SD-WAN cEdge IPsec Anti Replay 오류 트러블슈팅

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[SD-WAN Replay Detection 고려 사항](#)
[그룹 키와 페어와이즈 키 비교](#)
[인코딩된 SPI](#)
[QoS를 위한 다중 시퀀스 번호 공간](#)
[구성된 재생 창을 적용하는 명령](#)
[재생 삭제 실패 문제 해결](#)
[데이터 수집 문제 해결](#)
[워크플로 문제 해결](#)
[ASR1001-x의 문제 해결 예](#)
[솔루션](#)
[추가 Wireshark Capture 툴](#)

소개

이 문서에서는 SD-WAN IPsec for cEdges 라우터의 IPsec Anti-Replay 동작 및 Anti-Replay 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)
- 인터넷 프로토콜 보안(IPsec)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C8000V 버전 17.06.01
- ASR1001-X 버전 17.06.03a
- vManage 버전 20.7.1

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.

배경 정보

IPsec 인증은 이전 또는 중복된 IPsec 패킷에 대해 내장된 재전송 방지 보호 기능을 제공하며, 수신기에서 확인한 ESP 헤더의 시퀀스 번호를 사용합니다. 재전송 방지 패킷 삭제는 재전송 방지 창을 벗어나 잘못 전달된 패킷으로 인한 IPsec의 가장 일반적인 데이터 플레인 문제 중 하나입니다. IPsec 재전송 방지 삭제에 대한 일반적인 문제 해결 방식은 IPsec Anti Replay Check Failures에서 찾을 수 있으며, 일반적인 기술은 SD-WAN에도 적용됩니다. 그러나 기존 IPsec과 Cisco SD-WAN 솔루션에 사용되는 IPsec 간에는 몇 가지 구현 차이점이 있습니다. 이 문서에서는 Cisco IOS ®XE를 사용하는 cEdge 플랫폼의 차이점과 접근 방식을 설명하기 위해 마련되었습니다.

SD-WAN Replay Detection 고려 사항

그룹 키와 페어와이즈 키 비교

IKE 프로토콜을 사용하여 두 피어 간에 IPsec SA를 협상하는 기존 IPsec과 달리 SD-WAN은 그룹 키 개념을 사용합니다. 이 모델에서 SD-WAN 에지 디바이스는 TLOC당 데이터 플레인 인바운드 SA를 주기적으로 생성하고 이러한 SA를 vSmart 컨트롤러로 전송합니다. 그러면 vSmart 컨트롤러는 SA를 SD-WAN 네트워크의 나머지 에지 디바이스로 전파합니다. SD-WAN 데이터 플레인 작업에 대한 자세한 내용은 SD-WAN 데이터 플레인 보안 개요를 참조하십시오.

> **참고**: Cisco IOS ®XE 이후 6.12.1a/SD-WAN 19.2, IPsec 페어와이즈 키가 지원됩니다. IPsec Pairwise 키 개요를 참조하십시오. Pairwise 키를 사용하면 IPsec 재전송 방지 보호가 기존 IPsec과 동일하게 작동합니다. 이 글은 주로 그룹키 모형의 사용에 대한 리플레이 체크에 초점을 맞추고 있다.

인코딩된 SPI

IPsec ESP 헤더에서 SPI(Security Parameter Index)는 수신자가 인바운드 패킷이 해독되는 SA를 식별하는 데 사용하는 32비트 값입니다. SD-WAN을 사용하면 이 인바운드 SPI를 show crypto ipsec sa로 **식별할** 수 **있습니다**.

```
cedge-2#show crypto ipsec sa | se inbound
     inbound esp sas:
      spi: 0x123(291)
        transform: esp-gcm 256 ,
        in use settings ={Transport UDP-Encaps, esn}
        conn id: 2083, flow_id: CSR:83, sibling_flags FFFFFFFF80000008, crypto map: Tunnel1-
vesen-head-0
        sa timing: remaining key lifetime 9410 days, 4 hours, 6 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

> **참고**: 인바운드 SPI가 모든 터널에 대해 동일하더라도 SA가 소스, 대상 IP 주소, 소스, 대상 포트 4-튜플 및 SPI 번호로 식별되므로 수신자는 각 피어 에지 디바이스에 대해 SA와 관련된 다른 SA 및 해당 재생 창 객체를 가지고 있습니다. 기본적으로 각 피어는 자체 안티 릴레이 창 객체를 가지고 있습니다.

피어 디바이스에서 전송한 실제 패킷에서 SPI 값이 이전 출력과 다름을 확인합니다. 다음은 패킷 복사 옵션이 활성화된 packet-trace 출력의 예입니다.

```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

ESP 헤더의 실제 SPI는 **0x04000123입니다.** 그 이유는 SD-WAN을 위한 SPI의 첫 번째 비트들은 추가 정보로 인코딩되고, SPI 필드의 낮은 비트들만이 실제 SPI에 할당되기 때문이다.

기존 IPsec:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SD-WAN:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  CTR  | MSNS|         Security Parameters Index (SPI)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

여기서

- **CTR**(처음 4비트, 비트 0-3) - 제어 비트, 특정 유형의 제어 패킷을 표시하는 데 사용됩니다. 예를 들어 제어 비트 0x80000000은 BFD에 사용됩니다.
- **MSNS**(다음 3비트, 비트 4-6) - 다중 시퀀스 번호 공간 인덱스 시퀀스 카운터 배열에서 올바른 시퀀스 카운터를 찾아 지정된 패킷에 대한 재생을 확인하는 데 사용됩니다. SD-WAN의 경우 3비트 MSN을 사용하면 8개의 서로 다른 트래픽 클래스를 고유한 시퀀스 번호 공간에 매핑할 수 있습니다. 이는 SA 선택에 사용할 수 있는 유효 SPI 값이 필드의 전체 32비트 값에서 25비트로 감소한 것을 의미합니다.

QoS를 위한 다중 시퀀스 번호 공간

QoS는 항상 IPsec 암호화 및 캡슐화 후에 실행되므로, QoS(예: LLQ)로 인해 패킷이 순서에 맞지 않게 전달되는 환경에서 IPsec 재생 실패를 관찰하는 것이 일반적입니다. Multiple Sequence Number Space 솔루션은 지정된 보안 연결에 대해 서로 다른 QoS 트래픽 클래스에 매핑된 여러 시퀀스 번호 공간을 사용하여 이 문제를 해결합니다. 다른 시퀀스 번호 공간은 도시된 바와 같이 ESP 패킷 SPI 필드에 인코딩된 MSNS 비트에 의해 인덱싱된다. 자세한 설명은 QoS용 IPsec Anti Replay Mechanism을 참조하십시오.

앞서 언급한 바와 같이, 이 다중 시퀀스 번호 구현은 SA 선택에 사용할 수 있는 유효 SPI 값이 낮은 차수 25비트로 감소되었음을 의미합니다. 이 구현과 함께 재생 창 크기를 구성할 때 또 다른 실용적인 고려 사항은 구성된 재생 창 크기가 종합 재생 창에 대한 것이므로 각 시퀀스 번호 공간의 유효 재생 창 크기는 합계의 1/8입니다.

컨피그레이션 예시:

```
config-t
Security
IPsec
replay-window 1024
Commit
```

참고: 각 시퀀스 번호 공간의 유효 재생 창 크기는 1024/8 = 128!입니다.

참고: Cisco IOS ®XE 이후 17.2.1, 종합 재생 창 크기가 8192로 증가하여 각 시퀀스 번호 공간은 8192/8 = 1024 패킷의 최대 재생 창을 가질 수 있습니다.

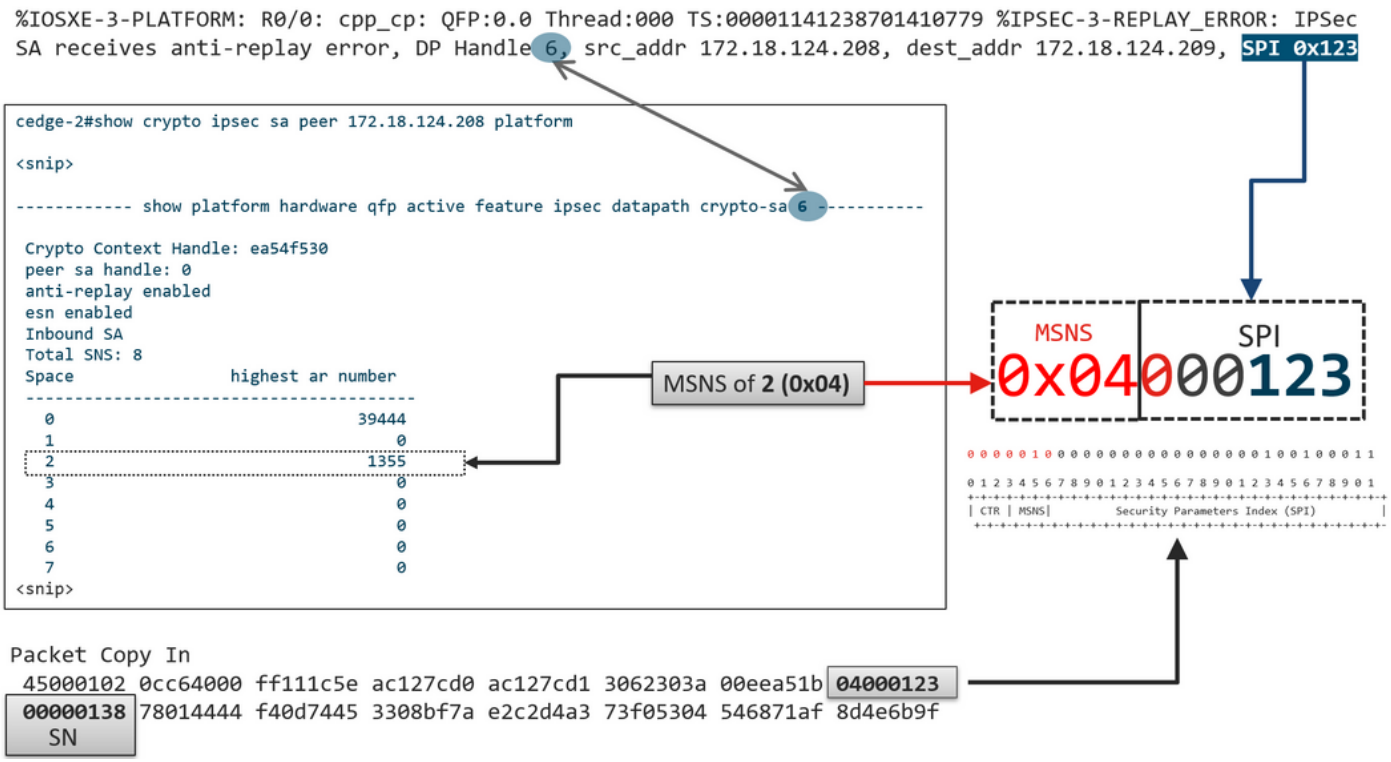
cEdge 디바이스에서 각 시퀀스 번호 공간에 대해 수신된 마지막 시퀀스 번호는 **show crypto ipsec sa peer x.x.x.x platform IPsec dataplane 출력에서** 얻을 수 있습니다.

```
cedge-2#show crypto ipsec sa peer 172.18.124.208 platform

<snip>

------------------ show platform hardware qfp active feature ipsec datapath crypto-sa 5 --------
----------

 Crypto Context Handle: ea54f530
 peer sa handle: 0
 anti-replay enabled
 esn enabled
 Inbound SA
 Total SNS: 8
 Space                highest ar number
 ---------------------------------------
   0                               39444
   1                                   0
   2                                1355
   3                                   0
   4                                   0
   5                                   0
   6                                   0
   7                                   0
<snip>
```

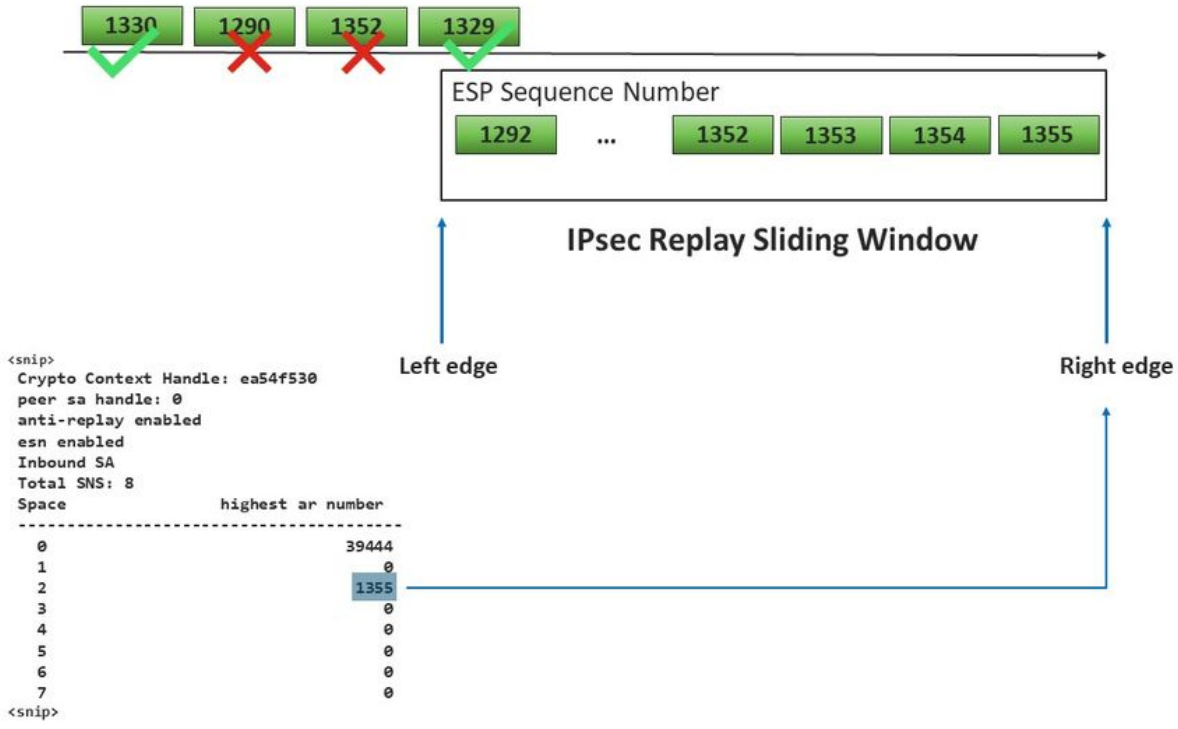
이 예에서 MSNS가 0**(0x00)**인 경우 가장 높은 재전송 방지 창(재전송 방지 슬라이딩 창의 오른쪽 가장자리)은 **3944이고**, **2(0x04)인 경우**는 **1335**이며, 이러한 카운터는 시퀀스 번호가 동일한 시퀀스 번호 공간의 패킷에 대한 재생 창 내부에 있는지 확인하는 데 사용됩니다.

참고: ASR1k 플랫폼과 나머지 Cisco IOS ®XE 라우팅 플랫폼(ISR4k, ISR1k, CSR1kv) 간에는 구현 차이가 있습니다. 따라서 이러한 플랫폼에 대한 show 명령 및 출력 측면에서 몇 가지 불일치가 있습니다.

Anti-Replay 오류 및 표시 출력을 연결하여 이미지에 표시된 대로 SPI 및 시퀀스 번호 인덱스를 찾을 수 있습니다.



이전 정보를 사용하여 오른쪽 가장자리(위쪽 창)와 슬라이딩 창이 이미지에 표시된 것처럼 보입니다.



구성된 재생 창을 적용하는 명령

일반 IPsec(non SD-WAN)과 달리 rekey 명령은 재전송 방지 창에 적용되지 않습니다.

```
request platform software sdwan security ipsec-rekey
```

다음 명령은 구성된 재생 창을 트리거하여 적용됩니다.

경고: 모든 명령의 잠재적인 영향을 이해하고, 제어 연결 및 데이터 플레인에 영향을 미치는지 확인하십시오.

```
clear sdwan control connection
```

또는

```
request platform software sdwan port_hop <color>
```

또는

```
Interface Tunnelx
shutdown/ no shutdown
```

재생 삭제 실패 문제 해결

데이터 수집 문제 해결

IPsec 재전송 방지 삭제의 경우 문제의 상태와 잠재적 트리거를 이해하는 것이 중요합니다. 최소한 컨텍스트를 제공하기 위해 정보 집합을 수집합니다.

- 재생 패킷의 발신자 및 수신자 모두에 대한 디바이스 정보에는 디바이스 유형, cEdge vs. vEdge, 소프트웨어 버전, 컨피그레이션이 포함됩니다.
- 문제 기록. 구축은 언제부터 진행되었습니까? 언제부터 문제가 발생했습니까? 네트워크 또는 트래픽 상태에 대한 최근 변경 사항.
- 예를 들어 재생이 중단되는 패턴은 산발적입니까, 아니면 일정합니까? 문제 및/또는 중요한 이벤트의 시간(예: 트래픽이 많은 피크 생산 시간 또는 키 재설정 동안에만 발생합니까? 등)

이전 정보를 수집한 후 문제 해결 워크플로를 진행합니다.

워크플로 문제 해결

IPsec 재생 문제에 대한 일반적인 트러블슈팅 방식은 기존 IPsec의 경우와 마찬가지로, 설명한 대로 피어별 SA 시퀀스 공간 및 다중 시퀀스 번호 공간을 고려합니다. 그런 다음 다음 다음 단계를 수행합니다.

1단계. 먼저 syslog에서 재생 삭제에 대한 피어와 삭제 속도를 식별합니다. 삭제 통계의 경우, 항상 출력의 여러 타임스탬프된 스냅샷을 수집하여 삭제 속도를 확인할 수 있도록 합니다.

```
*Feb 19 21:28:25.006: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00001141238701410779 %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 6,
src_addr 172.18.124.208, dest_addr 172.18.124.209, SPI 0x123

cedge-2#show platform hardware qfp active feature ipsec datapath drops
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
No time source, *11:25:53.524 EDT Wed Feb 26 2020
----------------------------------------------------------------------
Drop Type  Name                                          Packets
----------------------------------------------------------------------
        4  IN_US_V4_PKT_SA_NOT_FOUND_SPI                        30
       19  IN_CD_SW_IPSEC_ANTI_REPLAY_FAIL                      41
```

참고: 네트워크에서 패킷 전달 순서 변경으로 인해 가끔 재생이 삭제되는 경우가 드물지 않지만, 지속적인 재생이 삭제되면 서비스에 영향을 미치므로 조사할 수 있습니다.

2a 단계. 비교적 낮은 트래픽 속도를 얻으려면 조건이 peer ipv4 address with **copy packet 옵션**으로 설정된 패킷 추적을 수행하고 현재 재생 윈도우 오른쪽 가장자리에 대해 삭제된 패킷의 시퀀스 번호 및 인접 패킷의 시퀀스 번호를 검사하여 실제 복제 패킷인지 또는 재생 윈도우 외부에 있는지 확인합니다.

2b단계. 예측 가능한 트리거가 없는 높은 트래픽 속도를 위해 순환 버퍼와 EEM을 사용하여 EPC 캡처를 구성하여 재생 오류가 탐지될 때 캡처를 중지합니다. EEM은 19.3부터 현재 vManage에서 지원되지 않으므로, 이는 이 트러블슈팅 작업을 수행할 때 cEdge가 CLI 모드에 있어야 함을 의미합니다.

3단계. 패킷 캡처 또는 **패킷 추적이 수집되는 동시**에 이상적으로 수신기의 **show crypto ipsec sa peer x.x.x.x platform**을 수집합니다. 이 명령에는 인바운드 및 아웃바운드 SA에 대한 실시간 데이터 플레인 재생 창 정보가 포함됩니다.

4단계. 삭제된 패킷이 실제로 순서가 잘못된 경우 발신자와 수신자의 동시 캡처를 통해 소스 또는 언더레이 네트워크 전송 레이어에 문제가 있는지 확인합니다.

5단계. 패킷이 중복되거나 재생 창 외부에 있지 않더라도 삭제되는 경우 일반적으로 수신기의 소프트웨어 문제를 나타냅니다.

ASR1001-x의 문제 해결 예

문제 설명:

HW: ASR1001-X
소프트웨어: 17.06.03a

세션 피어 10.62.33.91에 대해 여러 재전송 방지 오류가 수신되므로 BFD 세션이 지속적으로 플랩하며 이러한 두 사이트 간의 트래픽이 영향을 받습니다.

```
Jul 26 20:31:20.879: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:027 TS:00000093139972173042
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:32:23.567: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:009 TS:00000093202660128696
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:33:33.939: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:051 TS:00000093273031417384
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
Jul 26 20:34:34.407: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:020 TS:00000093333499638628
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 22, src_addr 10.62.33.91,
dest_addr 10.62.63.251, SPI 0x106
```

1단계. Check Configured Anti Replay(구성된 재전송 방지 확인) 창은 8192입니다.

```
cEdge#sh sdwan security-info
security-info authentication-type deprecated
security-info rekey 86400
 security-info replay-window 8192
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Disabled
security-info pairwise-keying Disabled
security-info pwk-sym-rekey Enabled
security-info extended-ar-window Disabled
security-info integrity-type "ip-udp-esp esp"
```

주: 이 예에서는 각 시퀀스 번호 공간에 대한 유효 재생 창 크기가 8192/8= 1024여야 합니다.

2단계. 구성된 값을 비교 및 확인하려면 피어 10.62.33.91의 유효 재생 윈도우 크기를 확인합니다.

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64                  <-- Effective Window Size
window base(ESN): 0
Multi-SNS window_top
---------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

이 **창 크기: 64** 출력에 표시된 재생 창이 구성된 재생 창과 일치하지 않습니다 . **8192(8192//8=1024)**즉, 구성된 경우에도 명령이 적용되지 않았습니다.

참고: 유효 재생 창은 ASR 플랫폼에만 표시됩니다. 재전송 방지 창의 실제 크기가 구성된 크기와 같도록 하려면 섹션 명령에 있는 명령 중 하나를 적용하여 구성된 재생 창의 효과를 적용합니다.

3단계. 세션 소스 10.62.33.91, 대상 10.62.63.251의 인바운드 트래픽에 대해 패킷 추적을 구성하고 동시에 캡처 모니터링(선택 사항)을 활성화합니다

```
cEdge#debug platform packet-trace packet 2048 circular fia-trace data-size 2048
cEdge#debug platform packet-trace copy packet both size 2048 L3
cEdge#debug platform condition ipv4 10.62.33.91/32 in
cEdge#debug plat cond start
```

4단계. 패킷 추적 요약 수집:

```
cEdge#show platform packet summay
```

5단계. 캡처된 일부 삭제된(IpsecInput) 패킷을 확장합니다.

(IpsecInput) 패킷 삭제:

```
cEdge#sh platform pack pack 816
Packet: 816 CBUG ID: 973582
Summary
Input : TenGigabitEthernet0/0/0.972
Output : TenGigabitEthernet0/0/0.972
State : DROP 56 (IpsecInput)
Timestamp
Start : 97495234494754 ns (07/26/2022 21:43:56.25110 UTC)
Stop : 97495234610186 ns (07/26/2022 21:43:56.25225 UTC)
Path Trace
Feature: IPV4(Input)
Input : TenGigabitEthernet0/0/0.972
Output : <unknown>
Source : 10.62.33.91
Destination : 10.62.63.251
Protocol : 17 (UDP)
SrcPort : 12367
DstPort : 12347
<snip>

Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfed 00000000 d0a60d5b 6161b06e 453d0e3d 5ab694ce 5311bbb6 640ecd68
7ceb2726 80e39efd 70e5549e 57b24820 fb963be5 76d01ff8 273559b0 32382ab4
c601d886 da1b3b94 7a2826e2 ead8f308 c464
```

```
817 DROP:
------------------------------
Packet: 817
<snip>
Packet Copy In
45000072 ab314000 fd115c77 0a3e215b 0a3e3ffb 304f303b 005e0000 04000106
00b6dfec 00000000 cc72d5dd ef73fe25 2440bed6 31378b78 3c506ee5 98e3dba4
bc9e6aa0 50ea98f6 7dee25c8 c1579ce0 1212290c 650f5947 57b9bc04 97c7996c
d4dbf3e6 25b33684 a7129b67 141a5e73 8736
```

SD-WAN은 UDP 캡슐화된 ESP를 사용합니다.

- UDP 헤더는 304f303b 00770000,
- 다음은 SPI(**04000106**)입니다
- 따라서 **00b6e00d**는 SN(보안 번호)입니다.
- 32비트 SPI(**0 0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1)로 인해 MSNS 인덱스는 **2**(**x04**00106)입니다.

6단계. MSNS 인덱스 확인

```
show crypto ipsec sa peer 10.62.33.91 platform
<snip>
------------------ show platform hardware qfp active feature ipsec sa 22 ------------------
<snip>
------------------ show platform software ipsec fp active encryption-processor 0 context
c441ff4c ------------------
<snip>
       window size: 64
window base(ESN): 0
Multi-SNS window_top
----------------------------------
index: 0, win_top: 0x00000000010dc0
index: 1, win_top: 0000000000000000
  index: 2, win_top: 0x00000000b65f00
index: 3, win_top: 0000000000000000
index: 4, win_top: 0000000000000000
index: 5, win_top: 0000000000000000
index: 6, win_top: 0000000000000000
index: 7, win_top: 0000000000000000
traffic hard limit: 12876354284605669376
byte count: 0
packet count: 11378618
```

2(0x04)의 MSNS에 대한 가장 높은 재전송 방지 윈도우(재전송 방지 슬라이딩 윈도우의 오른쪽 가장자리)는 **0b65f00**이다.

7단계. 일부 전달(FWD) 캡처된 패킷을 확장합니다.

전달된 패킷:

```
Packet: 838
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
```

```
 00b6e015 00000000 088bbd6a f4e4b35f b131143f ef1f91eb 659149f7 dbe6b025
be7fbfd0 5fad1c71 014321f1 3e0d38f2 cc8d0e5f 1494e4fa 097c7723 dfc7ceef
4a14f444 abcc1777 0bb9337f cd70c1da 01fc5262 848b657c 3a834680 b07b7092
81f07310 4eacd656 ed36894a e468
```

패킷: 837

```
Packet: 837
<snip>
Packet Copy In
4564008e ab044000 fd115c24 0a3e215b 0a3e3ffb 304f303b 007a0000 04000106
00b6e014 00000000 76b2a256 8e835507 13d14430 ae16d62c c152cdfd 2657c20c
01d7ce1d b3dfa451 a2cbf6e9 32f267f9 e10e9dec 395a0f9e 38589adb aad8dfb8
a3b72c8d a96f2dce 2a1557ab 67959b6e 94bbbb0a cfc4fc9e 391888da af0e492c
80bebb0e 9d7365a4 153117a6 4089
```

8단계. 삭제 전, 후 및 삭제 전 FWD(Multipe Packets Forwarded)에서 시퀀스 번호 정보를 수집하고 가져옵니다.

```
FWD:
839 PKT: 00b6e003 FWD
838 PKT: 00b6e001 FWD
837 PKT: 00b6e000 FWD
815 PKT: 00b6e044 FWD
814 PKT: 00b6dfe8 FWD
813 PKT: 00b6e00d FWD

DROP:
816 PKT: 00b6dfed DROP
817 PKT: 00b6dfec DROP
818 PKT: 00b6dfeb DROP
819 PKT: 00b6dfe9 DROP
820 PKT: 00b6dfea DROP
```

9단계. SN을 Decimal로 변환하고 단순 계산으로 다시 정렬합니다.

```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

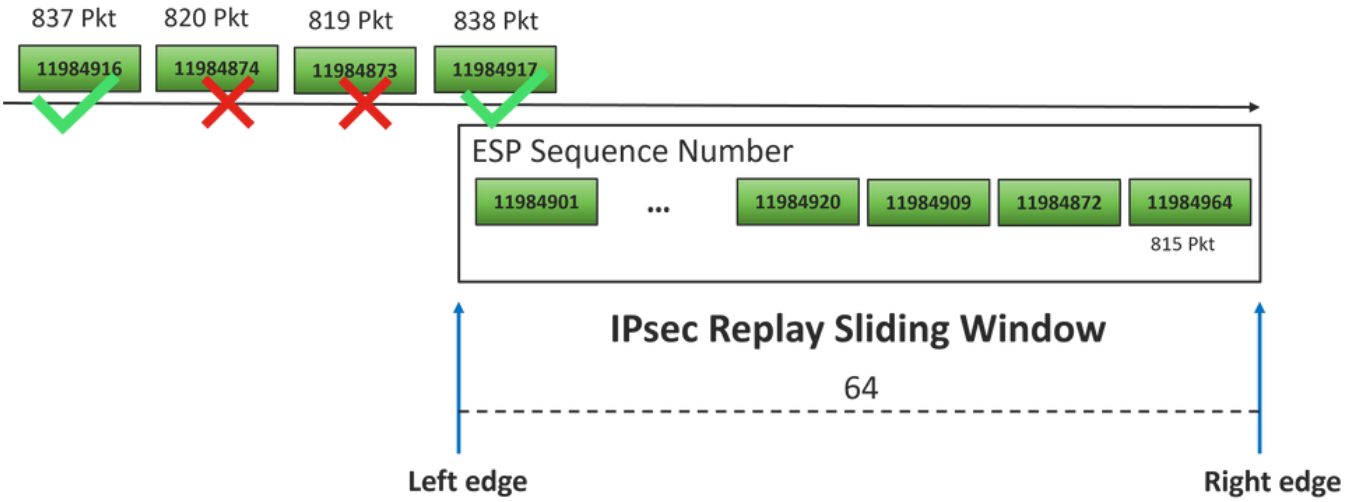
> **참고**: 시퀀스 번호가 창에서 가장 높은 시퀀스 번호보다 크면 패킷의 무결성이 검사됩니다. 패킷이 무결성 확인 검사를 통과하면 슬라이딩 창이 오른쪽으로 이동합니다.

10단계. SN을 Decimal로 변환하고 단순 계산으로 다시 정렬합니다.

```
Difference:
```

```
815 PKT: Decimal: 11984964 ***** Highest Value
-------------------------------------
815(Highest) - X PKT = Diff
-------------------------------------
816 PKT: 11984964 - 11984877 = 87 DROP
817 PKT: 11984964 - 11984876 = 88 DROP
818 PKT: 11984964 - 11984875 = 89 DROP
819 PKT: 11984964 - 11984873 = 91 DROP
820 PKT: 11984964 - 11984874 = 90 DROP
<snip>
837 PKT: 11984964 - 11984916 = 48 FWD
838 PKT: 11984964 - 11984917 = 47 FWD
839 PKT: 11984964 - 11984918 = 45 FWD
```

이 예에서는, 이미지와 같이, **창 사이즈(64)**와 **우측 에지11984964** 슬라이딩 창을 시각화할 수 있다 .



패킷 삭제에 대해 수신된 시퀀스 번호가 해당 시퀀스 공간에 대한 재생 창의 오른쪽 가장자리보다 훨씬 앞섭니다.

솔루션

창 크기가 2단계에서 보았던 이전 값(64)에 여전히 있으므로, 1024 창 크기에 영향을 미치기 위해 Commands to Take Effectiveness of the Configured Replay Window 섹션에 있는 명령 중 하나를 적용해야 합니다.

추가 Wireshark Capture 툴

ESP SPI와 시퀀스 번호의 상관관계를 분석하는 데 유용한 또 다른 툴로는 Wireshark 소프트웨어가 있습니다.

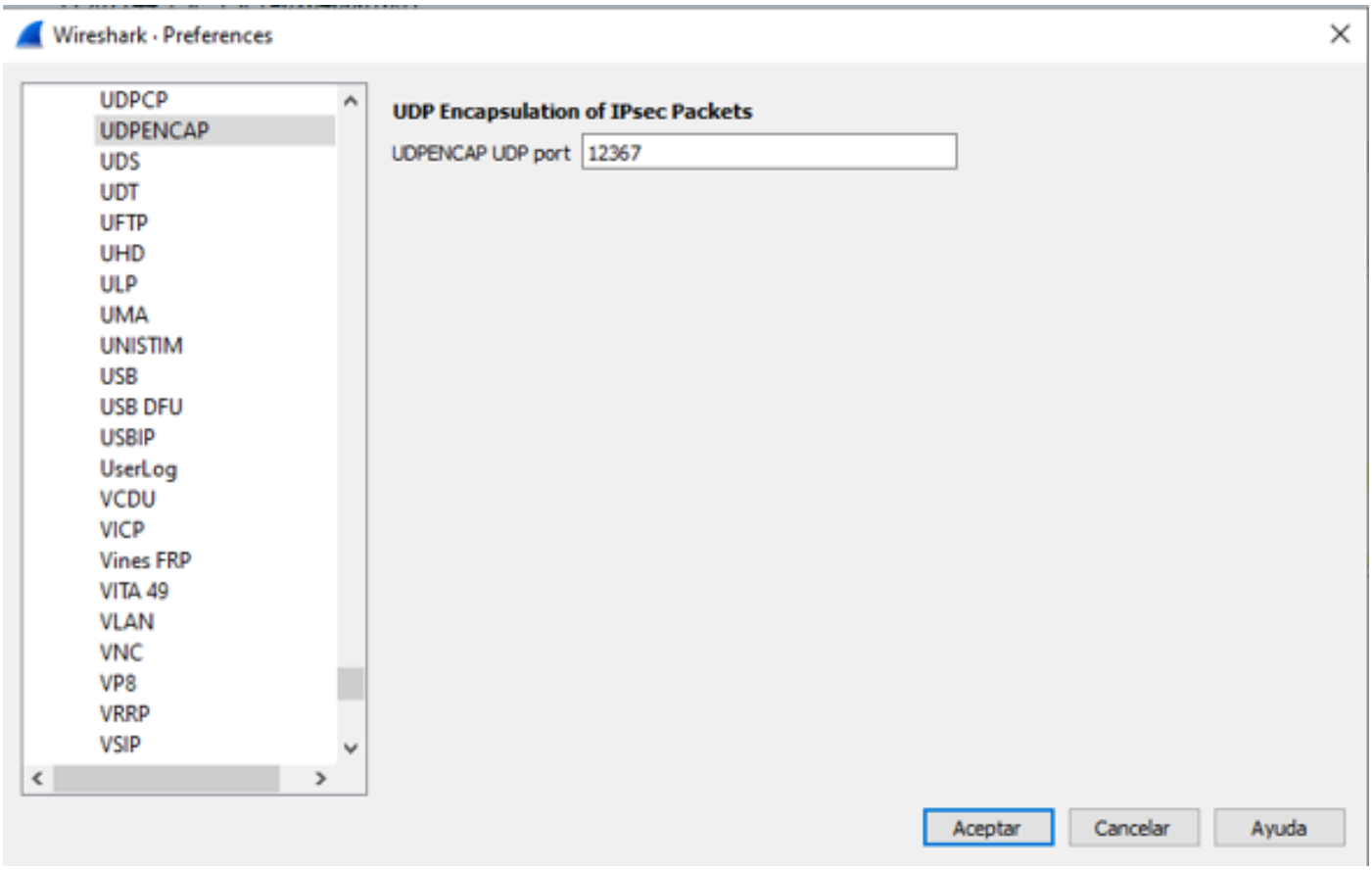
> **참고**: 문제가 발생할 때 패킷 캡처를 수집하는 것이 중요하며, 앞서 설명한 대로 파일 추적이 동시에 가능한 경우 패킷 추적을 수집하는 것이 중요합니다

인바운드 방향에 대한 패킷 캡처를 구성하고 pcap 파일로 내보냅니다.

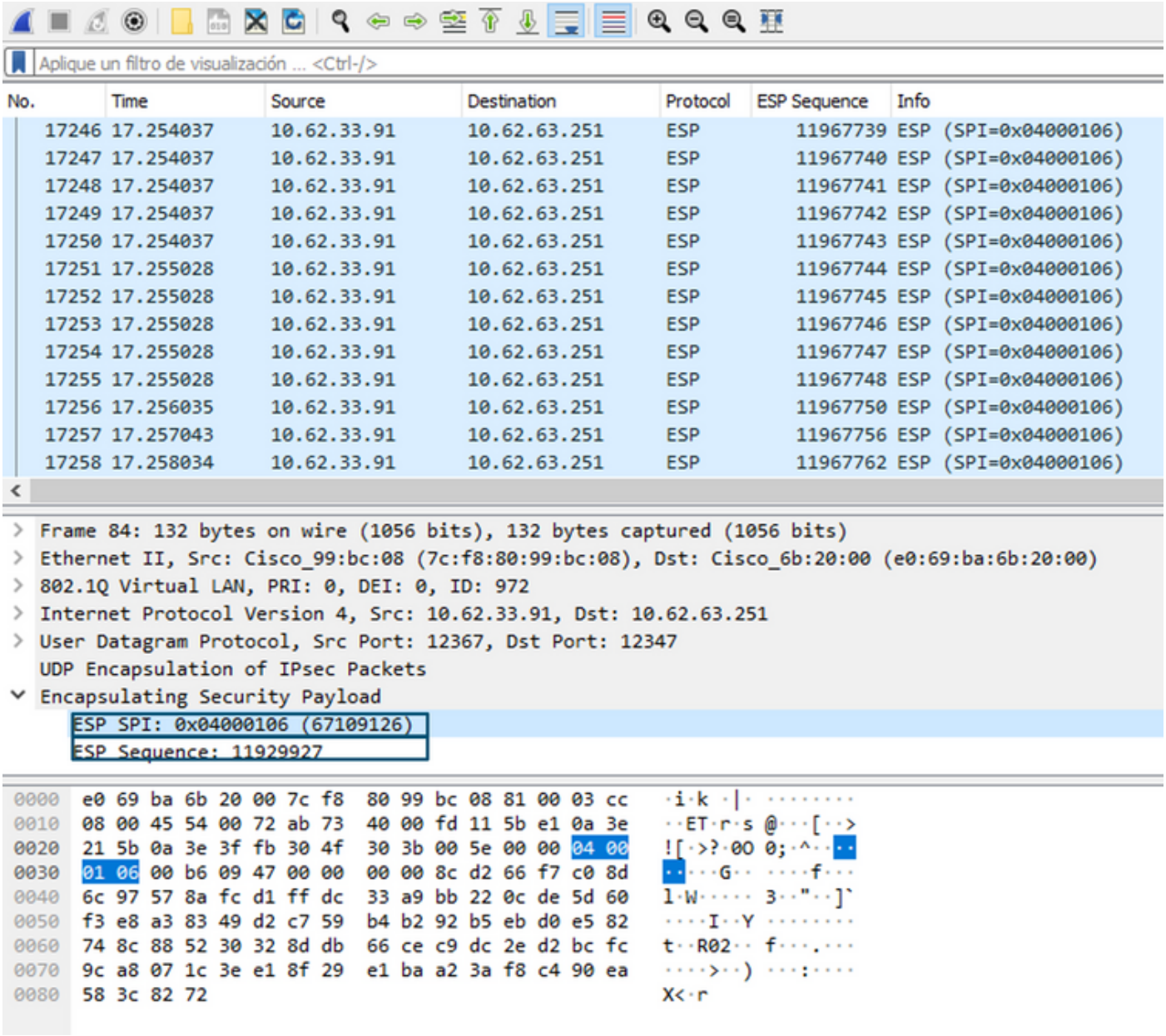
```
monitor caputure CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TenGigabitEthernet0/0/0 in
monitor caputure CAP star
```

```
monitor caputure CAP stop
monitor caputure CAP export bootflash:Anti-replay.pca
```

Wireshark에서 pcap 캐쳐가 열리면 ESP SPI와 시퀀스 번호를 볼 수 있도록 패킷 하나를 확장하고 마우스 오른쪽 버튼을 클릭한 다음 **프로토콜 환경 설정을** 선택하고 UPPENCAP을 검색하고 그림과 같이 기본 포트를 SD-WAN 포트(소스 포트)로 변경합니다.



UDPENCAP이 오른쪽 포트에 배치되면 ESP 정보가 그림과 같이 표시됩니다.



관련 정보

- [IPsec 재전송 방지 검사 실패 TechZone 문서]
- [IPsec Anti-Replay 창 확장 및 비활성화]
- [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.