IPsec %RECVD_PKT_INV_SPI 오류 및 잘못된 SPI 복구 기능 정보 확인

목차

소개

이 문서에서는 SA(Security Association)가 피어 디바이스 간에 동기화되지 않을 때 발생하는 IPsec 문제에 대해 설명합니다.

문제

가장 일반적인 IPsec 문제 중 하나는 SA가 피어 디바이스 간에 동기화되지 않을 수 있다는 것입니다. 따라서 암호화 엔드포인트는 피어가 모르는 SA로 트래픽을 암호화합니다. 이러한 패킷은 피어에 의해 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=10.10.1.2, prot=50, spi=0xB761863E(3076621886), srcaddr=10.1.1.1
```

참고: Cisco IOS® XE 라우팅 플랫폼(예: Cisco ASR(Aggregation Services Routers) 및 Cisco Catalyst 8000 Series 라우터)에서 이 특정 삭제는 다음 예에 표시된 것처럼 글로벌 QFP(Quantum Flow Processor) 삭제 카운터뿐 아니라 IPsec 기능 삭제 카운터에도 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
```

이 메시지는 Cisco IOS®에서 속도가 제한되어 있으며 보안상의 이유로 분당 1회의 속도로 전송됩니다. 특정 흐름(SRC, DST 또는 SPI)에 대한 이 메시지가 syslog에 한 번만 나타나는 경우 IPsec rekey와 동시에 일시적인 조건일 수 있습니다. 이 경우 피어 디바이스가 동일한 SA를 사용할 준비가 되지 않은 상태에서 한 피어가 새 SA를 사용하기 시작할 수 있습니다. 이 문제는 일반적으로 문제가 되지 않습니다. 이는 일시적일 뿐이며 몇 개의 패킷에만 영향을 줄 수 있습니다.

그러나 동일한 플로우 및 SPI 번호에 대해 동일한 메시지가 지속되는 경우 IPsec SA가 피어 간에 동기화되지 않았음을 나타냅니다. 예를 들면 다음과 같습니다.

```
Sep  2 13:36:47.287: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=10.10.1.2, 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=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643), srcaddr=10.1.1.1
```

이는 트래픽이 블랙홀링되어 전송 디바이스에서 SA가 만료되거나 DPD(Dead Peer Detection)가 활성화될 때까지 복구할 수 없음을 나타냅니다.

솔루션

이 섹션에서는 이전 섹션에서 설명한 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

잘못된 SPI 복구

이 문제를 해결하려면 잘못된 SPI 복구 기능을 사용하도록 설정하는 것이 좋습니다. 예를 들어 crypto isakmp invalid-spi-recovery 명령을 입력합니다. 이 명령의 사용을 설명하는 몇 가지 중요한 참고 사항은 다음과 같습니다.

- 첫째, 잘못된 SPI 복구는 SA가 동기화되지 않은 경우에만 복구 메커니즘으로 사용됩니다. 이 상태를 복구하는 데 도움이 되지만, SA가 처음부터 동기화되지 않도록 만든 근본 문제를 해결하지는 않습니다. 근본 원인을 더 잘 파악하려면 두 터널 엔드포인트 모두에서 ISAKMP 및 IPsec 디버그를 활성화해야 합니다. 문제가 자주 발생하는 경우 디버그를 가져와 근본 원인을 해결하려고 합니다(문제를 숨기기만 하는 것이 아님).

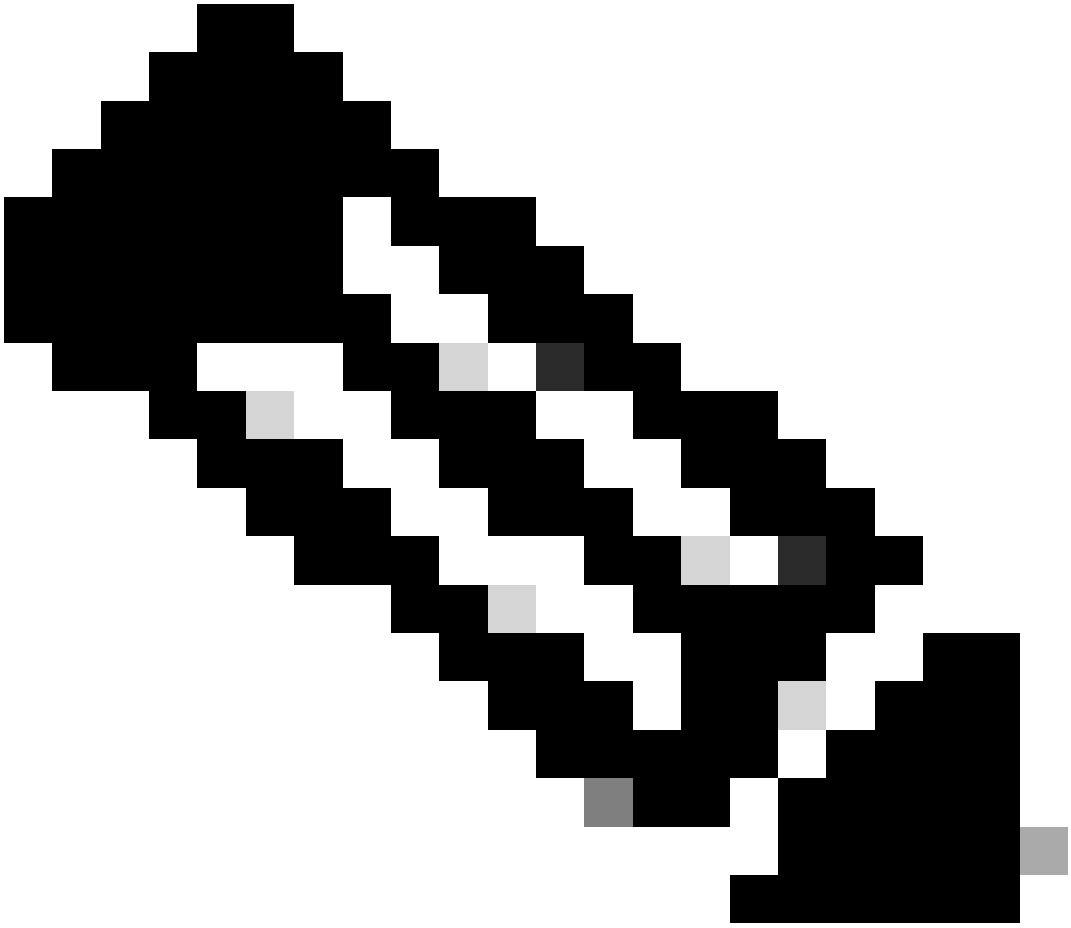
- crypto isakmp invalid-spi-recovery 명령의 목적 및 기능에 대한 일반적인 오해가 있습니다. 이 명령이 없더라도 Cisco IOS는 이미 해당 피어와 함께 IKE SA가 있는 경우 수신된 SA에 대해 전송 피어에 DELETE 알림을 전송할 때 잘못된 SPI 복구 기능 유형을 수행합니다. 다시, 이는 crypto isakmp invalid-spi-recovery 명령이 활성화되었는지 여부와 상관없이 발생합니다.

- crypto isakmp invalid-spi-recovery 명령은 라우터가 잘못된 SPI가 있는 IPsec 트래픽을 수신하고 해당 피어의 IKE SA가 없는 조건을 해결하려고 합니다. 이 경우 피어와 새 IKE 세션을 설정하려고 시도하고 새로 생성된 IKE SA를 통해 DELETE 알림을 보냅니다. 그러나 이 명령은 일부 crypto-configuration에서 작동하지 않습니다. 이 명령이 작동하는 유일한 컨피그레이션은 피어가 명시적으로 정의된 정적 암호화 맵과 VTI와 같이 인스턴스화된 암호화 맵에서 파생된 정적 피어입니다. 다음은 일반적으로 사용되는 암호화 컨피그레이션 및 잘못된 SPI 복구가 해당 컨피그레이션에서 작동하는지 여부를 요약한 것입니다.

암호화 컨피그레이션	잘못된 SPI 복구
정적 암호화 맵	예
동적 암호화 맵	아니요
터널 보호를 사용하는 P2P GRE	예
고정 NHRP 매핑을 사용하는 mGRE 터널 보호	예
동적 NHRP 매핑을 사용하는 mGRE 터널 보호	아니요
sVTI	예
EzVPN 클라이언트	해당 없음

간헐적으로 유효하지 않은 SPI 오류 메시지 트러블슈팅

잘못된 SPI 오류 메시지가 간헐적으로 발생하는 경우가 많습니다. 따라서 관련 디버그를 수집하기가 매우 어려워지므로 문제 해결이 어렵습니다. 이 경우 EEM(Embedded Event Manager) 스크립트가 매우 유용할 수 있습니다.



참고: 자세한 내용은 유효하지 않은 보안 매개변수 인덱스로 인한 터널 플랩 트러블슈팅에 사용되는 EEM 스크립트 Cisco 문서를 참조하십시오.

알려진 버그

이 목록에는 IPsec SA가 동기화되지 않거나 잘못된 SPI 복구와 관련된 버그가 표시됩니다.

- Cisco 버그 ID CSCvn31824 Cisco IOS XE ISAKMP는 설치를 완료하기 전에 rx 새 SPI 패킷을 삭제하면 새 SPI를 삭제합니다
- Cisco 버그 ID CSCvd40554 IKEv2: Cisco IOS에서 SPI 크기가 0인 INV_SPI 알림을 구문 분석할 수 없습니다. INVALID_SYNTAX를 보냅니다.
- Cisco 버그 ID CSCvp16730 0xFF로 시작하는 SPI 값이 있는 수신 ESP 패킷이 잘못된 SPI 오류로 인해 삭제됩니다

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.