

IKE 키 재설정 이벤트 중에 Azure VPN 게이트웨이로 보안 액세스 네트워크 터널 그룹 간헐적 플래핑 발생

목차

문제

Cisco Secure Access와 Azure VPN Gateway 간에 새로 구성된 네트워크 터널 그룹은 IKE 키 재설정 이벤트 중에 약 4시간마다 간헐적인 터널 플래핑을 경험합니다.

다음과 같은 특정 오류 메시지 및 증상이 관찰됩니다.

- BGP 피어링 중단, 보류 타이머 만료
- 경고: 실패한 IKE rekey
- IKE 터널 연결 끊김

터널 플래핑은 IKE rekey 실패, 무결성 검사 실패, 터널 연결 끊김, BGP 피어링 삭제 등 정기적인 중단을 초래하여 Azure 리소스에 대한 안정적인 연결에 영향을 줍니다. 인증 실패는 키 재설정 협상 중에 관찰됩니다.

환경

- Azure VPN 게이트웨이에 구성된 CSA(Cisco Secure Access) 네트워크 터널 그룹
- IKEv2를 사용하는 IPsec Site-to-Site VPN 터널
- AES-GCM-256 암호화가 주 모드(MM) 정책에 구성된 Azure VPN 게이트웨이
- 포트 4500을 사용하여 양쪽에서 NAT-T(NAT Traversal) 활성화
- 엔드포인트 간에 구성된 BGP 피어링

- 기본 IKE SA 수명은 4시간(28800초)
- 초기 IPsec SA 수명 컨피그레이션, 나중에 10800초로 수정
- PFS(Perfect Forward Secrecy)가 Azure 측에서 사용되지 않음

해결

Azure VPN 게이트웨이의 버그 식별에 따라 기본 모드 정책에서 AES-GCM 암호를 사용하지 않도록 구성 변경을 통해 문제가 해결되었습니다.

1단계: Azure VPN 게이트웨이 디버그 분석

IKE 디버그는 Azure VPN Gateway 측에서 수집되었으며, 키 재설정 시도 중에 이 동작이 드러났습니다.

```
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
```

2단계: 근본 원인 식별

Azure 지원에서 키 재설정 실패를 조사했습니다. Azure 분석에서는 Azure가 AES-GCM-256을 사용하여 MM-REKEY를 시작할 때 rekey 패킷의 형식이 잘못되었음을 확인했습니다. 온-프레미스 디바이스가 잘못된 형식의 rekey 요청에 응답하지 않아 터널 연결이 끊어집니다.

3단계: 컨피그레이션 해결 방법 구현

Azure의 권장 사항을 기반으로 이 완화 기능이 구현되었습니다.

- 네트워크 터널 그룹 컨피그레이션의 주 모드(MM) 정책에서 AES-GCM 암호를 제거합니다.

- GCM 모드를 사용하지 않는 대체 암호화 방법을 구성합니다.

<https://securitydocs.cisco.com/docs/csa/olh/121327.dita>의 17단계를 [참조하십시오](#).

4단계: 대체 완화 옵션

또한 Azure는 다음과 같은 추가 완화 전략을 제공했습니다.

- Azure에서 항상 키 재설정을 시작하도록 온-프레미스 MM 수명을 28800초보다 길게 구성합니다.
- 온-프레미스 SA 수명이 Azure 수명보다 작은 응답자 전용 모드로 Azure VPN 게이트웨이를 설정합니다.

원인

근본 원인은 AES-GCM rekey 작업에 영향을 주는 Azure VPN 게이트웨이의 버그입니다. Azure가 AES-GCM-256을 사용하여 MM-REKEY를 시작하면 rekey 패킷의 형식이 잘못되어 온-프레미스 Cisco Secure Access 장치가 잘못된 형식의 rekey 요청에 응답하지 않습니다. 이로 인해 IKE rekey 실패, 인증 오류 및 후속 터널 연결이 끊깁니다.

Azure는 이 버그를 기존 버그로 확인했으며 2026년 중반을 목표로 하는 향후 게이트웨이 릴리스에서 계획된 수정을 문서화했습니다.

관련 콘텐츠

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.