

# Échec de la connexion TLS de ressource privée basée sur le navigateur ZTA

## Table des matières

---

## Problème

Les utilisateurs ne peuvent pas accéder à une ressource privée basée sur un navigateur via Cisco Secure Access.

Lorsque vous tentez de vous connecter, les symptômes suivants se produisent :

- La connexion TCP en trois étapes s'effectue correctement, mais la négociation TLS échoue après le Hello du client.
- La connexion à l'URL mappée SSE publique (<https://example-orgid.ztna.sse.cisco.io>) atteint l'authentification Cisco mais renvoie une erreur HTTP 404.
- Après avoir ajouté le nom de domaine complet à la configuration de la ressource privée, le trafic est redirigé vers l'invite d'authentification, mais une page vide apparaît après l'authentification.
- Les fichiers HAR affichent des réponses HTTP 200, mais la connexion TLS ne se termine pas.
- Motif du blocage : "Accès privé : les données de posture récupérées pour le périphérique sont trop anciennes/doivent être actualisées ».

## Environnement

- Accès sécurisé Cisco (SSE)
- ID d'organisation d'accès sécurisé : xxxx
- ZTNA (Zero Trust Network Access) basé sur un navigateur

- Ressource privée : example.net
- Ressource privée active pour comparaison : abc.net
- Configuration de certificat générique

## Résolution

Le problème a été résolu en configurant la ressource privée pour qu'elle utilise la même configuration de certificat qu'une ressource privée opérationnelle.

Les étapes décrites dans les sections suivantes ont été suivies.

### Étape 1: Analyser la configuration de travail

Comparez la ressource privée défaillante (example.net) à une ressource privée opérationnelle (abc.net) pour identifier les différences de configuration.

La ressource de travail utilisée :

- Utiliser une URL dans votre option de domaine
- Référence à la paire certificat/clé générique existante

### Étape 2: Analyse de capture de paquets

Effectuez une analyse de capture de paquets à l'aide de Wireshark pour confirmer l'échec de la connexion TLS :

- Vérifiez que la connexion TCP en trois étapes s'est correctement effectuée.
- Confirmer l'échec de la négociation TLS après Hello du client.
- Collecter les artefacts de diagnostic : Fichiers HAR, bundle DART et captures de paquets.

## Étape 3: Vérification du certificat

Accédez à l'application via une connexion RAVPN pour vérifier la présentation du certificat :

- Vérifiez que le site Web `example.net` présente un certificat générique.
- Documentez les détails du certificat pour référence de configuration.

## Étape 4: Configurer la ressource privée

Appliquez la même approche de configuration que celle utilisée par la ressource privée active :

- Configurez la ressource privée pour utiliser l'option Utiliser une URL dans votre domaine.
- Faites référence à la paire certificat/clé générique existante.
- Assurez-vous que le nom de domaine complet est correctement configuré dans le champ de ressource privée.

## Étape 5: Validation

Testez l'accès basé sur le navigateur pour confirmer que la configuration résout le problème :

- Vérifiez que la connexion TLS a réussi.
- Confirmez le flux d'authentification approprié.
- Validez l'accessibilité des applications après l'authentification.

## Motif

La cause principale était une non-concordance de configuration dans la configuration de ressource privée. La ressource privée défaillante n'a pas été configurée pour référencer correctement le certificat générique que l'application cible présentait. La connexion TLS a échoué

car la configuration de la ressource privée ne s'alignait pas sur la configuration du certificat utilisée par le serveur d'applications. En configurant la ressource privée pour utiliser l'option Utiliser une URL dans votre domaine et en référençant la paire certificat/clé générique existante (correspondant à la configuration de travail), la négociation TLS a pu se terminer avec succès.

## Autres informations utiles

- [Guide de référence Cisco pour un accès sécurisé](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.