Défis posés par la configuration du split tunneling à accès sécurisé

Table des matières

Problème

Lors de la configuration de la fonctionnalité Cisco Secure Access (TIA) pour le trafic de tunnel partagé, plusieurs complications ont été rencontrées au cours du processus de configuration qui ont empêché un déploiement correct :

- Défis liés à l'identification du trafic Lors de la configuration de TIA pour la transmission tunnel partagée, tout le trafic VPN doit être exclu de l'inspection de sécurité Internet. L'identification des flux de trafic requis s'est avérée difficile, et certaines URL de redirection ont été particulièrement difficiles à suivre et à classer.
- Contraintes de trafic d'authentification : Dans certains scénarios de split-tunnel, le trafic d'authentification devait être exclu du proxy. Cependant, en fonction des stratégies existantes, le trafic lié à l'authentification ne pouvait pas être contourné à partir du proxy, ce qui entraînait des conflits de stratégie.
- Risques de sécurité lors de la déconnexion VPN : Le trafic de tunnel partagé est exposé à l'Internet ouvert lorsque le VPN se déconnecte, ce qui entraîne des risques de sécurité supplémentaires qui doivent être pris en compte lors de la configuration.

D'autres problèmes de configuration ont également été observés au cours du processus, qui ont nécessité une analyse et une résolution plus poussées.

Environnement

- Gamme de produits : SECACS (Secure Access)
- Technologie : Cisco Secure Access (TIA) avec fonction de transmission tunnel partagée
- Configuration: Scénarios de trafic de tunnel partagé avec les politiques existantes

- Authentification: Gestion du trafic d'authentification par proxy
- Sécurité du réseau : Exigences d'inspection de sécurité Internet pour le trafic VPN

Résolution

Sur la base des défis de configuration identifiés avec la tunnellisation partagée Cisco Secure Access, une demande de fonctionnalité complète a été soumise pour résoudre les limitations et les conflits de stratégie identifiés.

Envoi de demande de fonctionnalité

Une demande de fonctionnalité (CSE-I-5636) a été ouverte et soumise pour examen par l'équipe d'ingénierie concernée afin de résoudre les problèmes de configuration suivants :

- Fonctionnalités d'identification de trafic améliorées pour l'exclusion du trafic VPN de l'inspection de sécurité Internet
- Meilleure gestion des URL de redirection difficiles à suivre et à classer
- Résolution des limitations de contournement du trafic d'authentification avec les politiques existantes
- Atténuation des risques de sécurité en cas d'exposition du trafic en tunnel partagé pendant la déconnexion VPN

Motif

Les défis de configuration découlent des limites actuelles de la mise en oeuvre de la transmission tunnel partagée Cisco Secure Access (TIA) qui ne répondent pas adéquatement aux scénarios de déploiement d'entreprise complexes. Plus précisément, le système ne dispose pas d'un contrôle granulaire suffisant pour l'identification et la catégorisation du trafic, a des contraintes pour contourner le trafic d'authentification lorsque des politiques sont en place, et ne fournit pas de garanties de sécurité adéquates pour le trafic à tunnel partagé lorsque des connexions VPN sont interrompues.

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.