

Fonctions de la console d'administration Cisco Secure Access bloquées par le pare-feu

Table des matières

Problème

Plusieurs actions d'administration dans la console Cisco Secure Access ont échoué, empêchant l'administration quotidienne normale de l'environnement Secure Access. Les symptômes spécifiques observés étaient les suivants :

- Impossible de supprimer des périphériques de Ressources → Périphériques itinérants → Systèmes d'exploitation de bureau
- Impossible de récupérer les comptes à partir des comptes Admin → (impossible de récupérer la liste des administrateurs)
- Impossible de renommer les périphériques utilisateur depuis la console
- Impossible d'ajouter des utilisateurs via l'interface administrative
- Impossible de soulever des demandes d'assistance auprès de l'assistance Cisco via la console

Ces défaillances empêchaient l'exécution de tâches administratives essentielles dans l'interface de gestion Cisco Secure Access.

Environnement

- Console Cisco Secure Access
- Environnement réseau avec connectivité sortante restreinte
- Accès administratif au portail de gestion Cisco Secure Access

Résolution

La résolution impliquait d'autoriser les domaines Cisco requis via le pare-feu pour restaurer la connectivité aux services Cisco essentiels.

Étape 1: Identifier les domaines Cisco requis

La cause principale a été identifiée comme la connectivité bloquée aux domaines Cisco requis, en particulier les terminaux *.opendns.com nécessaires aux fonctions d'administration de Cisco Secure Access.

Étape 2: Configurer la liste verte du pare-feu

Ajoutez les domaines Cisco appropriés à la liste de contournement/autorisation du pare-feu :

- Ajoutez *.opendns.com terminaux à la liste d'autorisation du pare-feu
- Assurez-vous que la connectivité sortante vers ces domaines est autorisée
- Configurer le pare-feu pour contourner l'inspection pour ces domaines Cisco approuvés

Étape 3: Valider les fonctions administratives

Après avoir implémenté les modifications du pare-feu, vérifiez que toutes les fonctions administratives sont restaurées :

- Tester la capacité à récupérer la liste des administrateurs à partir des comptes Admin →
- Vérifier la fonctionnalité de suppression des périphériques dans Ressources → Périphériques itinérants → Systèmes d'exploitation de bureau
- Confirmer que les fonctionnalités d'ajout d'utilisateurs fonctionnent
- Fonctionnalité de changement de nom du périphérique test

- Vérifier l'accès à la création des dossiers

À la suite des modifications apportées à la configuration du pare-feu, toutes les fonctions administratives ont commencé à fonctionner comme prévu, sans aucun problème technique.

Motif

Le pare-feu bloquait la connectivité aux domaines Cisco requis, en particulier les terminaux *.opendns.com qui sont essentiels pour les opérations de la console d'administration Cisco Secure Access. Cette connectivité bloquée a empêché la console de communiquer avec les services back-end de Cisco, ce qui a entraîné l'échec de plusieurs fonctions d'administration, notamment la gestion des utilisateurs, la gestion des périphériques et la création de dossiers d'assistance.

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.