

Le module Secure Client Umbrella devient inactif en raison de la tempête DNS de l'application Codex

Table des matières

Problème

Plusieurs utilisateurs sur macOS voient le module d'itinérance Cisco Secure Client Umbrella passer par intermittence à l'état inactif (fail-open). Au cours de ces périodes, les requêtes DNS, y compris les commandes nslookup lancées par le terminal, ne parviennent pas à atteindre la couche réseau, ce qui a un impact sur la capacité des utilisateurs à résoudre des domaines et à accéder à des ressources basées sur Internet.

Le problème se manifeste par des défaillances répétées des sondes dans les journaux Umbrella, affichant des messages tels que :

```
Transparent probe failed  
Encrypted probe failed  
Switching to basic probe  
DNS probe failed by timeout - going open
```

L'analyse a révélé que le pilote de l'horloge plante pendant la même fenêtre de défaillance lorsque Umbrella devient inactif. Le problème est le plus souvent observé lorsque les utilisateurs utilisent activement les applications Codex et AI Assistant, avec un grand nombre de tentatives de connexion à chatgpt.com immédiatement après l'envoi des commandes à CODEX.

Environnement

- Cisco Secure Client versions 5.1.13, 5.1.16, 5.1.17
- macOS (plusieurs versions observées)

- Module d'itinérance Umbrella activé
- Module ZTNA/SIA (Secure Internet Access) activé
- Application du Codex utilisée
- Utilisateurs travaillant sur différents réseaux (domicile, bureau, différents FAI)

Résolution

Le problème a été résolu en implémentant des configurations de contournement de domaine pour empêcher la duplication des requêtes DNS. Les approches décrites dans les sections suivantes ont été validées.

Résolution principale : Contournement de domaine

- Étape 1: Ajoutez chatgpt.com à la liste de contournement dans la configuration Cisco Secure Access. Cela empêche le client sécurisé de dupliquer les requêtes DNS générées par l'application Codex, éliminant ainsi la tempête DNS qui provoque l'instabilité du pilote.
- Étape 2: Vérifiez la configuration du contournement. Testez la fonctionnalité du Codex pour confirmer que le problème ne se reproduit plus lorsque le contournement est en place.

Résolution alternative : Contournement de la configuration du Codex

Appliquez les modifications de configuration du Codex référencées dans le problème GitHub pour réduire le volume de requêtes DNS générées par l'application.

<https://github.com/openai/codex/issues/21218>

Étapes de dépannage avancées utilisées

Ces étapes de diagnostic ont été effectuées pour identifier la cause première.

1.- Activer la journalisation acsock explicite :

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -sdf 0x830801F2
```

2.- Reproduisez le problème et collectez le bundle DART immédiatement après l'échec.

3.- Désactiver la journalisation détaillée :

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4.- Activez la journalisation de débogage maximale pour SWG. Créez le fichier SWGConfigOverride.json avec le contenu suivant :

```
{"logLevel": "1"}
```

Enregistrez-le sur /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- Activer les journaux de suivi RSM pour DNS. Créez le fichier force_log_level.plist avec le contenu suivant :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

Enregistrez dans /opt/cisco/secureclient/umbrella/data.

Motif

Le problème principal est lié au comportement des applications Codex, qui génère un volume très

élevé de requêtes DNS. Lorsque chatgpt.com n'est pas contourné, ces requêtes sont dupliquées par le client sécurisé Cisco, créant une tempête DNS qui entraîne une utilisation élevée du processeur et une instabilité du pilote du noyau.

Le problème se produit parce que :

- Le Codex génère de nombreuses requêtes DNS vers chatgpt.com pendant le fonctionnement.
- Sans configuration de contournement, le client sécurisé intercepte et duplique ces requêtes.
- Le volume élevé de requêtes DNS dupliquées provoque la panne du pilote acsock.
- L'instabilité du pilote entraîne des défaillances de la sonde Umbrella et la transition vers l'état fail-open.

Lorsque chatgpt.com est contourné ou que la solution de contournement Codex est appliquée, cette duplication ne se produit pas et le problème ne se reproduit plus. Le problème affecte les configurations SIA Umbrella uniquement et ZTNA, indiquant que le problème se situe dans le mécanisme de gestion du trafic plutôt que dans un module spécifique.

Autres informations utiles

- [Dépannage du module d'itinérance Secure Access](#)
- [Dépannage et collecte des informations de base](#)
- [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.

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.