

Azure/AWS에서 호스팅되는 Secure Access와 C8000Vs 사이에서 IPsec 터널이 플랩합니다.

목차

문제

C8000V/Cisco IOS-XE 라우터와 us-east-2 지역의 Cisco Secure Access 네트워크 간의 IPsec 네트워크 터널이 펄럭이고 있습니다.

모든 터널 그룹이 영향을 받아 온프레미스 라우터와 Cisco Secure Access 네트워크 간에 터널이 다운됩니다.

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스 - 네트워크 터널(IPSEC, 사이트 간, 개인 리소스)
- 제품군: SECACS
- 라우터: C8000V/Cisco IOS-XE 라우터(온프레미스)
- 원격 엔드포인트: Cisco Secure Access 네트워크(미국 동부 2개 지역)
- 소프트웨어 버전: 지정되지 않음
- 오류 메시지, 로그, 디버깅
- 운영 중단 중에 영향을 받는 최종 사용자 없음

해결

CNHE Splunk 로그에서

포트 = 1409

sourceIpAddr = x.x.x.x

포트 = 1408

sourceIpAddr = x.x.x.x

1. 원격 엔드포인트 변경이 감지되었습니다(포트가 업데이트됨).
2. 이 업데이트에 대한 자식 키 다시 걸기
3. 새 포트를 사용하는 rekeys에서 클라이언트에서 응답하지 않으므로 cortex는 재시도를 취소하고 터널을 종료합니다
4. 터널이 가동되는 새 포트를 사용하여 클라이언트를 재가동한 직후

CSA Splunk 로그에서

2026-02-02T16:36:02.188+00:00 로컬 IP를 사용하는 ike 업데이트에 대해 자식 rekey를 트리거합니다. x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00 retransmit 1 of request with message ID 0

2026-02-02T16:36:08.207+00:00 재전송 2 메시지 ID 0의 요청

2026-02-02T16:36:16.207+00:00 재전송 요청 3 메시지 ID 0

2026-02-02T16:36:32.207+00:00 retransmit 4 of request with message ID 0

2026-02-02T16:37:04.207+00:00 retransmit 5 of request with message ID 0

2026-02-02T16:38:08.208+00:00 재전송 5회 후 포기

2026-02-02T16:38:08.208+00:00 종료 IKE, 하위 SA 키 다시 입력 실패

디버그 로그 1769305781091_vJY_CENTRAL_R2.log에서 다음을 수행합니다.

잘못된 SPI 오류 - 매우 자주 발생:

*1월 24일 07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC 패킷에 destaddr=x.x.x.x port=50, spi=, srcaddr=x.x.x.x, input interface=Tunnel12에 대한 잘못된 spi가 있습니다.

*1월 24일 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC 패킷에 destaddr=x.x.x.x, port=50, spi=, srcaddr=x.x.x.x, input interface=Tunnel11에 대한 잘못된 spi가 있습니다.

Tunnel Flapping(터널 플래핑) - 여러 터널 인스턴스가 작동/중단됨:

*1월 24일 08:33:12.069: %LINEPROTO-5-UPDOWN: 인터페이스 터널12의 라인 프로토콜에서 상태가 down으로 변경되었습니다.

*1월 24일 08:33:14.459: %LINEPROTO-5-UPDOWN: 인터페이스 터널11의 라인 프로토콜에서 상태가 down으로 변경되었습니다.

*1월 24일 08:33:15.275: %LINEPROTO-5-UPDOWN: 인터페이스 터널11의 라인 프로토콜에서 상태가 up으로 변경되었습니다.

원인

포트가 펄럭이는 경우 클라이언트 문제가 불안정해지는 것 같습니다.

Azure에서 변경 후 플래핑이 현재로서는 안정적인 것 같습니다.

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.