

Comportement de la connexion VPN manuelle TND du client sécurisé et considérations relatives au blocage des URL

Table des matières

Problème

Lors de l'utilisation d'un profil VPN avec la fonctionnalité TND (Trusted Network Detection) configurée avec le paramètre Trusted Network défini sur Disconnect, les points d'extrémité situés dans le réseau sécurisé peuvent toujours établir avec succès une connexion VPN lorsque les utilisateurs lancent manuellement des connexions à l'aide de Cisco Secure Client.

Ce comportement se produit bien que la configuration TND soit définie pour déconnecter les sessions VPN lorsque le point d'extrémité est détecté sur un réseau approuvé.

Les préoccupations particulières suivantes ont été soulevées :

- Les connexions VPN manuelles à partir de points d'extrémité de réseau sécurisé ne peuvent pas être contrôlées ou bloquées via la configuration TND standard
- Incertitude quant à savoir si les paramètres Cisco Secure Access (CSA) peuvent bloquer les connexions VPN manuelles à partir de points d'extrémité de réseau de confiance
- Questions relatives à la stabilité de l'URL de connexion au profil VPN (xxxx.vpn.sse.cisco.com) et à son éventuelle modification périodique, qui pourrait affecter les stratégies de blocage basées sur le pare-feu

Environnement

- Déploiement de Cisco Secure Access (CSA)
- Configuration du client sécurisé Cisco avec profil VPN

- Fonction TND (Trusted Network Detection) activée
- Paramètre TND Trusted Network configuré comme Disconnect
- Terminals situés dans le réseau sécurisé configuré
- Infrastructure pare-feu pour le contrôle d'accès réseau

Résolution

Comprendre le comportement de TND avec des connexions VPN manuelles

Le comportement observé est conforme à la fonctionnalité documentée de Cisco Secure Client. Selon la documentation Cisco, TND ne déconnecte pas ou n'empêche pas une session VPN qu'un utilisateur démarre manuellement sur un réseau sécurisé. Il s'agit du comportement attendu quels que soient les paramètres de configuration TND.

Les principaux faits techniques sont les suivants :

- La fonctionnalité de déconnexion automatique TND s'applique uniquement aux connexions VPN établies automatiquement.
- Les connexions VPN manuelles initiées par les utilisateurs contournent le comportement de déconnexion TND.
- Aucun paramètre de configuration CSA n'existe pour bloquer les connexions VPN manuelles à partir de points d'extrémité de réseau sécurisé.

Stratégie d'atténuation opérationnelle

La principale méthode de contrôle des connexions VPN manuelles à partir des points d'extrémité du réseau de confiance est le contrôle au niveau du réseau :

Étape 1: Implémenter le blocage des URL du pare-feu : Configurez le pare-feu Trusted Network pour bloquer l'accès à l'URL de connexion du profil VPN (xxxx.vpn.sse.cisco.com). Cela empêche les points d'extrémité du réseau sécurisé d'atteindre le point d'extrémité du service VPN.

Étape 2: Vérification de la stabilité des URL : L'identificateur d'URL de profil VPN (la partie xxxx) est spécifique au client et ne devrait pas changer périodiquement. Cela fournit une cible stable pour les règles de blocage de pare-feu.

Validation et tests

Les tests ont confirmé que le blocage de l'URL de connexion du profil VPN au niveau du pare-feu du réseau sécurisé empêche les terminaux d'établir des connexions VPN, même lorsque les utilisateurs tentent des connexions manuelles via Cisco Secure Client.

Motif

Ce comportement a été conçu dans le cadre de la mise en oeuvre TND de Cisco Secure Client. La fonctionnalité TND est spécifiquement conçue pour gérer les connexions VPN automatiques en fonction de l'état de confiance du réseau, mais elle n'interfère pas intentionnellement avec les connexions VPN manuelles initiées par l'utilisateur. Cette conception permet aux utilisateurs de remplacer le comportement automatique lorsque cela est nécessaire, tout en assurant la détection automatique du réseau et la gestion des connexions pour les cas d'utilisation classiques.

Autres informations utiles

- [Guide d'administration de Cisco Secure Client - Configuration TND](#)
- [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.