Intermittierendes Flapping der Tunnelgruppe des sicheren Zugriffs mit dem Azure VPN-Gateway während IKE-Rekey-Ereignissen

Inhalt

Problem

Bei einer neu konfigurierten Netzwerk-Tunnelgruppe zwischen Cisco Secure Access und Azure VPN Gateway treten bei IKE-Schlüsselereignissen etwa alle vier Stunden unterbrochene Tunnelflapping-Ereignisse auf.

Diese spezifischen Fehlermeldungen und Symptome wurden beobachtet:

- BGP-Peer-Down, Hold-Timer abgelaufen
- Warnung: Fehlgeschlagener IKE-Schlüssel
- IKE-Tunnel getrennt

Das Flapping des Tunnels führt zu regelmäßigen Unterbrechungen, IKE-Schlüsselfehlern, Integritätsprüfungsfehlern, Tunneltrennungen und BGP-Peering-Drops, was sich auf die stabile Verbindung mit Azure-Ressourcen auswirkt. Authentifizierungsfehler werden während der Schlüsselverhandlung festgestellt.

Umwelt

- Cisco Secure Access (CSA) Network Tunnel Group für Azure VPN-Gateway konfiguriert
- IPsec-Site-to-Site-VPN-Tunnel mit IKEv2
- Azure VPN-Gateway mit AES-GCM-256-Verschlüsselung, konfiguriert in Richtlinien für den Hauptmodus (MM)

- NAT-T (NAT Traversal) auf beiden Seiten über Port 4500 aktiviert
- Konfiguration von BGP-Peering zwischen Endpunkten
- IKE SA-Standardlebensdauer von 4 Stunden (28800 Sekunden)
- Erstkonfiguration der IPsec-SA-Lebensdauer, später auf 10800 Sekunden geändert
- PFS (Perfect Forward Secrecy) auf Azure-Seite nicht aktiviert

Auflösung

Das Problem wurde durch eine Konfigurationsänderung behoben, um AES-GCM-Verschlüsselungen in Richtlinien für den Hauptmodus zu vermeiden, die auf der Identifizierung eines Fehlers im Azure VPN-Gateway basieren.

Schritt 1: Azure VPN-Gateway-Fehleranalyse

IKE-Debugging-Vorgänge wurden auf der Seite des Azure VPN-Gateways gesammelt, um dieses Verhalten bei erneuten Schlüsselversuchen aufzudecken:

```
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
```

Phase 2: Ursachenidentifizierung

Die Azure-Unterstützung hat die erneuten Schlüsselfehler untersucht. Die Azure-Analyse hat festgestellt, dass das rekey-Paket fehlerhaft ist, wenn Azure einen MM-REKEY mit AES-GCM-256 initiiert. Das Gerät am Standort antwortet nicht auf die fehlerhafte Schlüsselanforderung, was zur Trennung des Tunnels führt.

Schritt 3: Implementierung von Configuration Workaround

Auf der Grundlage der Empfehlungen von Azure wurde diese Eindämmung implementiert:

- Entfernen Sie AES-GCM-Verschlüsselungen aus den MM-Richtlinien (Main Mode) in der Konfiguration der Netzwerk-Tunnelgruppe.
- Konfigurieren Sie alternative Verschlüsselungsmethoden, die den GCM-Modus nicht verwenden.

Weitere Informationen finden Sie unter Schritt 17 in https://securitydocs.cisco.com/docs/csa/olh/121327.dita.

Schritt 4: Optionen zur alternativen Risikominimierung

Azure bot außerdem weitere Strategien zur Risikominimierung an, die in Betracht gezogen werden können:

- Konfigurieren Sie die standortbasierte MM-Lebensdauer auf mehr als 28800 Sekunden, damit Azure immer den Schlüssel erneut initiiert.
- Legen Sie für das Azure VPN-Gateway den Antwortmodus fest, wobei die standortbasierte SA-Lebensdauer kürzer ist als die Lebensdauer von Azure.

Ursache

Die Ursache liegt in einem Fehler im Azure VPN Gateway, der sich auf die AES-GCM-Schlüsselvorgänge auswirkt. Wenn Azure einen MM-REKEY mit AES-GCM-256 initiiert, ist das rekey-Paket fehlerhaft, sodass das Cisco Secure Access-Gerät vor Ort nicht auf die fehlerhaft geformte rekey-Anforderung antwortet. Dies führt zu IKE-Neuschlüsselfehlern, Authentifizierungsfehlern und nachfolgenden Tunneltrennungen.

Azure hat dies als bestehenden Fehler bestätigt und einen geplanten Fix in einer zukünftigen Gateway-Version dokumentiert, die für Mitte 2026 geplant ist.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.