Demandes DNS excessives sur le port 53 pendant les sessions VPN AnyConnect

Table des matières

Problème

Après la mise en oeuvre du VPN d'accès à distance (RA-VPN), les utilisateurs se connectant via Cisco AnyConnect génèrent des dizaines de requêtes DNS sur le port 53 vers le serveur DNS secondaire. Ce comportement est observé dans le Moniteur d'activité pour tous les utilisateurs connectés au tunnel VPN et entraîne l'inondation du tunnel par de nombreuses requêtes autorisées. Cette activité DNS excessive ne se produit pas lorsque les utilisateurs se connectent via ZTA (Zero Trust Access), ce qui indique que le problème est spécifiquement lié à la méthode de connexion VPN AnyConnect.

Environnement

- Gamme de produits : Accès sécurisé
- Mise en oeuvre : Déploiement VPN d'accès à distance
- Environnement de comparaison : ZTA (Zero Trust Access) : comportement d'inondation DNS différent

Résolution

L'analyse des demandes DNS excessives nécessite la collecte et l'analyse de journaux pour identifier la cause première du comportement de diffusion DNS. La collecte de journaux comprend la collecte de la capture de paquets qui inclut le PID pour chaque paquet afin de déterminer quelle application sur un point d'extrémité génère le trafic et la sortie du Moniteur de processus.

Motif

L’analyse a montré que cette quantité de trafic DNS est attendue.

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.