Probleemoplossing voor SD-WAN cEdge IPsec anti-terugspelen fouten

Inhoud

Inleiding

Dit document beschrijft het gedrag van IPsec Anti-Replay in SD-WAN IPsec voor cEdge-routers en hoe u problemen met Anti-Replay kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)
- Internet Protocol Security (IPsec)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C800V versie 17.06.01
- ASR 1001-X versie 17.06.03a
- vManager versie 20.7.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

IPsec-verificatie biedt ingebouwde bescherming tegen terugspelen tegen oude of gedupliceerde IPsec-pakketten, waarbij het volgnummer in de ESP-header is ingeschakeld op de ontvanger. Anti-replay pakketdruppels is een van de meest voorkomende dataplatform-problemen met IPsec vanwege pakketten die buiten het venster voor anti-replay worden geleverd. Een algemene probleemoplossingsbenadering voor IPsec anti-replay druppels kan worden gevonden in IPsec Anti Replay Check Failures, en de algemene techniek is ook van toepassing op SD-WAN. Er bestaan echter enige implementatieverschillen tussen traditionele IPsec en IPsec die worden gebruikt in de Cisco SD-WAN oplossing. Dit artikel is bedoeld om deze verschillen en de benadering op de cEdge-platforms met Cisco IOS ®XE te verklaren.

Overwegingen bij SD-WAN Replay Detectie

Group Key vs. Pairwise Key

In tegenstelling tot traditionele IPsec, waar IPsec SA's worden onderhandeld tussen twee peers met behulp van het IKE-protocol, maakt SD-WAN gebruik van een groepssleutelconcept. In dit model genereert een SD-WAN randapparaat periodiek dataplatform inbound SA per TLOC en stuurt deze SA's naar de vSmart controller, die op zijn beurt de SA doorgeeft aan de rest van de randen apparaten in het SD-WAN netwerk. Voor een meer gedetailleerde beschrijving van de SD-WAN dataplatformbewerkingen, zie SD-WAN Data Plane Security Overzicht.

> **Opmerking**: sinds Cisco IOS ®XE. 6.12.1a/SD-WAN 19.2, IPsec-paarsgewijze toetsen worden ondersteund. Zie Overzicht van IPsec-paarsgewijze toetsen. Met paarsgewijze toetsen werkt IPsec anti-replay bescherming precies zoals traditionele IPsec. Dit artikel richt zich primair op replay check met het gebruik van het groepssleutelmodel.

Gecodeerde SPI

In de IPsec ESP-header is de SPI (Security Parameter Index) een 32-bits waarde die de ontvanger gebruikt om de SA te identificeren waarmee een inkomend pakket wordt gedecrypteerd. Met SD-WAN kan deze inkomende SPI worden geïdentificeerd met **show crypto ipsec sa**:

```
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)
```

Opmerking: ook al is de inkomende SPI hetzelfde voor alle tunnels, de ontvanger heeft een andere SA en het correspondent replay-venster object gekoppeld aan de SA voor elk peer-edge apparaat, aangezien de SA wordt geïdentificeerd door de bron, bestemming IP-adres, bron, bestemmingspoorten 4-tuple, en het SPI-nummer. In wezen heeft elke peer zijn eigen venster-object tegen herhaling.

In het daadwerkelijke pakket dat door het peer apparaat wordt verzonden, merk op de waarde van SPI van de vorige output verschillend is. Hier is een voorbeeld van de uitvoer van het pakketspoor met de toegelaten optie van het pakketexemplaar:

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

De eigenlijke SPI in de ESP-header is **0x04000123.** De reden hiervoor is dat de eerste bits in de SPI voor SD-WAN gecodeerd worden met aanvullende informatie, en dat alleen de lage bits van het SPI-veld toegewezen worden voor de eigenlijke SPI.

Traditionele 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)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

waarbij:

- **CTR** (eerste 4 bits, bits 0-3) - Control Bits, gebruikt om het specifieke type controlepakketten aan te geven. Zo wordt control bit 0x80000000 bijvoorbeeld gebruikt voor BFD.
- **MSNS** (volgende 3 bits, bits 4-6) - Meervoudige Sequence Number Space Index. Dit wordt gebruikt om de juiste sequentieteller in de sequentieteller-array te vinden om op terugspelen voor het gegeven pakket te controleren. Voor SD-WAN maakt de 3-bits MSNS het mogelijk dat 8 verschillende verkeersklassen in hun eigen sequentienummerruimte worden toegewezen. Dit impliceert de efficiënte waarde van SPI die voor selectie kan worden gebruikt SA is de verminderde lage orde 25 beetjes van de volledige waarde met 32 bits van het gebied.

Meervoudige sequentienummer voor QoS

Het is gebruikelijk om IPsec-terugspeelfouten te observeren in een omgeving waar pakketten niet op orde worden geleverd door QoS, bijvoorbeeld LLQ, omdat QoS altijd na IPsec-encryptie en insluiting wordt uitgevoerd. De Meervoudige Oplossing van de Ruimte van het Volgnummer lost dit probleem met het gebruik van de veelvoudige ruimten van het opeenvolgingsaantal die aan

verschillende QoS verkeersklassen voor een bepaalde Vereniging van de Veiligheid in kaart worden gebracht op. De verschillende ruimte van het opeenvolgingsaantal wordt geïndexeerd door de beetjes MSNS die in het ESP veld van pakketSPI zoals afgebeeld worden gecodeerd. Zie IPsec Anti Replay Mechanism voor QoS voor een meer gedetailleerde beschrijving.

Zoals eerder opgemerkt, impliceert deze Meervoudige implementatie van het Aantal van de Opeenvolging de efficiënte waarde van SPI die voor selectie kan worden gebruikt SA de verminderde lage orde 25 beetjes is. Een andere praktische overweging wanneer de replay venstergrootte met deze implementatie wordt gevormd is dat de gevormde replay-venstergrootte voor het gezamenlijke replay venster is, zodat is de efficiënte replay venstergrootte voor elke Ruimte van het Aantal van de Opeenvolging 1/8 van het totaal.

Configuratievoorbeeld:

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

> **Opmerking**: de effectieve replay venstergrootte voor elke Sequence Number Space is 1024/8 = 128!

> **Opmerking**: sinds Cisco IOS ®XE. 17.2.1 is de totale grootte van het replay venster verhoogd tot 8192 zodat elke Sequence Number Space een maximaal replay venster van 8192/8 = 1024 pakketten kan hebben.

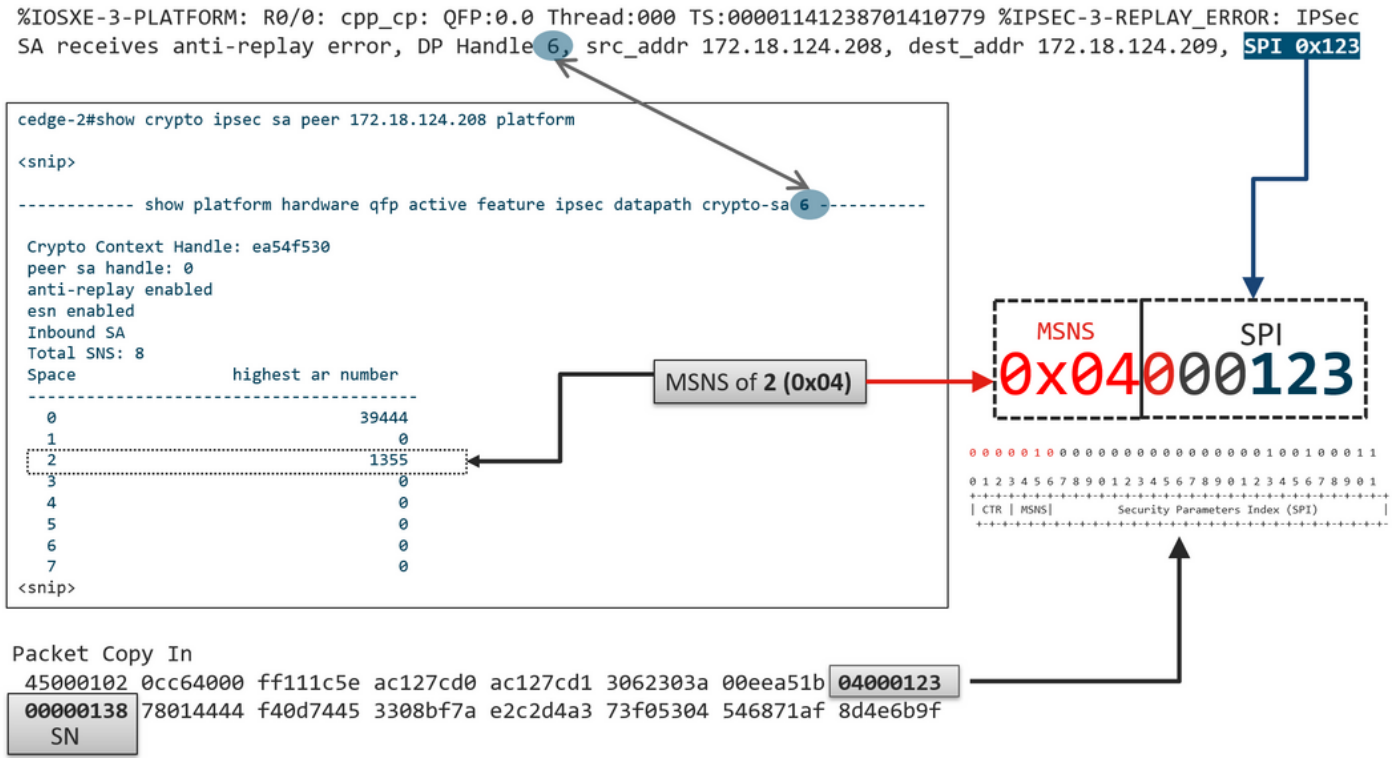
Op een cEdge-apparaat kan het laatste volgnummer dat voor elke ruimte in het volgnummer is ontvangen, worden verkregen uit de output van het **showcrypto ipsec als peer x.x.x.x platform** IPsec dataplane:

```
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>
```

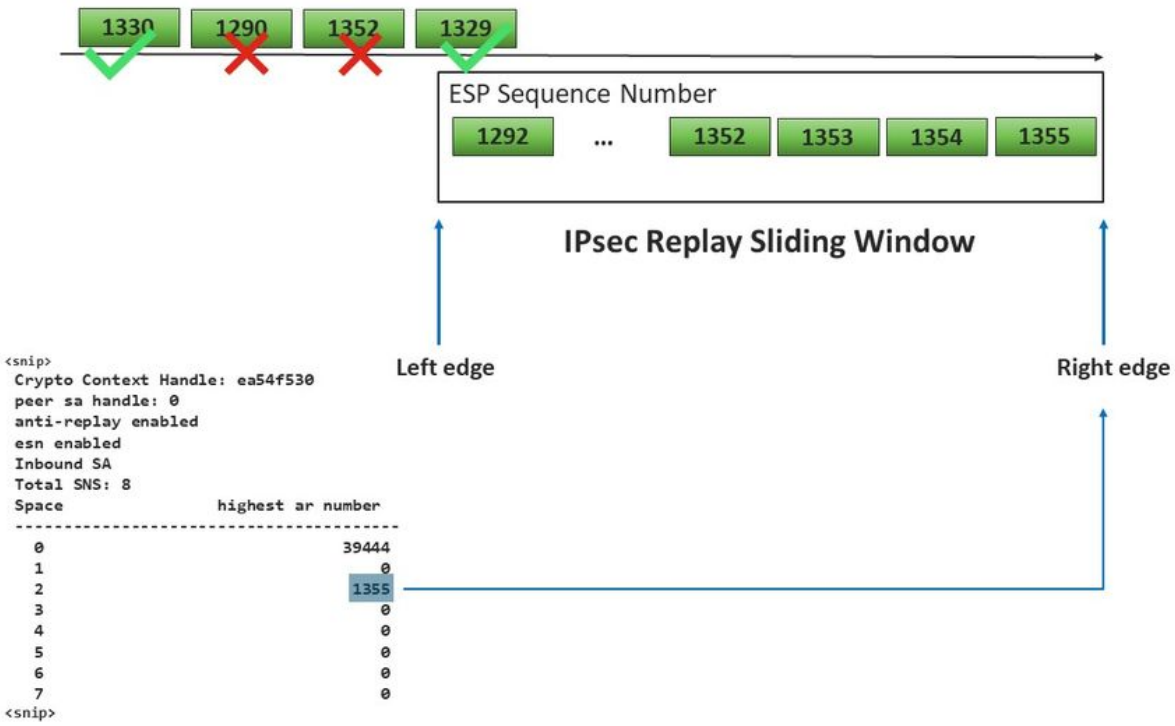
In het voorbeeld is het hoogste anti-replay venster (rechterrand van het anti-replay schuifvenster) voor MSNS van 0 **(0x00)** is **3944**, en dat voor MSNS van **2 (0x04)** is **1335**, en deze tellers worden gebruikt om te controleren of het opeenvolgingsaantal binnen van het replay venster voor pakketten in de zelfde ruimte van het opeenvolgingsaantal is.

> **Opmerking**: er zijn implementatieverschillen tussen het ASR1k-platform en de rest van de Cisco IOS ®XE-routerplatforms (ISR4k, ISR1k, CSR1kv). Dientengevolge, zijn er sommige discrepanties in termen van de showbevelen en hun output voor deze platforms.

Het is mogelijk om de Anti-Replay fouten en de show output te corraliëren om de SPI, en de Sequence number index zoals getoond in het beeld te vinden.



Met de vorige informatie verkregen de rechterrand (bovenste venster) en het glijdende venster ziet eruit zoals getoond in de afbeelding.



Opdrachten om de effectiviteit van het geconfigureerde terugspeelvenster te realiseren

In tegenstelling tot de gewone IPsec (niet SD-WAN) wordt de opdracht rekey niet van kracht voor het venster voor anti-terugspelen.

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

Met deze opdrachten wordt het ingesteld terugspeelvenster geactiveerd:

> **Waarschuwing**: zorg ervoor dat u de potentiële impact van een opdracht begrijpt, ze beïnvloeden de besturingsverbindingen en het dataplatform.

```
clear sdwan control connection
```

of

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

of

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

Fouten in Replay Drop (terugspelen) voor probleemoplossing

Probleemoplossing voor gegevensverzameling

Voor de druppels van de IPsec-antireplay is het belangrijk dat u de omstandigheden en mogelijke triggers van het probleem begrijpt. Verzamel ten minste de informatie die nodig is om de context te bieden:

- Apparaatinformatie voor zowel de zender als de ontvanger voor de replay-pakketdruppels, het bevat het type apparaat, cEdge vs. vEdge, softwareversie en configuratie.
- Probleemgeschiedenis. Hoe lang is de inzet al gerealiseerd? Wanneer is het probleem begonnen? Eventuele recente wijzigingen in het netwerk of de verkeersomstandigheden.
- Enig patroon van de terugspelen druppels, bijvoorbeeld., is het sporadisch of constant? Tijdstip van het probleem en/of belangrijke gebeurtenis, bijvoorbeeld, gebeurt het alleen tijdens hoge piekuren van het verkeer, of alleen tijdens rekey, enzovoort.?

Met de vorige verzamelde informatie, ga met de probleemoplossingswerkstroom verder.

Werkstroom voor probleemoplossing

De algemene benadering van probleemoplossing voor IPsec-replay problemen is net als hoe het wordt uitgevoerd voor traditionele IPsec, rekening houden met de per-peer SA-sequentieruimte en de Meervoudige Sequence Number-ruimte zoals uitgelegd. Ga vervolgens door deze stappen:

Stap 1. Identificeer eerst de peer voor de replay drop van de syslog en de drop rate. Voor drop-statistieken verzamelt u altijd meerdere getimede momentopnamen van de uitvoer, zodat de drop rate kan worden gekwantificeerd:

```
*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
```

> **Opmerking**: het is niet ongebruikelijk om incidentele terugspeeldruppels te zien als gevolg van pakketbezorging die in het netwerk opnieuw geordend wordt, maar aanhoudende terugspeeldruppels beïnvloeden de service en kunnen worden onderzocht.

Stap 2a. Voor relatief weinig verkeer kunt u een packet-trace nemen met de voorwaarde die is ingesteld als het peer-ipv4-adres met de optie **Copy Packet** en de sequentienummers onderzoeken voor het pakket dat is gedropt tegen de huidige rechts rand van het terugspeelvenster en de sequentienummers in de aangrenzende pakketten om te bevestigen of deze inderdaad duplicaat zijn of buiten het terugspeelvenster.

Stap 2b. Voor een hoge verkeerssnelheid zonder voorspelbare trigger moet u een EPC-opname met circulaire buffer en EEM configureren om de opname te stoppen wanneer replay-fouten worden gedetecteerd. Aangezien EEM momenteel niet wordt ondersteund op vManager vanaf

19.3, impliceert dit dat de cEdge in CLI-modus moet zijn wanneer deze probleemoplossing wordt uitgevoerd.

Stap 3. Verzamel de **show crypto ipsec als peer x.x.x.x** platform op de ontvanger in het meest ideale geval op hetzelfde moment dat de pakketopname of het pakketspoor wordt verzameld. Deze opdracht bevat de realtime-vensterinformatie voor het terugspelen van dataplane voor zowel de inkomende als de uitgaande SA.

Stap 4. Als het pakketverlies inderdaad niet goed werkt, neem dan gelijktijdige opnamen van zowel de afzender als de ontvanger om te identificeren als het probleem met de bron of met de laag van het onderliggennetwerk is.

Stap 5. Als de pakketten worden gelaten vallen ook al zijn ze noch duplicaat noch buiten het replay venster, dan is het meestal een aanwijzing voor een softwareprobleem op de ontvanger.

Voorbeeld van probleemoplossing voor ASR 1001-x

Probleembeschrijving:

HP: ASR 1001-X
SW: 17.06.03a

Meervoudige Anti-replay fouten ontvangen voor de sessie peer 10.62.33.91, daarom de BFD sessie voortdurend flaps en het verkeer tussen deze twee sites wordt beïnvloed.

```
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
```

Stap 1. Controleer geconfigureerd anti-terugspelen venster is 8192.

```
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"
```

> **Opmerking**: de effectieve grootte van het terugspeelvenster voor elke sequentienummer ruimte moet 8192/8= 1024 zijn in dit voorbeeld.

Stap 2. Controleer de effectieve grootte van het terugspeelvenster voor peer 10.62.33.91 om de ingestelde waarde te vergelijken en te bevestigen.

```
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
```

Het venstergrootte: 64 weergegeven in de uitvoer niet overeenkomt met wat het ingestelde terugspeelvenster 8192 (8192/8=1024)Dat betekent dat zelfs het was geconfigureerd het commando niet van kracht werd.

> Opmerking: het effectieve terugspeelvenster wordt alleen op de ASR-platforms weergegeven. Als u er zeker van wilt zijn dat de feitelijke grootte voor het venster voor anti-terugspelen hetzelfde is als de ingestelde grootte, past u een van de opdrachten in de sectieopdrachten toe om de effectiviteit van het geconfigureerde venster voor terugspelen te nemen.

Stap 3. Configureer pakkettracering en monitorvastlegging (optioneel) tegelijkertijd voor inkomend verkeer vanaf sessiebron: 10.62.33.91, bestemming: 10.62.63.251

```
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
```

Stap 4. Samenvatting van pakkettracering verzamelen:

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

Stap 5. Vouw een aantal opgenomen gevallen (IPsec Input) pakketten uit.

(IPsec (invoer) pakketdruppels:

```
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-WAN gebruikt in ESP ingesloten UDP:

- De UDP-header is 304f303b 00770000,
- De volgende is SPI (**04000106**)
- Daarom is **00b6e00d** het serienummer (SN).
- De MSNS-index is **2** (**x04**00106) vanwege 32-bits SPI (**0 0 0 0 1 0 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1 1.)

Stap 6. Controleer de MSNS-index

```
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
```

Het hoogste anti-replay venster (rechterrand van het anti-replay schuifvenster) voor MSNS van 2 (0x04) is **0b65f00.**

Stap 7. Breid enkele doorgestuurde (FWD) opgenomen pakketten uit.

Doorgestuurde pakketten:

```
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
```

Packet: 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
```

Stap 8. Verzamel en verkrijg de volgnummer informatie uit meerdere pakketten doorgestuurd (FWD) voor, na en de druppels.

```
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
```

Stap 9. Converteer naar Decimal the SN en bestel deze naar eenvoudige berekening:

```
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
```

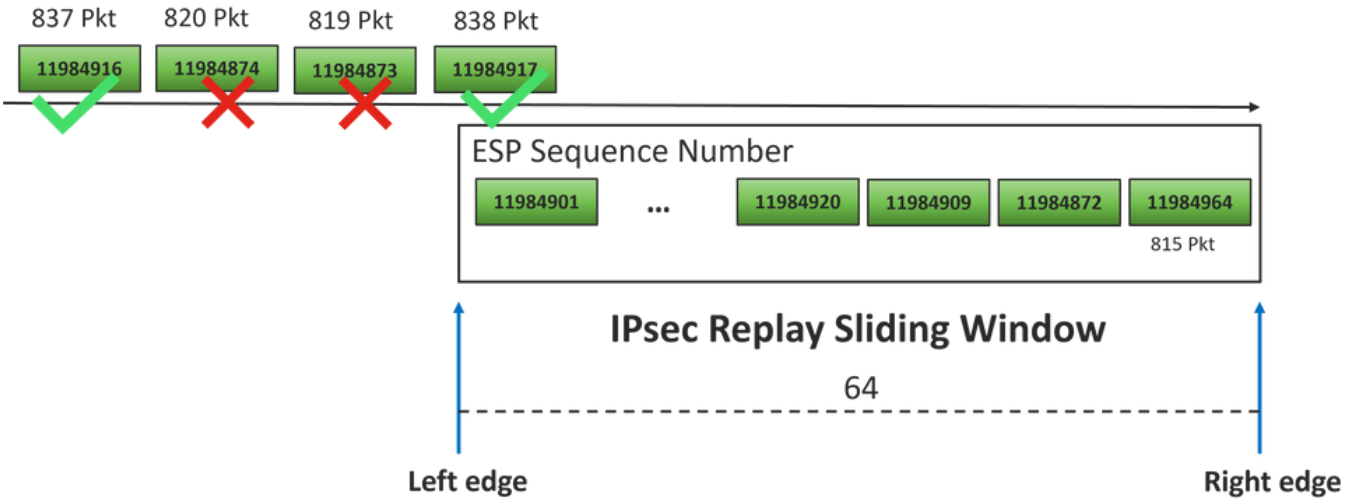
> Opmerking: Als het volgnummer groter is dan het hoogste volgnummer in het venster, wordt de integriteit van het pakket gecontroleerd. Als het pakket de integriteitscontrole passeert, wordt het glijvenster naar rechts verplaatst.

Stap 10. Converteer naar Decimal the SN en bestel deze naar eenvoudige berekening:

```
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
```

Bij dit voorbeeld is het mogelijk om het schuifvenster te visualiseren met **venstergrootte 64** en de **rechterrand11984964** zoals in de afbeelding.



Het ontvangen opeenvolgingsaantal voor dalingspakketten is ver voor de juiste rand van het terugspeelvenster voor die opeenvolgingsruimte.

Oplossing

Aangezien het vensterformaat nog steeds de vorige waarde 64 heeft, zoals in stap 2 is beschreven, moet een van de opdrachten in het vak Opdrachten om de effectiviteit van het geconfigureerde terugspeelvenster te bereiken, worden toegepast om ervoor te zorgen dat de venstergrootte 1024 van invloed is.

Aanvullende Wireshark Capture Tool

Een andere handige tool om de ESP SPI en het volgnummer te correleren is de Wireshark software.

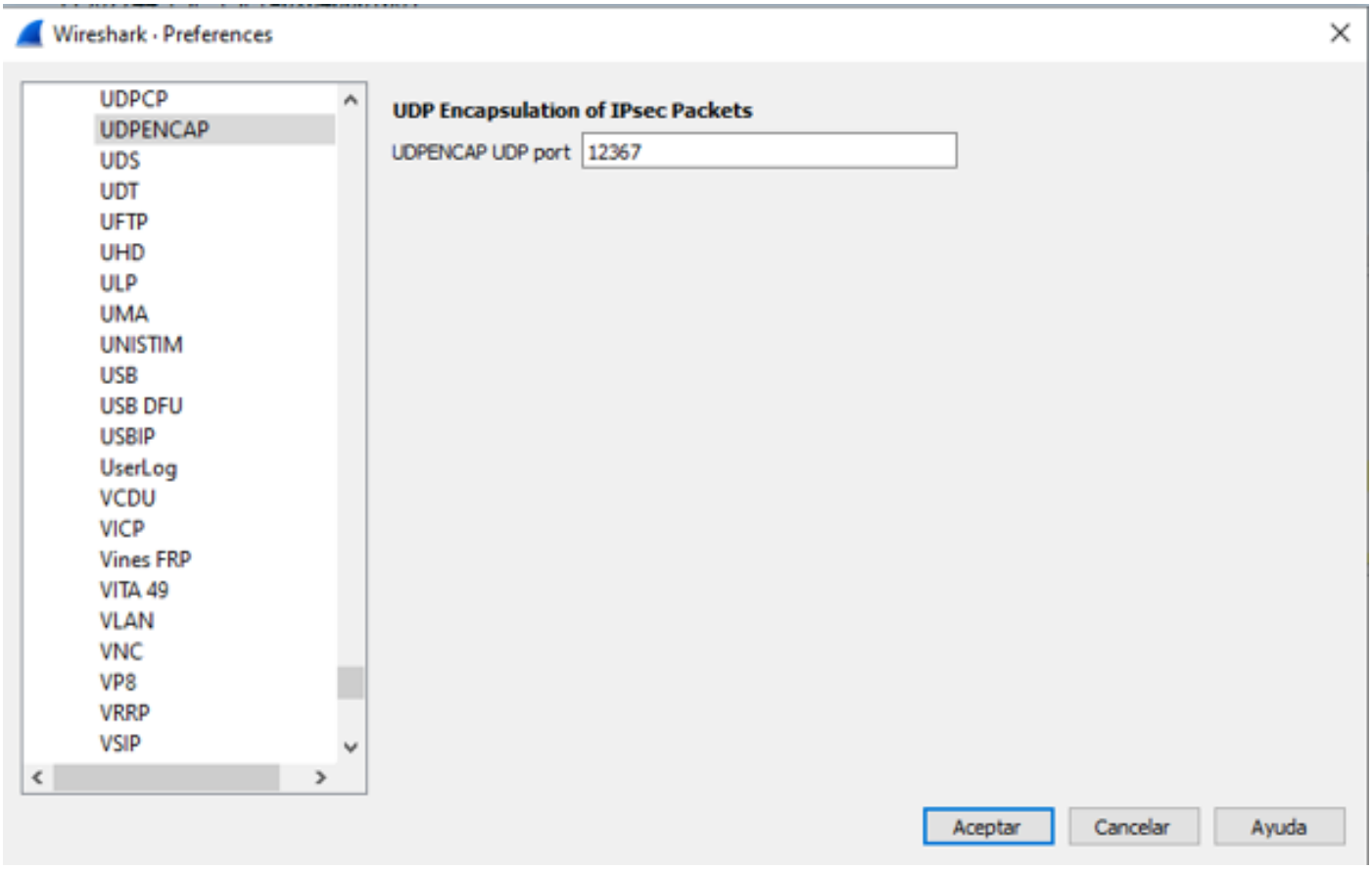
> **Opmerking**: het is belangrijk om het pakketvastlegging te verzamelen wanneer het probleem optreedt en als het mogelijk is om tegelijkertijd het fia-spoor te verzamelen zoals eerder beschreven

Configureer de pakketopname voor inkomende richting en exporteer deze naar het PCAP-bestand.

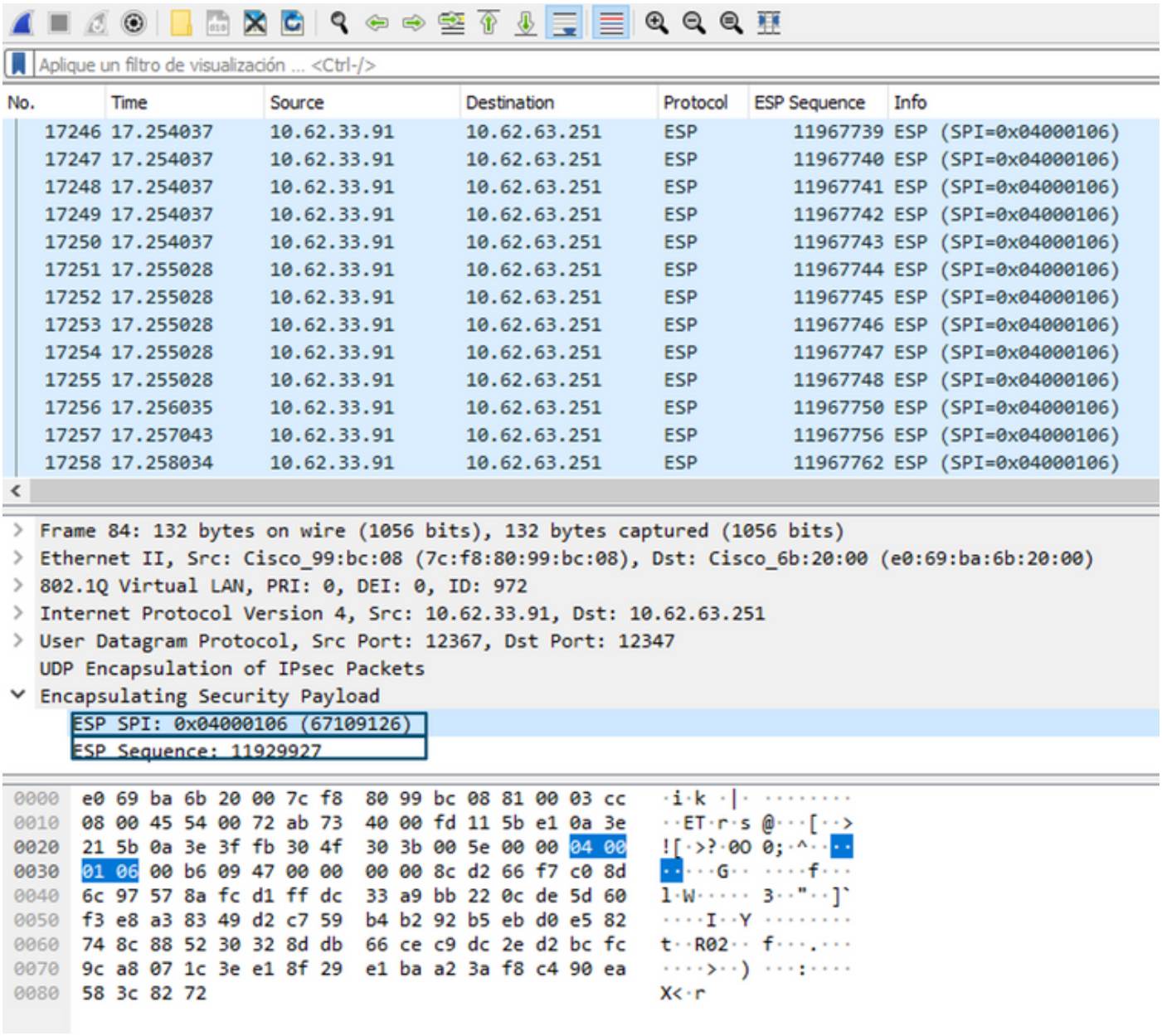
```
monitor caputure CAP match ipv4 host 10.62.33.91 host 10.62.63.251 buffer size 20 inter
TenGigabitEthernet0/0/0 in
monitor caputure CAP star
monitor caputure CAP stop
monitor caputure CAP export bootflash:Anti-replay.pca
```

Wanneer pcap-opname wordt geopend in Wireshark, om het ESP SPI- en volgnummer te kunnen zien, één pakket uit te vouwen, rechtsklik en selecteer **protocolvoorkeuren**, zoek naar **UDPENCAP**

en verander de standaardpoort naar SD-WAN poort (bronpoort) zoals in het beeld.



Nadat UDPENCAP met de juiste poort is geïnstalleerd, wordt de ESP-informatie nu weergegeven zoals in het beeld.



Gerelateerde informatie

- [TechZone-artikel voor IPsec-controle tegen terugspelen]
- [IPsec Anti-Replay-venster uitbreiden en uitschakelen]
- [Cisco technische ondersteuning en downloads]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.