Connexion VPN AnyConnect refusée en raison des conditions de position du terminal, notamment Cortex

Table des matières

Problème

Plusieurs utilisateurs ne peuvent pas se connecter par intermittence à Secure Client Remote Access (RAVPN) et reçoivent le message d'erreur « Connexion VPN AnyConnect refusée. Votre environnement ne répond pas aux critères d'accès définis par votre administrateur." Le problème affecte les MacBooks et les ordinateurs portables Surface, les utilisateurs nécessitant souvent plusieurs tentatives de connexion ou des redémarrages du système pour établir une connexion réussie. Les défaillances de connexion semblent être liées aux conditions de validation de la position des terminaux, en particulier les exigences de version de macOS et la vérification de l'état de Cortex XDR.

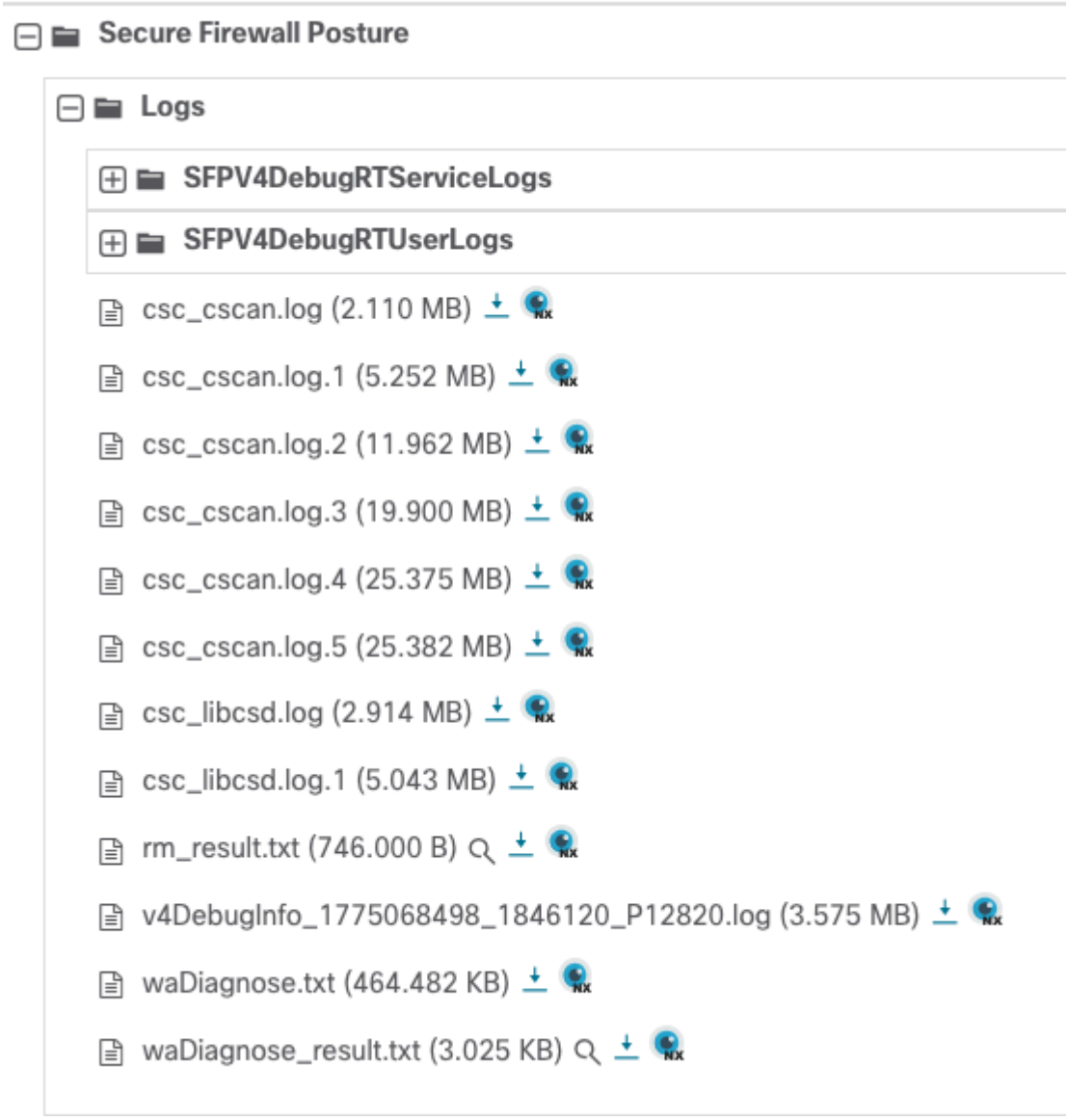
Environnement

- Déploiement RAVPN (Secure Client Remote Access) avec évaluation de la position
- Environnement mixte de terminaux, y compris MacBooks et ordinateurs portables Surface
- Exigences de positionnement des terminaux : macOS version 26.2 ou ultérieure et Cortex XDR en cours d'exécution
- Solution d'accès sécurisé avec application de la politique d'accès aux périphériques (DAP)

Résolution

1: Collectez DART.

2: Accédez au dossier Secure Firewall Posture et téléchargez csc_scan.log :



image_en_ligne_0.png

3: Recherchez ces journaux :

[ven. 27 mars 13:53:10.419 2026] debug :: Joindre en tant que {"input":{"method":1000,"signature":}}

[ven. 27 mars 13:53:10.420 2026] erreur :: Opswat a renvoyé une erreur : -22 et converti en : 6

[ven. 27 mars 13:53:10.420 2026] erreur :: Échec dans la condition : état opSuccess !=

[ven. 27 mars 13:53:10.420 2026] debug :: L'accès au statut de retour Opswat est refusé

[ven. 27 mars 13:53:10.420 2026] debug :: utilisation du service pour vérifier l'état rtp de

l'antimalware.

[ven. 27 mars 13:53:10.420 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[ven. 27 mars 13:53:10.420 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[ven. 27 mars 13:53:10.420 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[ven. 27 mars 13:53:10.420 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[ven. 27 mars 13:53:15.060 2026] erreur :: réception de la réponse.

[Ven Mar 27 13:53:15.060 2026] debug :: impossible d'effectuer une vérification de la mémoire vive rtp.<<<<--------

[ven. 27 mars 13:53:15.060 2026] info :: l'état RTP renvoyé est failed

[ven. 27 mars 13:53:15.060 2026] info :: La date de définition du retour Opswat est 1

[Ven Mar 27 13:53:15.060 2026] debug :: utilisation du service pour obtenir la date de définition de l'antimalware.

[Ven mars 27 13:53:15.060 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[Ven mars 27 13:53:15.060 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[Ven mars 27 13:53:15.060 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[Ven mars 27 13:53:15.060 2026] trace :: État TCP/IP Ipv4(1),Ipv6(1)

[ven. 27 mars 13:53:20.079 2026] erreur :: réception de la réponse.

[ven. 27 mars 13:53:20.079 2026] debug :: impossible d'effectuer l'opération de date de définition de l'antimalware <<<<<<—

[ven. 27 mars 13:53:20.079 2026] debug :: a détecté un programme anti-programme malveillant ==> () (Cortex XDR (Mac)) (9.1.0) () () (échec) .

[Ven Mar 27 13:53:20.084 2026] debug :: Échec de la correspondance : Les noms de processus sont « ciscod » et « cscan »

[Ven Mar 27 13:53:20.084 2026] debug :: état de vérification de la connexion internet edr (1)

Remarque : Sur cette base, il semble être soit une restriction par Cortex à nos processus ou une restriction à l'accès à Internet et l'autre chose que nous pouvons vérifier si Cortex n'interfère pas avec le processus. Il peut bloquer la position du pare-feu sécurisé, car l'analyse peut être traitée comme un programme malveillant.

Liste d'exclusion d'AntiMalware

Cisco Secure Client (CSC) : tous les modules - système

1. Windows : C:\Program Files (x86)\Cisco\Cisco Secure Client*
2. macOS : /opt/cisco/secureclient/*
3. Linux : /opt/cisco/secureclient/*

Cisco Secure Client (CSC) : tous les modules - utilisateur

1. Windows : %localappdata%\\Cisco\Cisco Secure Client*
2. macOS: ~/.cisco/secureclient/*
3. Linux: ~/.cisco/secureclient/*

Motif

Le problème est causé par des défaillances intermittentes dans le processus d'évaluation de la position des terminaux, en particulier liées à la validation des exigences de version de macOS et de l'état de Cortex XDR. Le système d'évaluation de la position détecte ou valide de manière incohérente les conditions de sécurité requises (macOS 26.2 ou version ultérieure et état

d'exécution de Cortex XDR), ce qui entraîne des refus de connexion même lorsque les terminaux répondent aux critères spécifiés. Les utilisateurs ont donc besoin de plusieurs tentatives de connexion ou de redémarrages du système pour réussir l'évaluation de la position et la connexion VPN.

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.