Restriction d'accès géographique pour l'accès sans confiance et les connexions VPN

Table des matières

Problème

Les entreprises qui ont besoin de restrictions d'accès géographiques pour les connexions ZTA (Zero Trust Access) et VPN peuvent constater que les politiques ZTA et VPN existantes doivent être désactivées lorsqu'elles tentent de mettre en oeuvre des contrôles d'accès basés sur les pays. Les utilisateurs perdent totalement l'accès aux ressources requises lorsque les politiques sont désactivées en raison de l'impossibilité de localiser les options de restriction géographique natives dans l'interface du produit Secure SSE. L'exigence spécifique de restreindre l'accès aux connexions provenant uniquement d'un pays particulier ne peut pas être configurée à l'aide de fonctionnalités intégrées du produit, ce qui entraîne un impact généralisé pour l'utilisateur lorsque les politiques existantes sont désactivées dans une tentative d'implémentation de telles restrictions.

Environnement

- Produit Cisco Secure Access Service Edge (SASE) / Secure SSE
- Mise en oeuvre ZTNA (Zero Trust Access)
- Services VPN nécessitant un contrôle d'accès géographique
- Stratégies d'accès aux ressources privées
- Organisation nécessitant des restrictions d'accès spécifiques au pays

Résolution

Le produit Cisco Secure SSE n'offre pas actuellement de fonctionnalité native permettant de

limiter l'accès aux ressources privées en fonction de l'emplacement géographique ou du pays de l'utilisateur. Les approches décrites dans les sections suivantes peuvent être envisagées pour remédier à cette limitation.

Envoi de demande de fonctionnalité

Une demande de fonctionnalité doit être envoyée à Cisco pour ajouter des fonctionnalités de restriction géographique pour l'accès ZTA et VPN. Cette demande d'amélioration est évaluée par l'équipe produit en vue d'une éventuelle inclusion dans des versions futures. Les entreprises peuvent collaborer avec leur responsable de compte Cisco pour hiérarchiser ces demandes de fonctionnalités en fonction des besoins de l'entreprise.

Considérations de contournement manuel

Une solution manuelle consiste à ajouter des plages d’adresses IP publiques spécifiques à chaque pays en tant que groupes d’objets réseau dans les politiques d’accès.

Étape 1: Obtenez les plages d'adresses IP publiques du pays auprès du registre Internet régional (RIR) approprié.

Étape 2: Créez des groupes d'objets réseau contenant les plages IP identifiées. Configurez les groupes d'objets réseau dans la configuration de la stratégie d'accès pour inclure les plages d'adresses IP spécifiques allouées au pays cible.

Étape 3: Appliquez les groupes d'objets réseau aux stratégies d'accès. Modifiez les stratégies d'accès existantes pour référencer les groupes d'objets réseau créés, limitant ainsi l'accès aux connexions provenant des plages IP spécifiées.

Limites importantes

Cette approche manuelle présente des limites importantes, car elle repose sur des définitions de plages IP statiques et ne peut pas prendre en compte les allocations IP dynamiques, les utilisateurs mobiles ou les services VPN qui pourraient contourner les restrictions géographiques. En outre, cette méthode nécessite une maintenance continue pour garantir la précision de la plage IP.

Gestion temporaire des stratégies

Tant qu'une solution permanente n'est pas disponible, les entreprises doivent éviter de désactiver toutes les politiques ZTA et VPN simultanément. Envisagez plutôt de mettre en oeuvre une approche progressive où les politiques d'accès critiques restent actives pendant que les exigences de restriction géographique sont traitées par d'autres moyens ou en attente d'améliorations du produit.

Motif

L'architecture du produit Cisco Secure SSE ne comprend pas de fonctionnalités natives de contrôle d'accès géographique pour l'accès aux ressources privées. Le cadre de politique d'accès aux produits est conçu autour de l'identité des utilisateurs, de la position des périphériques et des contrôles réseau, mais n'intègre pas l'emplacement géographique comme paramètre d'application de la politique. Il s'agit d'une lacune de capacité du produit plutôt que d'un problème de configuration ou d'un défaut logiciel.

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.