Suppression du profil d'accès sans approbation entraînant une perte d'accès utilisateur

Table des matières

Problème

Après la suppression d'un profil ZTA (Zero Trust Access) considéré comme inutilisé, tous les utilisateurs du module ZTNA ont subi une perte totale d'accès aux ressources privées et à la navigation sur Internet. La suppression de ce profil a entraîné une interruption immédiate du service pour tous les utilisateurs ZTNA, les empêchant d'accéder à toutes les ressources via l'infrastructure d'accès réseau Zero Trust.

Les utilisateurs affectés n'ont pas pu établir de connexions à :

- Ressources internes privées
- Navigation Internet via le module ZTNA

Environnement

- Accès sécurisé (accès réseau sans confiance)
- Module ZTNA déployé avec plusieurs profils utilisateur
- Stratégie par défaut configurée avec le contrôle ZTNA
- Plusieurs profils ZTA configurés pour la gestion des accès utilisateur

Résolution

Comprendre la logique de correspondance des profils ZTA

Les profils Zero Trust Access sont appliqués en fonction d'un ordre et d'une logique spécifiques :

- Ordre de correspondance du profil : Les profils ZTA sont évalués dans l'ordre en fonction des critères de correspondance utilisateur et destination
- Comportement du profil par défaut : Lorsqu'aucun profil spécifique ne correspond aux critères d'utilisateur ou de destination, le système revient au profil par défaut
- Dépendances de profil : La suppression d'un profil qui sert de profil par défaut peut entraîner une interruption de service, même s'il semble inutilisé

Le profil supprimé fonctionnait probablement comme profil par défaut effectif pour la correspondance des utilisateurs, bien qu'il apparaisse inutilisé dans l'interface de configuration. Lorsque ce profil a été supprimé, les utilisateurs ont perdu leur chemin d'accès principal via l'infrastructure ZTNA.

Étapes de validation

Pour éviter des problèmes similaires à l'avenir, cette approche de validation doit être mise en oeuvre :

1.- Vérifiez tous les profils ZTA configurés et leurs critères de correspondance avant la suppression.

2.- Identifiez le profil qui sert de valeur par défaut pour l'accès utilisateur.

3.- Vérifiez le mappage utilisateur-profil à l'aide de captures d'écran de configuration et de l'examen des stratégies.

4.- Tester les changements de profil d'une manière contrôlée avant d'appliquer à la production.

Motif

La cause principale était la suppression d'un profil ZTA qui fonctionnait comme profil par défaut effectif pour l'accès utilisateur ZTNA, bien qu'il apparaisse inutilisé dans l'interface de configuration. Lorsque ce profil a été supprimé, le système a perdu les principaux critères de correspondance pour l'accès utilisateur, entraînant la perte de connectivité de tous les utilisateurs ZTNA aux ressources privées et à la navigation sur Internet. La logique de mise en correspondance des profils dépend de la disponibilité d'un profil par défaut valide pour la reprise lorsque des critères utilisateur ou de destination spécifiques ne sont pas satisfaits par d'autres profils configurés.

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.