Fluctuation intermittente du groupe de tunnels réseau d'accès sécurisé avec Azure VPN Gateway pendant les événements de nouvelle clé IKE

Table des matières

Problème

Un groupe de tunnels réseau nouvellement configuré entre Cisco Secure Access et Azure VPN Gateway subit des battements de tunnel intermittents environ toutes les 4 heures pendant les événements de nouvelle clé IKE.

Les messages d'erreur et les symptômes suivants sont observés :

- Homologue BGP désactivé, temporisateur d'attente expiré
- Alerte : échec de la nouvelle clé IKE
- Tunnel IKE déconnecté

Le battement de tunnel entraîne des interruptions périodiques, des échecs de réattribution de clé IKE, des échecs de vérification d'intégrité, des déconnexions de tunnel et des abandons d'appairage BGP, ce qui a un impact sur la connectivité stable aux ressources Azure. Les échecs d'authentification sont observés lors des négociations de nouvelle clé.

Environnement

- Groupe de tunnels réseau Cisco Secure Access (CSA) configuré pour Azure VPN Gateway
- Tunnels VPN site à site IPsec utilisant IKEv2
- Passerelle VPN Azure avec cryptage AES-GCM-256 configuré dans les stratégies de mode

principal (MM)

- NAT-T (NAT Traversal) activé des deux côtés via le port 4500
- Homologation BGP configurée entre les points de terminaison
- Durée de vie de la SA IKE par défaut de 4 heures (28800 secondes)
- Configuration initiale de la durée de vie de SA IPsec, modifiée ultérieurement à 10800 secondes
- PFS (Perfect Forward Secrecy) non activé côté Azure

Résolution

Le problème a été résolu par une modification de la configuration afin d'éviter les chiffrements AES-GCM dans les stratégies de mode principal, en fonction de l'identification d'un bogue dans la passerelle VPN Azure.

Étape 1: Analyse de débogage Azure VPN Gateway

Des débogages IKE ont été collectés du côté de la passerelle VPN Azure, révélant ce comportement lors des tentatives de nouvelle clé :

```
SESSION_ID :{} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

Étape 2: Identification de la cause première

Le support Azure a enquêté sur les échecs de nouvelle clé. L'analyse Azure a identifié que lorsqu'Azure lance une MM-REKEY à l'aide d'AES-GCM-256, le paquet de nouvelle clé est mal formé. Le périphérique local ne répond pas à la demande de nouvelle clé mal formée, ce qui entraîne la déconnexion du tunnel.

Étape 3: Configuration Solution de contournement Implémentation

Sur la base des recommandations d'Azure, cette atténuation a été mise en oeuvre :

- Supprimez les chiffrements AES-GCM des stratégies de mode principal (MM) dans la configuration du groupe de tunnels réseau.
- Configurez d'autres méthodes de cryptage qui n'utilisent pas le mode GCM.

Reportez-vous à l'étape 17 de https://securitydocs.cisco.com/docs/csa/olh/121327.dita.

Étape 4: Autres options d'atténuation

Azure a également fourni des stratégies d'atténuation supplémentaires qui peuvent être prises en compte :

- Configurez une durée de vie MM sur site supérieure à 28800 secondes afin qu'Azure lance toujours une nouvelle clé.
- Définissez Azure VPN Gateway en mode répondeur uniquement avec une durée de vie SA locale inférieure à la durée de vie d'Azure.

Motif

La cause principale est un bogue dans la passerelle VPN Azure qui affecte les opérations de renouvellement de clé AES-GCM. Lorsqu'Azure lance une requête MM-REKEY à l'aide d'AES-GCM-256, le paquet de nouvelle clé est mal formé, ce qui empêche le périphérique Cisco Secure Access sur site de répondre à la requête de nouvelle clé mal formée. Il en résulte des échecs de renouvellement de clé IKE, des erreurs d'authentification et des déconnexions de tunnel ultérieures.

Azure a confirmé qu'il s'agissait d'un bogue existant et a documenté un correctif planifié dans une future version de passerelle prévue pour la mi-2026.

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.