Secure Access Network Tunnel Group Internal Server Error Reverting Primary Peer IP

Table des matières

Problème

Lors de la tentative de modification de l'adresse IP de l'homologue distant dans un groupe de tunnels de réseau (NTG) sur Cisco Secure Access, les utilisateurs peuvent rencontrer une « erreur de serveur interne » dans l'interface utilisateur lors de la tentative de retour de l'adresse IP du tunnel principal à une valeur précédemment configurée. Le scénario spécifique implique :

- Un NTG initialement configuré avec une adresse IP de tunnel principale et une adresse IP secondaire, les deux tunnels s'établissant avec succès.
- L'adresse IP du tunnel principal est changée en une autre adresse IP à des fins de test, qui est acceptée sans problème.
- Lorsque vous essayez de rétablir la valeur d'origine de l'adresse IP du tunnel principal, le système ne parvient pas à enregistrer la configuration et renvoie une erreur de serveur interne dans l'interface utilisateur.
- Ce comportement est toujours reproductible et apparaît lorsque vous tentez de réutiliser une adresse IP précédemment configurée.
- L'adresse IP d'origine fonctionnait auparavant et il n'y a aucun conflit avec l'adresse IP du tunnel secondaire.

Environnement

- Cisco Secure Access (anciennement Cisco Umbrella pour SSE)
- Configuration du groupe de tunnels réseau pour l'accès privé
- Configuration à double tunnel avec IP homologues principal et secondaire
- Interface de gestion basée sur le Web

Résolution

Ce problème est causé par un problème de validation/d'état du serveur principal où l'IP homologue d'origine reste réservée ou bloquée dans le système principal après des modifications de configuration. Les étapes de dépannage et de résolution décrites dans la section suivante doivent être suivies :

Étape 1: Collecte des informations de diagnostic

Collectez les informations suivantes pour la validation du back-end :

- ID d'organisation d'accès sécurisé
- Nom du groupe de tunnels réseau
- ID de tunnel pour le tunnel principal affecté
- Région/Data center sélectionné pour le NTG
- Horodatage exact d'une tentative d'enregistrement ayant échoué, fuseau horaire compris
- Confirmation de l'affichage de l'adresse IP d'origine dans un autre NTG, actuel ou précédent
- Capture HAR du navigateur de la tentative d'enregistrement ayant échoué

Étape 2: Fichier HAR du navigateur de capture

Pour collecter des données de diagnostic pour la tentative d'enregistrement ayant échoué :

- Ouvrir le navigateur Outils de développement
- Accédez à l'onglet Réseau
- Activer le journal de conservation
- Reproduire l'échec de sauvegarde
- Exportez le fichier HAR et joignez-le au dossier d'assistance


Remarque : Désinfectez/supprimez les jetons de session ou les cookies avant de télécharger le fichier HAR.

Étape 3: Validation et nettoyage du back-end

Ce problème nécessite une intervention du serveur principal et ne peut pas être résolu à partir de l'interface utilisateur seule. L'assistance technique Cisco doit effectuer les actions suivantes :

- Impliquer l'équipe Secure Access backend/SSE Platform
- Valider pour une réservation IP homologue périmée
- Rechercher les objets de tunnel orphelins
- Identifier les clés principales en double liées à la configuration NTG spécifique
- Effacer la référence d'homologue de tunnel obsolète pour l'IP d'origine
- Forcer la resynchronisation principale des objets NTG si nécessaire
- Libérer l'allocation d'homologue IP liée à l'UUID NTG

Étape 4: méthode de résolution alternative

Si le nettoyage du serveur principal n'est pas immédiatement disponible, procédez comme suit :

- Supprimer la configuration principale du groupe de tunnels réseau
- Attendez 5 minutes.
- Ajoutez à nouveau le NTG avec l'adresse IP requise


Mise en garde : Possible. Les détails mentionnés ici semblent contenir des procédures ou des commandes qui pourraient avoir un impact significatif si elles étaient exécutées. Veuillez vous assurer que les procédures ou commandes ci-dessus ont été évaluées par un expert ou une unité commerciale avant de les exécuter ou de les recommander.

Étape 5: Contournement temporaire

Si le NTG est en production et ne peut pas être supprimé :

- Continuer à utiliser le tunnel secondaire pour la connectivité
- Obtenir une adresse IP publique alternative auprès de votre fournisseur/partenaire
- Mettre à jour le primaire NTG pour utiliser l'IP alternative
- Reconnaître la redondance réduite jusqu'à la résolution du problème de back-end

Motif

Ce problème est causé par un bogue logiciel dans le système principal d'accès sécurisé Cisco. Lorsqu'une adresse IP d'homologue primaire est modifiée et rétablie à sa valeur d'origine, le système de validation principal traite incorrectement l'adresse IP d'origine comme étant toujours allouée ou réservée, même si elle devrait être disponible pour une réutilisation. Il en résulte un échec de validation back-end masqué par l'interface utilisateur comme une « erreur interne de serveur » générique. Le système principal ne parvient pas à nettoyer correctement ou à libérer la réservation IP pendant le processus de modification de la configuration, ce qui crée un problème d'état persistant qui empêche l'IP d'être réutilisée dans le même NTG.

Autres informations utiles

- Dépannage et collecte des informations de base pour Cisco Secure Access
- 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.