor de red" que el cliente mostraba.
- Para solucionar este problema por el momento, vaya a los recursos privados y asegúrese de que los espacios en blanco no estén presentes en el FQDN de la dirección de acceso remoto.

Causa

El error de interceptor de red en Cisco Secure Access Zero Trust Access se debe normalmente a definiciones de recursos privados mal configuradas o problemáticas dentro del entorno ZTNA. Cuando se verificó el campo de dirección de acceso remoto, había un espacio en blanco adicional en el FQDN de la dirección de acceso remoto (por ejemplo, 'cisco.com' frente a 'cisco.com ').

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).