Nexus 9000 스위치에서 MACSec MKA PDU 무결성 검사 오류 해결

목차

문제

Nexus 9000 스위치 간에 구성된 MACSec(Media Access Control Security)는 MACsec MKA(Key Agreement) 세션을 "secure"로 표시하지만 약 2초마다 반복되는 오류 메시지를 생성합니다. 다음 패턴은 시스템 로그를 플러딩합니다.

```
device# %CTS-5-CTS_MKPDU_ICV_SUCCESS: MACSec: MKPDU verified. Primary keys match for Interface
device# %CTS-4-CTS_MKPDU_ICV_FAILURE: MACSec: MKA PDU integrity check failed for Interface
```

이러한 성공 및 실패 메시지가 번갈아 표시되면서 MACSec 기능을 유지하면서 수정해야 하는 과도한 로그 항목이 생성됩니다.

환경

- 제품: Cisco Nexus 스위치
- 기술: MACSec(Link Encryption)

해결

이 문제를 해결하려면 기본 키 체인에 구성된 것과 다른 키 ID를 사용하도록 대체 키 체인 컨피그레이션을 수정합니다.

1. 기존 MACSec 키 체인 컨피그레이션을 검토하여 이 명령으로 기본 및 대체 키 체인 간에 일치하

는 키 ID를 식별합니다.

```
device# show running-configuration
...
key chain primary macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
key chain fallback macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
...
```

2. 이러한 명령에서 다른 키 ID를 사용하도록 대체 키 체인을 변경합니다. 예를 들어 기본 키 체인이 키 ID 01을 사용하는 경우 대신 키 ID 10을 사용하도록 대체 키 체인을 구성합니다.

```
device# configure terminal
device(config)# key chain fallback macsec
device(config)# no key 01
device(config)# key 10
device(config)# key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
```

3. 시스템 로그를 모니터링하여 CTS_MKPDU_ICV_SUCCESS 및 CTS_MKPDU_ICV_FAILURE 대체 메시지가 더 이상 나타나지 않음을 확인합니다.

원인

근본 원인은 폴백 키 체인이 기본 키 체인과 동일한 키 ID를 사용하는 컨피그레이션 충돌입니다. 이렇게 하면 MKA 프로토콜에서 모호성이 생성되므로, 기본 키와 폴백 키를 평가하는 사이에서 시스템이 전환될 때 무결성 검사가 성공하고 실패합니다. Nexus MACSec 컨피그레이션 가이드에서 이러한 충돌을 방지하기 위해 "폴백 키 ID는 기본 키 체인의 어떤 키 ID와도 일치하지 않아야 합니다."라고 설명합니다.

관련 콘텐츠

- Nexus MACSec 컨피그레이션 가이드
- 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.