Secure Access Network Tunnel Group Intermittent Flapping with Azure VPN Gateway During IKE Rekey Events

Contents

Issue

A newly configured Network Tunnel Group between Cisco Secure Access and Azure VPN Gateway experiences intermittent tunnel flapping approximately every 4 hours during IKE rekey events.

This specific error messages and symptoms are observed:

- BGP peering down, Hold timer expired
- Alert: failed IKE rekey
- IKE tunnel disconnected

The tunnel flapping results in periodic disruptions, IKE rekey failures, integrity check failures, tunnel disconnects, and BGP peering drops, impacting stable connectivity to Azure resources. Authentication failures are observed during rekey negotiations.

Environment

- Cisco Secure Access (CSA) Network Tunnel Group configured to Azure VPN Gateway
- IPsec Site-to-Site VPN tunnels using IKEv2
- Azure VPN Gateway with AES-GCM-256 encryption configured in Main Mode (MM) policies
- NAT-T (NAT Traversal) enabled on both sides using port 4500
- BGP peering configured between endpoints
- Default IKE SA lifetime of 4 hours (28800 seconds)
- Initial IPsec SA lifetime configuration, later modified to 10800 seconds

- PFS (Perfect Forward Secrecy) not enabled on Azure side

Resolution

The issue was resolved through a configuration change to avoid AES-GCM ciphers in Main Mode policies, based on the identification of a bug in the Azure VPN Gateway.

Step 1: Azure VPN Gateway Debug Analysis

IKE debugs were collected from the Azure VPN Gateway side, revealing this behavior during rekey attempts:

```
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
```

Step 2: Root Cause Identification

Azure support investigated the rekey failures. The Azure analysis identified that when Azure initiates an MM-REKEY using AES-GCM-256, the rekey packet is malformed. The on-premises device does not reply to the malformed rekey request, resulting in tunnel disconnection.

Step 3: Configuration Workaround Implementation

Based on recommendations of Azure, this mitigation was implemented:

- Remove AES-GCM ciphers from Main Mode (MM) policies in the Network Tunnel Group configuration.
- Configure alternative encryption methods that do not use GCM mode.

Refer to Step 17 in https://securitydocs.cisco.com/docs/csa/olh/121327.dita.

Step 4: Alternative Mitigation Options

Azure also provided additional mitigation strategies that can be considered:

- Configure on-premises MM lifetime to be greater than 28800 seconds so Azure always initiates rekey.
- Set Azure VPN Gateway to responder-only mode with on-premises SA lifetime smaller than lifetime of Azure.

Cause

The root cause is a bug in the Azure VPN Gateway that affects AES-GCM rekey operations. When Azure initiates an MM-REKEY using AES-GCM-256, the rekey packet is malformed, causing the on-premises Cisco Secure Access device to not respond to the malformed rekey request. This results in IKE rekey failures, authentication errors, and subsequent tunnel disconnections.

Azure has confirmed this as an existing bug and documented a planned fix in a future gateway release targeted for Mid-2026.

Related Content

- Cisco Technical Support & Downloads