Connexion VPN client sécurisé Cisco réinitialisée par homologue avec interférence de décodage SSL/TLS Zscaler

Table des matières

Problème

Un utilisateur rencontre des échecs de connexion VPN lorsqu'il tente d'établir une connexion à l'aide de Cisco Secure Client.

Environnement

- Technologie : Accès sécurisé Cisco - Accès à distance sécurisé du client (VPN, position, ressource privée)
- Gamme de produits : SECACS
- Système d'exploitation : macOS (basé sur les chemins d'accès des fichiers journaux affichant /Users/admin/workspace/secure-client-macos_Raccoon_MR15/)
- Logiciels tiers : Zscaler installé sur le système client
- Protocole VPN : CSTP (Cisco SSL Tunnel Protocol)
- Version TLS : TLS 1.3 avec chiffrement TLS_AES_256_GCM_SHA384

Résolution

La résolution implique l'identification et la résolution du conflit entre le client sécurisé Cisco et la fonctionnalité de déchiffrement SSL/TLS de Zscaler.

Étape 1: Analyse et diagnostic du journal

Capturez et analysez les journaux DART du client sécurisé Cisco pour identifier le modèle d'échec de connexion. Les journaux affichent l'établissement réussi de la session TLS suivi d'une réinitialisation immédiate de la connexion.

Indicateurs de diagnostic clés dans les journaux :

- Établissement de la connexion TLS 1.3 avec le chiffrement TLS_AES_256_GCM_SHA384
- Calcul MTU et négociation HTTP en cours normalement
- Erreur de réinitialisation de la connexion par l'homologue (code de retour : 54) pendant l'opération de lecture de socket

La session TLS 1.3 s'établit avec succès à l'aide du chiffrement TLS_AES_256_GCM_SHA384, mais immédiatement après l'établissement de la session, un paquet de réinitialisation est envoyé qui met fin à la connexion, entraînant l'arrêt du tunnel VPN. L'erreur spécifique observée dans les journaux montre "Connection reset by peer" avec le code de retour 54 (0x00000036) pendant l'opération de lecture de socket.

La séquence d'erreurs suivante se produit lors des tentatives de connexion :

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

Étape 2: Identification des logiciels tiers

Étudiez la présence de logiciels de sécurité tiers susceptibles d'effectuer une inspection ou un déchiffrement SSL/TLS sur le système client. Dans ce cas, Zscaler a été identifié comme l'application brouilleuse.

Étape 3: Résolution des conflits de déchiffrement SSL/TLS

Gérez le conflit entre le trafic VPN du client sécurisé Cisco et la fonctionnalité de déchiffrement SSL/TLS de Zscaler. Le trafic VPN semble subir un déchiffrement SSL/TLS par Zscaler, ce qui interfère avec l'établissement du tunnel VPN et provoque la réinitialisation de la connexion.

Les approches de résolution possibles incluent :

- Configurer Zscaler pour exclure le trafic VPN du client sécurisé Cisco de l'inspection SSL/TLS
- Créer des règles de contournement dans Zscaler pour les terminaux du serveur VPN
- Désactiver temporairement Zscaler pendant le test de la connexion VPN pour confirmer le conflit
- Coordination avec l'équipe de sécurité du réseau pour définir les exclusions appropriées

Motif

La cause principale de ce problème est un conflit entre le trafic VPN du client sécurisé Cisco et la fonctionnalité de déchiffrement SSL/TLS de Zscaler. Lorsque Zscaler tente de décrypter ou d'inspecter le trafic TLS du VPN, il interfère avec le processus d'établissement de tunnel sécurisé. Cette interférence se manifeste sous la forme d'une réinitialisation de connexion immédiatement après l'établissement de la session TLS, empêchant le tunnel VPN de terminer sa phase de négociation. La synchronisation du paquet de réinitialisation (qui se produit juste après l'établissement réussi de TLS mais avant l'achèvement du tunnel) est caractéristique des interférences d'inspection SSL/TLS provenant des appareils de sécurité ou du logiciel.

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.