La fenêtre contextuelle Secure Client Machine Tunnel Authentication provoque des déconnexions sur les réseaux non approuvés

Table des matières

Problème

Cisco Secure Client (AnyConnect) demande à plusieurs reprises un nom d'utilisateur et un mot de passe lorsqu'un tunnel de machine est connecté, en particulier lorsque les utilisateurs se connectent à partir de réseaux non fiables. La fenêtre contextuelle d'authentification interrompt la connectivité du tunnel de l'ordinateur et entraîne des déconnexions, ce qui affecte la capacité des utilisateurs à maintenir un accès distant stable. Ce problème se produit bien que le tunnel de la machine soit correctement établi et authentifié, avec la fenêtre contextuelle apparaissant de manière inattendue et interrompant la continuité de la session VPN.

Environnement

- Cisco Secure Client (AnyConnect) avec configuration de tunnel machine
- Profil VPN d'accès à distance avec la fonctionnalité Trust Network Detection (TND) activée
- Machine utilisateur connectée au tunnel de machine
- Objets de stratégie de groupe (GPO) utilisés pour la distribution des profils clients
- Profils de tunnel utilisateur et de tunnel machine configurés avec les paramètres TND

Résolution

Le problème a été résolu en modifiant les paramètres de configuration TND (Trust Network Detection) pour les profils de tunnel de machine et de tunnel d'utilisateur. La solution implique de

configurer le comportement de l'action TND pour empêcher les invites d'authentification inutiles sur les réseaux non approuvés.

Étape 1: Configuration des paramètres TND pour les réseaux non approuvés

Définissez l'action Détection du réseau approuvé sur Ne rien faire pour les réseaux non approuvés sur les profils de tunnel de machine et de tunnel d'utilisateur. Cette configuration empêche le client de demander des informations d'identification supplémentaires lorsqu'il est connecté à des réseaux non approuvés.

Étape 2: Configuration des paramètres TND pour les réseaux approuvés

Définissez l'action Détection du réseau sécurisé sur Déconnexion pour les réseaux sécurisés, en conservant le comportement de sécurité prévu pour les environnements réseau sécurisés connus.

Étape 3: Déployer les modifications de configuration

Déployez les paramètres TND mis à jour via la diffusion d'objet de stratégie de groupe (GPO) pour distribuer les modifications de configuration à toutes les machines clientes affectées.

Étape 4: Redémarrer les machines clientes

Redémarrez les ordinateurs clients après la mise à jour du profil pour vous assurer que les nouveaux paramètres TND prennent effet correctement.

Étape 5: Test de validation

Testez la connectivité du tunnel de la machine sur plusieurs réseaux non approuvés pour vérifier que :

- La fenêtre contextuelle d'authentification n'apparaît plus
- Le tunnel de la machine reste connecté de manière cohérente
- Aucune invite d'informations d'identification n'interrompt la session VPN
- Les utilisateurs peuvent maintenir un accès à distance stable sans déconnexions

L'utilisateur a confirmé une résolution réussie après la mise en oeuvre de ces modifications, avec plusieurs tests utilisateur validant la continuité stable de la session VPN dans diverses conditions du réseau.

Motif

La cause principale était une configuration incorrecte des paramètres TND (Trust Network Detection) sur les profils Cisco Secure Client. La fonctionnalité TND déclenchait des invites d'authentification lorsque des utilisateurs se connectaient à partir de réseaux non approuvés, même si le tunnel de la machine était déjà correctement authentifié et établi. Les actions TND pour les profils de tunnel utilisateur et de tunnel machine n'ont pas été configurées de manière optimale pour l'environnement réseau, ce qui a amené le client à demander des informations d'identification supplémentaires inutilement et a perturbé la connectivité du tunnel machine.

Autres informations utiles

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.