# IPsec %RECVD_PKT_INV_SPI 오류 및 잘못된 SPI 복구 기능 정보

## 목차



## 소개

이 문서에서는 피어 디바이스 간에 SA(Security Associations)가 동기화되지 않은 경우 IPsec 문제를 설명합니다.

## 문제

가장 일반적인 IPsec 문제 중 하나는 SA가 피어 디바이스 간에 동기화되지 않을 수 있다는 것입니다.그 결과, 암호화 디바이스는 피어가 모르는 SA로 트래픽을 암호화합니다.이러한 패킷은 피어에서 삭제되며 이 메시지는 syslog에 나타납니다.

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=20.1.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> **참고:**NAT-T를 사용하면 Cisco 버그 ID CSCsq59183이 수정될 때까지 RECVD_**PKT_INV_SPI** 메시지가 올바르게 보고되지 않았습니다.(IPsec은 NAT-T**를 사용하여 RECVD_PKT_INV_SPI** 메시지를 보고하지 않습니다.)

> **참고:**Cisco ASR(Aggregation Services Router) 플랫폼에서 %CRYPTO**-4-RECVD_PKT_INV_SPI** 메시지는 Cisco IOS® XE 릴리스 2.3.2(12.2(33)XNC2)가 구현될 때까지 구현되지 않았습니다. 또한 ASR 플랫폼에서는 다음 예에서와 같이 이 특정 삭제가 전역 QFP(Quantum Flow Processor) 드롭 카운터와 IPsec 기능 드롭 카운터에 모두 등록됩니다.

```
Router# show platform hardware qfp active statistics drop | inc Ipsec
IpsecDenyDrop 0 0
IpsecIkeIndicate 0 0
IpsecInput 0 0 <======
IpsecInvalidSa 0 0
IpsecOutput 0 0
IpsecTailDrop 0 0
IpsecTedIndicate 0 0

Router# show platform hardware qfp active feature ipsec datapath drops all | in SPI
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
```

```
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Cisco IOS에서는 이 특정 메시지가 분명한 보안 이유로 분당 1회 속도로 제한된다는 점에 유의해야 합니다.특정 흐름(SRC, DST 또는 SPI)에 대한 이 메시지가 로그에 한 번만 나타나면 IPsec rekey와 동시에 나타나는 일시적인 조건일 수 있습니다. 이 상태는 피어 디바이스가 동일한 SA를 사용할 준비가 되지 않은 상태에서 한 피어가 새 SA를 사용하기 시작할 수 있습니다.이는 일시적이며 일부 패킷에만 영향을 주기 때문에 일반적으로 문제가 아닙니다.그러나 문제가 될 수 있는 버그가 있습니다.

> **팁**:예를 보려면 Cisco 버그 ID CSCsl68327(키 재설정 중 패킷 손실), Cisco 버그 ID CSCtr14840(ASR:특정 조건에서 2단계 재키 중에 패킷이 삭제되거나 Cisco 버그 ID CSCty30063(ASR은 QM이 완료되기 전에 새 SPI를 사용)

또는 동일한 메시지에 대해 동일한 SPI를 동일한 플로우에 대해 둘 이상의 인스턴스가 보고되는 경우 다음과 같은 문제가 발생합니다.

```
Sep  2 13:36:47.287: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=20.1.1.2, prot=50, spi=0x1DB73BBB(498547643),
srcaddr=10.1.1.1 Sep 2 13:37:48.039: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=20.1.1.2, prot=50, spi=0x1DB73BBB(498547643),
srcaddr=10.1.1.1
```

이는 트래픽이 블랙홀이며 SA가 전송 디바이스에서 만료되거나 DPD(Dead Peer Detection)가 활성화될 때까지 복구되지 않을 수 있음을 나타냅니다.

# 솔루션

이 섹션에서는 이전 섹션에서 설명한 문제를 해결하기 위해 사용할 수 있는 정보를 제공합니다.

## 잘못된 SPI 복구

이 문제를 해결하려면 잘못된 SPI 복구 기능을 활성화하는 것이 좋습니다.예를 들어 crypto isakmp invalid-**spi-recovery** 명령을 입력합니다.다음은 이 명령의 사용에 대해 설명하는 몇 가지 중요한 참고 사항입니다.

- 첫째, 잘못된 SPI 복구는 SA가 동기화되지 않은 경우에만 복구 메커니즘 역할을 합니다.이 경우 이 상태로부터 복구하는 데 도움이 되지만, SA가 처음부터 동기화되지 않은 근본 문제는 다루지 않습니다.근본 원인을 더 잘 이해하려면 두 터널 엔드포인트 모두에서 ISAKMP 및 IPsec 디버그를 활성화해야 합니다.문제가 자주 발생하는 경우 디버그를 가져와서 문제를 마스킹하는 것이 아니라 근본 원인을 해결합니다.

- crypto isakmp invalid-**spi-recovery** 명령의 목적 및 기능에 대한 일반적인 오해가 있습니다.이 명령이 없어도 Cisco IOS는 이미 해당 피어가 있는 IKE SA가 있는 경우 수신된 SA에 대한 전송 피어에 DELETE 알림을 보낼 때 이미 잘못된 SPI 복구 기능 유형을 수행합니다.다시 한 번, crypto isakmp invalid-**spi-recovery** 명령이 활성화되었는지 여부와 상관없이 이가 발생합니다.

- crypto isakmp invalid-**spi-recovery** 명령은 라우터가 잘못된 SPI로 IPsec 트래픽을 수신하고 해당 피어가 있는 IKE SA가 없는 조건을 처리하려고 시도합니다.이 경우 피어와 새 IKE 세션을 설정하려고 시도하고 새로 생성된 IKE SA를 통해 DELETE 알림을 보냅니다.그러나 이 명령은 모든 crypto-configurations에서 작동하지 않습니다.이 명령이 작동하는 유일한 컨피그레이션은

피어가 명시적으로 정의된 고정 암호화 맵과 인스턴스화된 암호화 맵에서 파생된 고정 피어(예: VTI)입니다.다음은 일반적으로 사용되는 암호화 컨피그레이션 및 잘못된 SPI 복구가 해당 컨피그레이션에서 작동하는지 여부를 요약한 것입니다.

| 암호화 구성 | 잘못된 SPI 복구입니까? |
| --- | --- |
| 정적 암호화 맵 | 예 |
| 동적 암호화 맵 | 아니요 |
| 터널 보호가 포함된 P2P GRE | 예 |
| 정적 NHRP 매핑을 사용하는 mGRE 터널 보호 | 예 |
| 동적 NHRP 매핑을 사용하는 mGRE 터널 보호 | 아니요 |
| VTI | 예 |
| EzVPN 클라이언트 | 해당 없음 |

## 간헐적으로 유효하지 않은 SPI 오류 메시지 문제 해결

잘못된 SPI 오류 메시지가 간헐적으로 발생하는 경우가 많습니다.따라서 관련 디버그를 수집하기가 매우 어렵기 때문에 문제를 해결하기가 어렵습니다.이 경우 EEM(Embedded Event Manager) 스크립트가 매우 유용할 수 있습니다.

> **참고:**자세한 내용은 Invalid Security Parameter Indexes Cisco 문서로 인해 발생한 터널 플랩 트러블슈팅에 사용되는 EEM 스크립트를 참조하십시오.