Le VPN client sécurisé se déconnecte avec le code de raison de terminaison 7 sur Ubuntu 24.04

Table des matières

Problème

Cisco Secure Client sur Ubuntu 24.04 établit une connexion VPN, mais se déconnecte en quelques secondes. La déconnexion est systématiquement accompagnée du code de raison de terminaison 7 et des pannes impliquant libvpnapi.so, ce qui empêche une connectivité VPN stable requise pour un accès professionnel normal.

La séquence de connexion montre le client atteignant l'état « Connected » mais revenant immédiatement à l'état Disconnected lors de la vérification de l'état. Le client VPN affiche le code de raison de terminaison 7 : L'agent a été « arrêté » dans les journaux, ainsi que les entrées de changement d'état de tunnel et les messages indiquant que les connexions DTLS/SSL sont démantelées avec des alertes de « notification de fermeture ».

Cette séquence de commandes illustre le problème :

```
/opt/cisco/secureclient/bin/vpn connect
```

Le résultat de la connexion indique un établissement réussi :

```
Cisco Secure Client (version 5.1.12.146) release.
Copyright (c) 2004 - 2025, Cisco Systems, Inc. All rights reserved.
  >> state: Unknown
  >> state: Disconnected
  >> state: Disconnected
  >> notice: Ready to connect.
  >> registered with local VPN subsystem.
  >> contacting host (vpn.sse.cisco.com) for login information...
  >> notice: Contacting vpn.sse.cisco.com.
  >> Your client certificate will be used for authentication
Group:
  >> state: Connecting
```

```
  >> notice: Establishing VPN session...
The Cisco Secure Client - Downloader is analyzing this computer. Please wait...
Initializing the Cisco Secure Client - Downloader...
The Cisco Secure Client - Downloader is performing update checks...
The Cisco Secure Client - Downloader update checks have been completed.
  >> notice: The Cisco Secure Client - Downloader is performing update checks...
  >> notice: Checking for profile updates...
  >> notice: Checking for customization updates...
  >> notice: Performing any required updates...
  >> notice: The Cisco Secure Client - Downloader update checks have been completed.
Please wait while the VPN connection is established...
  >> state: Connecting
  >> notice: Establishing VPN session...
  >> notice: Establishing VPN - Initiating connection...
  >> notice: Establishing VPN - Examining system...
  >> notice: Establishing VPN - Activating VPN adapter...
  >> notice: Establishing VPN - Configuring system...
  >> notice: Establishing VPN...
  >> state: Connected
```

Cependant, lors de la vérification de l'état immédiatement après la connexion :

```
/opt/cisco/secureclient/bin/vpn status
```

Le client affiche l'état déconnecté :

```
Cisco Secure Client (version 5.1.12.146) release.
Copyright (c) 2004 - 2025, Cisco Systems, Inc. All rights reserved.
  >> state: Unknown
  >> state: Disconnected
  >> state: Disconnected
  >> state: Disconnected
  >> notice: Ready to connect.
  >> registered with local VPN subsystem.
VPN>
```

Environnement

- Système d'exploitation : Ubuntu 24.04
- Version du client sécurisé Cisco : 5.1.12.146
- Méthode d'authentification : Authentification du certificat client

- Interface virtuelle : cscotun0 (ou interface virtuelle Cisco Secure Client similaire)
- L'environnement inclut des scripts d'automatisation pour la gestion système

Résolution

Le problème a été résolu en identifiant et en corrigeant un script d'automatisation qui identifiait de manière incorrecte l'interface virtuelle du client sécurisé Cisco (cscotun0) en tant que nouveau périphérique physique et en lui appliquant une configuration de proxy HTTP/transparent. Les étapes suivantes décrivent le processus de résolution.

Étape 1: Collecter les informations de diagnostic

Générez des offres groupées DART (Diagnostic and Reporting Tool) à partir du terminal affecté pour capturer des journaux client VPN détaillés et des informations système :

```
Generate DART bundle from Cisco Secure Client interface or command line
```

Les ensembles DART contiennent des entrées du journal de l'agent VPN indiquant les étapes de configuration de l'interface et du profil, y compris les paramètres DNS pour l'interface cscotun0, la configuration de l'adaptateur VPN et les modifications de la table de routage.

```
Mar 13 16:41:08  Message type information sent to
> the user: Contacting vpn.sse.cisco.com.
> Mar 13 16:41:08 : VPN SESSION START: Initiating
> VPN connection to the secure gateway hvpn.sse.cisco.com
> Mar 13 16:41:08 The Cisco Secure Client -
> AnyConnect VPN has obtained the following proxy server configuration from
> the operating system: http://x.x.x.x:3128/
> Mar 13 16:41:08 The Cisco Secure Client -
> AnyConnect VPN has obtained the following proxy exception list from the
> operating system: localhost,127.0.0.0/8,::1
> Mar 13 16:41:11 Termination reason code 7: The
> agent has been stopped.
```

Étape 2: Analyser le comportement des scripts d'automatisation

Étudier les scripts d'automatisation locaux qui gèrent les interfaces réseau et les configurations de proxy. Recherchez des scripts qui détectent automatiquement les nouvelles interfaces réseau et appliquent des stratégies de configuration.

Étape 3: Identifier le problème d'affectation proxy

Déterminez si les scripts d'automatisation traitent l'interface virtuelle Cisco Secure Client comme un nouveau périphérique physique et appliquent des paramètres de proxy inappropriés. La configuration de proxy HTTP/transparent ne peut pas être appliquée à l'interface virtuelle (cscotun0 ou similaire).

Étape 4: Supprimer la configuration du proxy de l'interface virtuelle

Supprimez ou corrigez l'affectation de proxy qui a été automatiquement appliquée à l'interface virtuelle du client sécurisé Cisco par le script d'automatisation. Cela empêche le proxy d'interférer avec le flux de trafic VPN.

Étape 5: Mettre à jour la logique de script Automation

Modifiez le script d'automatisation pour exclure les interfaces virtuelles du client sécurisé Cisco (généralement nommées cscotun0, cscotun1) des stratégies de configuration de proxy automatique. Ajoutez une logique pour identifier et ignorer les interfaces virtuelles VPN pendant les processus de configuration réseau automatisés.

Étape 6: Vérification de la connectivité VPN

Testez la connectivité VPN après avoir supprimé la configuration du proxy pour confirmer la connexion stable :

```
/opt/cisco/secureclient/bin/vpn connect vpn.sse.cisco.com
```

Vérifiez que la connexion reste stable en vérifiant son état après l'établissement de la connexion :

```
/opt/cisco/secureclient/bin/vpn status
```

Autres étapes de dépannage

Si le problème persiste ou se produit dans des environnements similaires, envisagez les approches de dépannage supplémentaires suivantes :

- Tester le client sécurisé Cisco sur un terminal Linux neuf sans scripts d'automatisation
- Désactivez temporairement les services tiers qui peuvent interférer avec libvpnapi ou l'agent VPN
- Mettre à niveau Cisco Secure Client vers la dernière version disponible
- Examiner les journaux système pour les conflits avec la création et la configuration d'interface virtuelle VPN

Motif

La cause principale était un script d'automatisation interne qui a identifié de manière incorrecte l'interface virtuelle du client sécurisé Cisco (cscotun0 ou similaire) comme nouveau périphérique réseau physique. Le script a automatiquement appliqué la configuration de proxy HTTP/transparent à cette interface virtuelle, ce qui a interféré avec le flux de trafic VPN et provoqué l'arrêt de la connexion avec le code de raison 7.

Lorsque le client VPN établit une connexion, il crée une interface réseau virtuelle pour gérer le trafic chiffré. Le script d'automatisation a détecté cette création d'interface en tant que nouveau périphérique réseau rejoignant le système et a appliqué des politiques de proxy standard destinées aux interfaces réseau physiques. Cette configuration de proxy a perturbé la capacité du tunnel VPN à acheminer correctement le trafic chiffré, entraînant une déconnexion immédiate après l'établissement réussi de la connexion.

Le code de raison de fin 7 (« L'agent a été arrêté ») et les pannes libvpnapi.so étaient des symptômes de l'interférence proxy sous-jacente plutôt que des problèmes logiciels client VPN

directs.

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.