

L'accès Internet échoue lorsque le service Secure Client Umbrella SWG Agent est actif

Table des matières

Problème

Lorsque le service Cisco Secure Client - Umbrella SWG Agent est exécuté sur un ordinateur portable Dell Windows, les utilisateurs ne peuvent accéder à aucun site Web. Une fois le service Umbrella SWG Agent arrêté, l'accès Web normal est rétabli. Le problème se produit avec la version 5.1.14.145 de Cisco Secure Client, qui inclut les modules AnyConnect VPN et Umbrella. Le fichier OrgInfo.json se trouve dans le répertoire prévu et le certificat d'autorité de certification racine d'accès sécurisé Cisco est installé dans le magasin de certificats racine approuvé.

Environnement

- Produit : Cisco Secure Client (modules VPN AnyConnect et Umbrella)
- Version du logiciel: 5.1.14.145
- Système d'exploitation : Windows (ordinateur portable Dell)
- Service d'agent SWG Umbrella activé/désactivé
- OrgInfo.json présent dans %ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
- Autorité de certification racine Cisco Secure Access installée dans le magasin Autorités de certification racine de confiance
- Sécurité DNS/Web activée dans le tableau de bord d'accès sécurisé
- Profil de sécurité affecté avec déchiffrement activé

Résolution

Le problème a été résolu en identifiant et en corrigeant une erreur de synchronisation NTP (Network Time Protocol) sur le périphérique client. L'incapacité à synchroniser le temps a empêché la communication sécurisée requise par l'agent SWG Umbrella pour le trafic Web proxy, ce qui a entraîné des paquets de réinitialisation TCP (RST) et une perte d'accès Web. Une fois la synchronisation NTP restaurée, l'accès Web a fonctionné normalement avec l'agent SWG actif.

Suivez ce workflow de dépannage complet.

Étape 1 : vérification de la configuration et des conditions préalables

- Assurez-vous que OrgInfo.json se trouve dans
%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json.
- Vérifiez que l'autorité de certification racine d'accès sécurisé Cisco est présente dans le

magasin Autorités de certification racine de confiance.

- Vérifiez que la sécurité DNS/Web est activée dans le tableau de bord Accès sécurisé.
- Vérifiez que le décodage est activé sur le profil de sécurité affecté.

Étape 2 : Capturer et analyser le trafic réseau

Obtenez une capture de paquets du trafic client dirigé vers le proxy SWG pour identifier les comportements anormaux, tels que les paquets de réinitialisation TCP inattendus.

Description de la capture de paquets montrant le problème :

The packet capture revealed that TCP reset (RST) packets were being sent to the client, disrupting the

Étape 4 : Validez les règles du pare-feu de périmètre

- Inspectez les règles de pare-feu de périmètre pour vous assurer que le trafic en provenance et à destination des serveurs SWG est autorisé sur l'interface d'entrée.

Étape 5 : Exécutez les tests de diagnostic du système et du protocole

Exécutez cette commande sur le client pour vérifier les erreurs de synchronisation NTP :

```
curl ipinfo.io
```

Description du résultat du diagnostic :

The output indicated NTP timing was out of sync on the client device.

Motif

La cause principale était une défaillance dans la synchronisation NTP (Network Time Protocol) sur le périphérique client. Ce problème de synchronisation a empêché la communication sécurisée entre le client et le service proxy SWG Umbrella, ce qui a entraîné la réinitialisation des paquets TCP et la perte de l'accès Web lorsque le service SWG Agent était actif. La résolution du problème de synchronisation NTP a restauré le bon fonctionnement de l'agent SWG Umbrella, permettant ainsi le proxy sécurisé du trafic Web.

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.