

MACSec XPN 트래픽이 Catalyst 9500과 Nexus 9000 사이에서 실패하고 유효하지 않은 패킷 및 FCS 오류가 증가함

목차

문제

Catalyst 9500-28C8D와 Nexus N9K-C93180YC-FX 사이에서 MACSec XPN이 활성화되면 MKA 세션이 성공적으로 설정되지만 링크를 통과하는 데이터 트래픽은 없습니다. Catalyst 9500은 물리적 인터페이스에서 SA 통계 및 FCS 입력 오류 아래에 증가하는 "Notvalid pkt"를 보고합니다. 특히 다음과 같은 증상이 관찰되었습니다.

- MACSec이 활성화된 후 연결 없음
- MKA 세션은 설정된 것으로 표시되지만 Catalyst 9500 측은 "Notvalid pkts 118"이 증가하고 "Valid pkts: 0"
- Catalyst 9500 물리적 인터페이스에서 FCS 입력 오류 증가
- MACSec 컨피그레이션을 제거하면 연결이 즉시 복원되고 FCS 오류가 중지됩니다

MKA 세션은 두 디바이스에서 설정되었으며 GCM-AES-XPB-256 암호를 성공적으로 협상했습니다. Nexus 측에서 암호화를 활성으로 표시했지만 Catalyst 9500이 암호화된 패킷을 수신하고 검증 불일치로 인해 거부하여 유효한 패킷이 0개 수락되었습니다.

환경

- Cisco IOS®를 실행하는 Catalyst 9500-28C8D
- Nexus N9K-C93180YC-F
- GCM-AES-XPB-256 암호 그룹을 사용하는 MACSec XPN 컨피그레이션
- 400기가비트 이더넷 인터페이스(Catalyst의 경우 FourHundredGigE1/0/15, Nexus의 경우

Ethernet1/52)

- Catalyst 9500이 키 서버 우선순위 1로 구성되고 Nexus가 키 서버 우선순위 100으로 구성됨
- 사전 공유 키용 AES-256-CMAC 암호화 알고리즘

해결

장치 간의 키 서버 역할 할당을 변경하는 해결 방법을 구현하여 문제를 해결했습니다. 권장되는 해결 방법은 다음과 같습니다.

1단계: 키-서버 컨피그레이션 문제 식별

두 디바이스에서 현재 키-서버 우선순위 컨피그레이션을 확인합니다. 문제가 있는 컨피그레이션은 다음과 같이 나타났습니다.

Catalyst 9500 구성:

```
mka policy MEHEALTH-ORG-XPN
key-server priority 1
macsec-cipher-suite gcm-aes-xpn-256
```

Nexus 구성:

```
macsec policy MEHEALTH-ORG-XPN
key-server-priority 100
```

2단계: 주요 서버 역할 해결 방법 구현

Nexus 디바이스를 Catalyst 9500 대신 MACSec 키 서버로 구성합니다. 여기에는 Nexus가 키 서버 역할을 수행하도록 키 서버 우선순위 값을 조정하는 것이 포함됩니다.

Nexus 컨피그레이션을 낮은 키-서버 우선순위 값으로 수정합니다(낮은 값의 우선순위가 더 높음).

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 1
```

Catalyst 9500 컨피그레이션을 더 높은 키-서버 우선순위 값으로 수정합니다.

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 100
  macsec-cipher-suite gcm-aes-xpn-256
```

3단계: MACSec 작업 확인

키-서버 역할 변경을 구현한 후 다음을 확인합니다.

- MKA 세션이 두 디바이스 모두에서 성공적으로 설정됨
- 데이터 트래픽이 MACSec 지원 링크를 통해 전달됨
- Catalyst 9500 SA 통계에서 "유효하지 않은 패킷"이 증가하지 않습니다.
- FCS 입력 오류가 물리적 인터페이스에서 발생하지 않음

이 방법을 사용하면 플랫폼 조사 및 소프트웨어 업그레이드 계획을 완료할 때까지 MACSec XPN 컨피그레이션이 제대로 작동할 수 있습니다.

원인

이 문제의 근본 원인은 Cisco 버그 ID CSCvs00410과 관련이 있습니다. 이 시나리오에서는 Nexus 디바이스와의 특정 상호 운용성 조건에서 키 서버 역할의 Catalyst 9500에서 AES-256-XPN을 사용할 때 MKA 세션이 성공적으로 설정되지만 데이터가 링크를 통과할 수 없는 시나리오를 설명합니다. 이 동작은 Catalyst 9500이 Nexus에서 암호화된 패킷을 거부하는 검증 불일치로 나타나며, 이로 인해 잘못된 패킷 수와 FCS 오류가 증가합니다. Cisco IOS가 이 결함에 대해 고정된 것으로 표시된 것과 관련하여 불일치가 발생하여 Catalyst 플랫폼 팀의 추가 조사가 필요합니다.

관련 콘텐츠

- Cisco Bug ID CSCvs00410 - MKA 세션이 작동하지만 Catalyst 9500 키 서버 역할의 AES-256-XPN을 사용하는 경우 링크를 통해 데이터를 전달할 수 없습니다.

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.