

# Problèmes de pilotage du trafic ZTNA basé sur le client avec le client sécurisé

## Table des matières

---

### Problème

ZTNA (Zero Trust Network Access) basé sur le client ne parvient pas à fournir l'accès aux applications internes lorsqu'elles sont accessibles par FQDN ou adresse IP directe, alors que les mêmes applications restent accessibles via une connexion VPN.

Les symptômes spécifiques observés sont les suivants :

- Secure Client ZTNA ne peut pas atteindre les applications internes par FQDN ou IP direct lorsque le VPN est déconnecté.
- L'accès ZTNA basé sur navigateur fonctionne correctement pour les mêmes applications.
- Aucun événement ZTNA n'apparaît dans les journaux d'activité lorsque le VPN est en panne, ce qui indique que le trafic client n'est pas acheminé via le chemin ZTNA.
- Les définitions d'applications privées ont été vérifiées pour correspondre aux ressources routables VPN avec les configurations IP/port/FQDN correctes.
- Les stratégies ZTNA ont été confirmées pour correspondre aux affectations d'utilisateurs et de groupes de test.

Le problème se situe spécifiquement au niveau du mécanisme d'application ou de direction du trafic ZTNA du client sécurisé, car le ZTNA basé sur navigateur confirme que la publication et l'application du back-end fonctionnent correctement.

### Environnement

- Technologie : Accès sécurisé - ZTNA (Zero Trust Network Access)

- Composants: ZTNA basé sur le client, posture, inscription, accès aux ressources privées
- Client sécurisé avec profils VPN coexistants
- Applications privées accessibles via FQDN et adressage IP direct
- Fonctionnalité ZTNA basée sur un navigateur, fonctionnement confirmé
- Application de stratégie configurée en mode d'application des correspondances les plus spécifiques

## Résolution

La résolution impliquait des ajustements de configuration du profil ZTA et la validation de la politique. Les étapes décrites dans les sections suivantes ont été suivies pour restaurer la fonctionnalité client ZTNA.

### Étape 1: Ajouter des ressources privées au profil ZTA

Des ressources privées ont été ajoutées à la configuration du profil ZTA. Après cette modification, les événements bloqués ont commencé à apparaître dans les journaux d'activité et les captures d'écran, indiquant que le trafic client était désormais correctement acheminé via le chemin ZTNA.

### Étape 2: Vérification et test des politiques

Une règle temporaire « permet any » a été ajoutée pour valider le flux de trafic. Alors que cette règle était active, l'accès ZTNA basé sur le client fonctionnait correctement, confirmant que le mécanisme de pilotage du trafic fonctionnait, mais que l'application de la politique nécessitait un ajustement.

### Étape 3: Affinement des politiques

La règle permet-any temporaire a été supprimée et les politiques d'accès spécifiques ont été validées. Il a été confirmé que la ressource privée était accessible dans le cadre de la stratégie

d'accès nommée Ressources\_Cyril privées à l'aide du mode d'application de correspondance le plus spécifique de la plate-forme.

## Étape 4: Validation de configuration

L'utilisateur a confirmé que l'accès ZTNA basé sur le client a commencé à fonctionner de manière cohérente après les modifications de configuration. Le problème a été résolu sans nécessiter de modifications supplémentaires de la stratégie ou du système.

## Motif

La cause principale était une configuration de ressource privée incomplète dans le profil ZTA. Sans ressources privées appropriées définies dans le profil ZTA, le trafic client n'était pas dirigé via le chemin d'application ZTNA, ce qui l'a amené à revenir aux mécanismes de routage locaux. Cela a entraîné le contournement complet des politiques ZTNA par le trafic, ce qui a expliqué pourquoi aucun événement ZTNA n'apparaissait dans les journaux d'activité lorsque le VPN était déconnecté.

Le problème était spécifique à la configuration de direction de trafic ZTNA basée sur le client, tandis que ZTNA basée sur le navigateur a continué à fonctionner parce qu'il utilise un mécanisme de gestion de trafic différent qui a été correctement configuré.

## Autres informations utiles

- [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.