

# Comportement de pilotage du trafic d'accès sécurisé et configuration des listes d'exceptions

## Table des matières

---

## Problème

Les utilisateurs ont besoin de clarification sur le comportement de Cisco Secure Access Traffic Steering lors de l'utilisation de Use ZTA pour sécuriser toutes les destinations Internet paramètre avec des configurations d'exception par défaut. Des questions spécifiques se posent concernant :

- Indique si les décisions de direction du trafic sont basées sur les adresses IP de destination post-résolution DNS.
- Comment le trafic DNS lui-même est géré dans le processus de direction.
- Indique si des entrées de domaine local supplémentaires doivent être configurées au-delà de l'entrée de domaine .local par défaut dans la liste des exceptions.

La configuration en question se trouve à l'adresse suivante : Connect > End User Connectivity > Zero Trust Access > (profils d'accès sans confiance) > Secure Internet Access > Traffic Steering > Utilisez ZTA pour sécuriser toutes les destinations Internet

La liste d'exceptions par défaut inclut les plages d'adresses IP privées (classes A, B et C) et le domaine .local, et les utilisateurs doivent comprendre le comportement opérationnel de ces paramètres.

## Environnement

- Accès sécurisé Cisco
- Configuration ZTA (Zero Trust Access)
- Fonctionnalité de pilotage du trafic activée

- Liste d'exceptions par défaut contenant des plages IP privées et un domaine .local

## Résolution

Le comportement de Cisco Secure Access Traffic Steering fonctionne comme suit :

### Processus Décisionnel De Pilotage Du Trafic

Les décisions de direction du trafic sont prises en fonction de l'adresse IP de destination après la résolution DNS. Le système évalue l'adresse IP de destination réelle résultant de la résolution de noms DNS afin de déterminer si le trafic doit être dirigé via la pile de sécurité Zero Trust Access.

### Gestion du trafic DNS

Les requêtes DNS elles-mêmes ne sont pas soumises à la direction du trafic. Lorsque des points d'extrémité reçoivent des affectations de serveur DNS via DHCP qui pointent vers des serveurs DNS internes (généralement à l'aide d'adresses IP privées), ces communications DNS contournent le mécanisme de direction du trafic et sont gérées localement.

### Configuration de la liste des exceptions

La liste des exceptions par défaut comprend :

- Plages d'adresses IP privées (classe A : 10.0.0.0/8, Classe B : 172.16.0.0/12, classe C : 192.168.0.0/16)
- Le domaine .local

Pour les organisations utilisant des domaines locaux personnalisés (noms de domaine internes), des entrées de domaine supplémentaires doivent être ajoutées à la liste des exceptions pour garantir que le trafic interne n'est pas inutilement dirigé à travers la pile de sécurité. L'entrée .local par défaut couvre les protocoles de détection de réseau local standard, mais peut-être n'englobe

pas tous les domaines internes de l'organisation.

## Vérification de la configuration

Pour vérifier la configuration appropriée :

Accédez à Connect > End User Connectivity > Zero Trust Access > Secure Internet Access > Traffic Steering.

Vérifiez la liste des exceptions pour vous assurer qu'elle inclut toutes les plages d'adresses IP privées et tous les noms de domaine locaux nécessaires spécifiques à l'infrastructure interne de votre organisation.

## Motif

Il s'agit d'une demande d'informations concernant le comportement opérationnel des fonctionnalités Cisco Secure Access Traffic Steering. Il est nécessaire de clarifier les choses en raison de la complexité de la logique d'orientation du trafic et de l'interaction entre la résolution DNS, les décisions de routage basées sur IP et les mécanismes de gestion des exceptions.

## 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.