

Secure Access Network Tunnel Group Intermittent Flapping met Azure VPN Gateway tijdens IKE Rekey-evenementen

Inhoud

uitgifte

Een nieuw geconfigureerde Network Tunnel Group tussen Cisco Secure Access en Azure VPN Gateway ervaart een intermitterende tunnel die ongeveer elke 4 uur fladdert tijdens IKE rekey-evenementen.

Deze specifieke foutmeldingen en symptomen worden waargenomen:

- BGP peering down, Hold timer verlopen
- Dringend bericht: IKE-sleutel is mislukt
- IKE-tunnel losgekoppeld

Het klappen van de tunnel resulteert in periodieke verstoringen, IKE-rekey-storingen, integriteitscontrolefouten, tunnelonderbrekingen en BGP-peering-druppels, wat een invloed heeft op de stabiele connectiviteit met Azure-bronnen. Authenticatiefouten worden waargenomen tijdens herkansingsonderhandelingen.

milieu

- Cisco Secure Access (CSA) Network Tunnel Group geconfigureerd voor Azure VPN Gateway
- IPsec Site-to-Site VPN-tunnels met IKEv2
- Azure VPN Gateway met AES-GCM-256-codering geconfigureerd in hoofdmodus (MM)-beleid

- NAT-T (NAT Traversal) ingeschakeld aan beide zijden met poort 4500
- BGP peering geconfigureerd tussen eindpunten
- Standaard Ikesa levensduur van 4 uur (28800 seconden)
- Initiële IPsec SA levenslange configuratie, later gewijzigd naar 10800 seconden
- PFS (Perfect Forward Secrecy) niet ingeschakeld aan Azure-zijde

resolutie

Het probleem is opgelost door een configuratiewijziging om AES-GCM-cijfers in het hoofdmodebeleid te vermijden, op basis van de identificatie van een bug in de Azure VPN Gateway.

Stap 1: Azure VPN Gateway Debug Analysis

IKE debugs werden verzameld van de Azure VPN Gateway kant, onthullen dit gedrag tijdens rekey pogingen:

```
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
```

Stap 2: Identificatie van de onderliggende oorzaak

Azure-ondersteuning onderzocht de rekey-fouten. De Azure-analyse identificeerde dat wanneer Azure een MM-REKEY initieert met AES-GCM-256, het rekey-pakket misvormd is. Het on-premise apparaat reageert niet op het foutieve rekey-verzoek, wat leidt tot het verbreken van de tunnel.

Stap 3: Implementatie van de configuratieworkaround

Op basis van aanbevelingen van Azure werd deze beperking geïmplementeerd:

- Verwijder AES-GCM-coderingen uit het MM-beleid (hoofdmodus) in de configuratie van de netwerktunnelgroep.
- Configureer alternatieve coderingsmethoden die geen GCM-modus gebruiken.

Zie stap 17 in <https://securitydocs.cisco.com/docs/csa/olh/121327.dita>.

Stap 4: Alternatieve mitigatiemogelijkheden

Azure bood ook aanvullende mitigatiestrategieën die kunnen worden overwogen:

- Configureer on-premises MM lifetime voor meer dan 28800 seconden, zodat Azure altijd rekey initieert.
- Stel Azure VPN Gateway in op de modus voor alleen responders met een on-site SA-levensduur die kleiner is dan de levensduur van Azure.

Oorzaak

De hoofdoorzaak is een bug in de Azure VPN Gateway die van invloed is op AES-GCM rekey-bewerkingen. Wanneer Azure een MM-REKEY initieert met AES-GCM-256, is het rekey-pakket misvormd, waardoor het Cisco Secure Access-apparaat op locatie niet reageert op het misvormde rekey-verzoek. Dit resulteert in IKE rekey-fouten, verificatiefouten en daaropvolgende tunnelonderbrekingen.

Azure heeft dit bevestigd als een bestaande bug en heeft een geplande oplossing gedocumenteerd in een toekomstige gateway-release die is bedoeld voor medio 2026.

Gerelateerde inhoud

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.