Accès sécurisé Échec de l'accès aux ressources privées ZTNA RDP pour une ressource spécifique

Table des matières

Problème

Les utilisateurs n'ont pas pu accéder à une ressource privée RDP spécifique via Cisco Secure Access Zero Trust Network Access (ZTNA). Lors de la tentative de connexion, les utilisateurs ont reçu un message d'erreur interne. Le problème a affecté plusieurs utilisateurs, y compris les utilisateurs nouvellement ajoutés, et a empêché les utilisateurs travaillant à domicile d'accéder aux ressources de bureau requises. D'autres ressources RDP et des ressources privées non RDP sont restées accessibles, ce qui indique que le problème était spécifique à cette configuration de ressource particulière.

Environnement

- Accès sécurisé Cisco - ZTNA (Zero Trust Network Access)
- Configuration de ressources privées avec le protocole RDP
- Stratégies d'accès basées sur les groupes Active Directory (AD)
- Configurations de ressources privées multiples avec des adresses IP qui se chevauchent
- Inscription client et évaluation de la position

Résolution

Le problème a été résolu en identifiant et en corrigeant les conflits de configuration dans la configuration des ressources privées. Les étapes décrites dans les sections suivantes ont été

suivies pour résoudre le problème.

Identifier les conflits de configuration

L’enquête a révélé que la ressource RDP spécifique a été configurée sous plusieurs ressources privées : Connectez-vous au Tableau de bord CSA > Connectez-vous > Connectivité de l'utilisateur final > Sous Accès sans approbation > Ajouter un profil ZTA > Donnez-lui un nom, puis recherchez une destination spécifique.

Supprimer les affectations d'adresses IP conflictuelles

L'adresse IP 172.26.106.136 a été supprimée des ressources privées en conflit.

L'adresse IP était laissée uniquement sous la ressource appropriée qui correspondait aux appartenances au groupe Active Directory des utilisateurs et aux exigences de la stratégie d'accès.

Vérifier l'appartenance au groupe utilisateur

Il a été confirmé que les utilisateurs nouvellement ajoutés qui rencontraient des problèmes d'accès n'étaient pas membres du groupe Active Directory (AD) correct requis pour l'accès conformément à la stratégie d'accès configurée.

Assurez-vous également que le groupe AD ou l'utilisateur approprié est associé au profil d'accès sans approbation.

Tester l'accès après les modifications de configuration

Une fois les modifications de configuration implémentées, les utilisateurs ont pu accéder à la ressource RDP comme requis. Il a été confirmé que le problème a été résolu et que les utilisateurs peuvent se connecter sans recevoir le message « Une erreur interne s'est produite ».

Motif

La cause principale du problème était un conflit de configuration où la ressource spécifique était affectée à plusieurs ressources privées avec des stratégies d'accès différentes. Cela a créé une situation où les utilisateurs étaient évalués par rapport à des stratégies pour lesquelles ils n'avaient pas l'appartenance de groupe Active Directory appropriée, ce qui a entraîné des refus d'accès et le message « Une erreur interne s'est produite ». Les utilisateurs nouvellement ajoutés n'étaient pas membres des groupes AD corrects requis pour les stratégies en conflit, ce qui les a empêchés d'accéder à la ressource même s'ils devaient avoir accès via la stratégie appropriée.

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.