Échec de la confiance SSL/TLS du module Secure Client Umbrella lors de l'enregistrement du périphérique

Table des matières

Problème

Lors du déploiement de Cisco Secure Client avec le module Umbrella, les périphériques ont cessé de se synchroniser avec le tableau de bord et ont été signalés comme étant « inactifs ». Les clients affectés ont rencontré des échecs d'approbation SSL/TLS lors de leur tentative d'inscription à devices.api.sse.cisco.com, ce qui a empêché l'inscription réussie du périphérique et la couverture de protection.

L'interface utilisateur a indiqué que Umbrella était inactif avec ces messages d'état :

- Le parapluie est inactif.
- Vous n'êtes actuellement pas protégé par une passerelle Web sécurisée.
- La passerelle Web sécurisée n'est pas sous licence / est désactivée.

Les résultats du diagnostic ont révélé un échec d'approbation SSL/TLS cohérent lors de l'enregistrement avec ce message d'erreur dans les journaux du client sécurisé :

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

Environnement

- Déploiement de Cisco Secure Client avec module Umbrella sur plus de 2 000 terminaux
- Infrastructure SD-WAN avec politiques de routage

- Tunnels Umbrella hérités en place
- Configuration du réseau permettant toutes les destinations requises par la documentation Cisco
- Aucun déchiffrement SSL actif pour les destinations Cisco sur le périmètre

Résolution

La résolution impliquait l'identification et la correction d'un problème de configuration de routage qui entraînait une mauvaise orientation du trafic d'enregistrement des périphériques via les tunnels Umbrella hérités.

Identification de la cause première

L'analyse des données de capture de paquets a révélé que le certificat TLS présenté pour la connexion API était un certificat Cisco Umbrella plutôt que le certificat Cisco Secure Access/Let's Encrypt attendu. Identifiez l'adresse IP de devices.api.sse.cisco.com.

Un examen plus approfondi a permis d’identifier une politique de route SD-WAN qui correspondait au sous-réseau 146.112.0.0/16, entraînant le routage du trafic vers devices.api.sse.cisco.com dans les tunnels Umbrella hérités au lieu de la destination prévue.

Problèmes liés à la modification de la configuration

Les mesures suivantes ont été prises pour résoudre le problème :

- Étape 1: Supprimez les routes statiques problématiques. Les routes statiques pointant vers 146.112.0.0/16 vers les tunnels Umbrella hérités ont été supprimées de la configuration SD-WAN.
- Étape 2: Validez la connectivité. Après la suppression des routes statiques, les clients affectés ont été testés pour s'assurer qu'ils pouvaient se connecter et s'inscrire à devices.api.sse.cisco.com.

Vérification

La chaîne de certificats attendue pour devices.api.sse.cisco.com doit apparaître comme suit :

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
   i:C = US, O = Let's Encrypt, CN = R13
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

Après avoir implémenté les modifications de configuration, les clients concernés se sont connectés et inscrits avec succès, et le déploiement s'est terminé avec succès.

Motif

La cause principale était une stratégie de route SD-WAN qui correspondait au sous-réseau 146.112.0.0/16, ce qui entraînait un routage incorrect du trafic d'enregistrement de périphérique destiné à devices.api.sse.cisco.com (146.112.59.104) via des tunnels Umbrella hérités. Cela a entraîné la présentation d'un certificat TLS incorrect (certificat Cisco Umbrella au lieu du certificat Cisco Secure Access/Let's Encrypt attendu), ce qui a entraîné des échecs de confiance SSL/TLS lors du processus d'enregistrement du périphérique.

Autres informations utiles

- Documentation sur les exigences du réseau Cisco Secure Client

- 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.