SD-WAN 및 기존 터널 이해 SPI 차이점 복구

목차

소개

이 문서에서는 %RECVD_PKT_INV_SPI 오류에서 SD-WAN 및 서드파티 터널을 복구하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst SD-WAN(Software-Defined Wide Area Network)
- IPSec(Internet Protocol Security)
- BFD(Bidirectional Forwarding Detection).

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Cisco IOS® XE Catalyst SD-WAN Edge.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

IPSec에는 SA(Security Association)의 개념이 필수적입니다. SA는 엔드포인트가 보안 서비스를 사용하여 안전하게 통신하는 방법을 설명하는 두 엔드포인트 간의 관계입니다.

SPI(Security Parameter Index)는 IPSec을 사용하여 연결된 디바이스에 대해 특정 SA를 고유하게 식별하기 위해 선택한 32비트 숫자입니다.

가장 일반적인 IPsec 문제 중 하나는 잘못된 SPI 값으로 인해 SA가 동기화되지 않을 수 있으며, 이로 인해 피어에서 패킷이 삭제되고 라우터에서 syslog 메시지가 수신됨에 따라 IPSEC 터널 다운 상태가 발생할 수 있다는 것입니다.

타사 터널:

```
Jan  8 15:00:23.723 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

SD-WAN 터널의 경우:

```
Jan 10 12:18:43.404 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

이러한 로그는 FP(Forwarding Processor)에 속한 QFP(Quantum Flow Processor)에서 드롭과 함께 제공됩니다.

<#root>

```
Router#
show platform hardware qfp active feature ipsec datapath drops

------------------------------------------------------------------------
Drop Type Name                                                  Packets
------------------------------------------------------------------------
1 IN_V4_PKT_HIT_INVALID_SA                                            1
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 9393888 <-- sub code error

19 IN_OCT_ANTI_REPLAY_FAIL                                          342
```

솔루션

기존 IPSec 터널 복구

기존 IPSec 터널을 복구하려면 현재 SA 값 관계를 수동으로 갱신해야 합니다. 이 작업은 EXEC mode 명령으로 IPSec SA를 지워서 수행합니다.

<#root>

```
Router#
clear crypto sa peer 10.20.20.1
```

SD-WAN 터널 복구 - 시나리오 1

clear crypto sa peer EXEC 명령은 IKE(Internet Key Exchange)가 있으므로 기존 IPSec 터널에서만 작동합니다. 연결을 자동으로 협상하고 새 SPI 값을 생성합니다. 그러나 SD-WAN 터널에서는 이 명령을 사용할 수 없습니다. 그 이유는 SD-WAN 터널에서는 IKE가 사용되지 않기 때문입니다.

이 때문에 SD-WAN 터널에 대한 homous 명령이 사용됩니다.

```
<#root>
Router#
request platform software sdwan security ipsec-rekey
```

요청 플랫폼 소프트웨어 sdwan security ipsec-rekey 명령은 새 키를 즉시 생성한 다음 터널이 시작됩니다. 이와 반대로, 기존 IPSec 터널이 있는 경우 이 명령은 영향을 주지 않습니다.

참고: 요청 플랫폼 소프트웨어 sdwan 보안 ipsec-rekey 이 명령은 지정된 SA에서만 적용되는 clear crypto sa peer의 반대에 있는 모든 기존 SD-WAN 터널에서 적용됩니다.

SD-WAN 터널 복구 - 시나리오 2

실수로 clear crypto sa peer 명령을 사용하여 SD-WAN 터널 SA 중 하나를 삭제한 경우 삭제는 성공적으로 수행됩니다. 그러나 새 SPI 값이 다시 생성되지 않습니다. SD-WAN 터널에서는 OMP가 IKE가 아닌 작업을 트리거하는 값이기 때문입니다. 이 상태가 되면 clear crypto sa peer를 실행한 후 명령 요청 플랫폼 소프트웨어 sdwan 보안 ipsec-rekey가 실행되더라도 터널이 나타나지 않습니다. SA의 캡슐화 및 역캡슐화는 0으로 유지되고, 결과적으로 BFD 세션은 다운 상태로 유지된다.

```
Router#clear crypto sa peer 10.20.20.1
Router#show crypto ipsec sa peer 10.20.20.1
interface: Tunnel10001
Crypto map tag: Tunnel10001-vesen-head-0, local addr 10.10.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/12346)
remote ident (addr/mask/prot/port): (10.20.20.1/255.255.255.255/0/12366)
current_peer 10.20.20.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

SA를 삭제한 후 유일한 복구 옵션은 다음 세 가지 EXEC 명령 중 하나와 함께 사용할 수 있습니다.

<#root>

Router#

clear sdwan omp all

clear sdwan omp all 명령은 디바이스에 있는 모든 BFD 세션을 플랩합니다.

<#root>

Router#

request platforms software sdwan port_hop

clear sdwan control connections 명령을 사용하면 TLOC에서 지정된 로컬 색상에서 사용 가능한 다음 포트 번호를 사용하게 되므로 해당 색상의 모든 BFD 세션뿐만 아니라 해당 색상의 제어 연결도 플랩됩니다.

<#root>

Router#

clear sdwan control connections

마지막 명령은 또한 복구를 지원하지만, 이 명령의 영향은 디바이스에 있는 모든 제어 연결 및 BFD 세션에 미칩니다.

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.