Utilisateurs d'accès distant ne pouvant pas accéder aux services internes sur RAVPN

Table des matières

Problème

Les utilisateurs de l'accès à distance utilisant l'accès sécurisé n'ont pas pu accéder aux services internes, y compris le contrôleur de domaine du siège, tandis que l'accès à Internet a continué à fonctionner normalement. Les utilisateurs ont pu naviguer sur Internet avec succès mais n'ont pas pu accéder aux ressources internes telles que le contrôleur de domaine sur RAVPN (Remote Access VPN).

Environnement

- Accès sécurisé Cisco - Accès à distance sécurisé du client (VPN, position, ressource privée)
- Tunnels RAVPN (Remote Access VPN) signalés comme opérationnels et en bon état
- Infrastructure SD-WAN utilisée
- Serveurs DNS internes au siège
- Services de contrôleur de domaine au siège
- Plusieurs réseaux de filiales connectés via l'infrastructure

Résolution

Les étapes de dépannage et de résolution suivantes ont été effectuées pour résoudre le problème de connectivité de l'accès à distance :

Étape 1: Analyse de capture de paquets

Collectez la capture simultanée de paquets du client et de votre périphérique de périphérie (bidirectionnelle) pour analyser les modèles de flux de trafic.

Flux :

Client VPN RA ----------Accès sécurisé Cisco --------Tunnel IPSec ---------- Périphérique de périphérie ---------Ressource privée

- Vérifiez si les requêtes DNS des clients ont réussi à atteindre le périphérique de périphérie et à être envoyées vers le serveur DNS.
- Vérifiez si aucune réponse DNS n'a été observée en retour du serveur DNS local vers les clients
- Le serveur DNS local envoyait une réponse, mais ces réponses n'ont jamais été renvoyées à l'interface du tunnel.

Étape 2: Identification de la cause première

D’après l’analyse de capture de paquets, le problème a été identifié comme un problème de routage de chemin de retour. L'analyse du trafic a indiqué que, alors que les requêtes DNS atteignaient avec succès le serveur DNS local via l'infrastructure d'accès sécurisé Cisco, le trafic de retour contenant les réponses DNS n'atteignait pas les clients d'accès à distance en raison de problèmes de routage ou de configuration sur votre infrastructure.

Étape 3: Révision et correction de la configuration

Examiner et corriger la configuration du réseau interne et la configuration du réseau interne, en se concentrant plus particulièrement sur :

- Configuration DNS et routage du trafic de retour
- Politiques de routage interne pour le trafic de retour VPN
- Configuration du routage réseau interne

- Éléments de configuration manquants du côté périphérique

Étape 4: Vérification du rétablissement du service

À la suite de la révision et des corrections de la configuration, la fonctionnalité Secure Access a été largement restaurée. La plupart des utilisateurs d'accès à distance ont retrouvé l'accès aux services internes, y compris le contrôleur de domaine du siège.

Motif

La cause principale a été identifiée comme un problème de routage de chemin de retour au sein de l'infrastructure réseau interne. Alors que les requêtes DNS des clients d'accès à distance atteignaient le serveur DNS local via l'infrastructure d'accès sécurisé Cisco, le trafic de retour contenant les réponses DNS n'était pas correctement routé vers les clients. Cela est dû à une configuration manquante ou incorrecte du côté de l'infrastructure réseau interne qui a empêché les réponses DNS et TCP d'atteindre les clients d'accès à distance via la connexion VPN.

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.