排除SD-WAN cEdge IPsec Anti Replay故障

目錄

簡介

本文檔介紹適用於cEdge的SD-WAN IPsec路由器中的IPsec反重播行為，以及如何排除反重播問題。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- 網際網路通訊協定安全(IPsec)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IPsec身份驗證針對在接收方檢查的ESP報頭中的序列號為舊或重複的IPsec資料包提供內建的反重播保護。由於資料包在反重播視窗外以亂序傳送，因此反重播資料包丟棄是IPsec最常見的資料平面問題之一。在IPsec Anti Replay Check Failures中可找到IPsec反重播丟棄的一般故障排除方法，該通用技術也適用於SD-WAN。但是，在Cisco SD-WAN解決方案中使用的傳統IPsec和IPsec之間存在一些實施差異。本文旨在解釋這些差異以及使用Cisco IOS ®XE的cEdge平台上的方法。

SD-WAN重放檢測注意事項

組金鑰與成對金鑰

SD-WAN與傳統IPsec不同，傳統IPsec SA是使用IKE協定在兩個對等體之間協商的，SD-WAN使用組金鑰概念。在此模型中，SD-WAN邊緣裝置定期生成每個TLOC的資料平面入站SA，並將這些SA傳送到vSmart控制器，而vSmart控制器又將SA傳播到SD-WAN網路中的其餘邊緣裝置。有關SD-WAN資料平面操作的更詳細說明，請參閱SD-WAN資料平面安全概述。

> **註**：自Cisco IOS ®XE。 支援6.12.1a/SD-WAN 19.2,IPsec成對金鑰。請參閱IPsec Pairwise金鑰概述。使用Pairwise金鑰時，IPsec防重播保護的工作方式與傳統IPsec完全相同。本文重點介紹使用組金鑰模型重播檢查的方法。

編碼的SPI

在IPsec ESP報頭中，SPI（安全引數索引）是一個32位值，接收方使用該值來標識入站資料包解密到的SA。使用SD-WAN時，可以使用**show crypto ipsec sa**標識此入站SPI:

```
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)
```

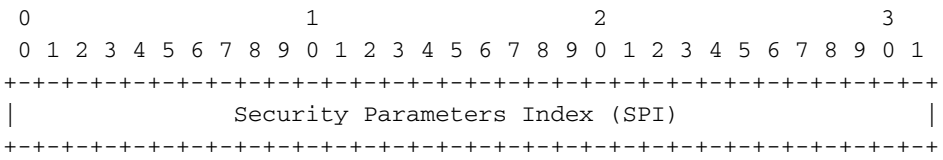
> **註**：即使所有隧道的入站SPI都相同，但接收方對每個對等邊緣裝置的SA都有一個不同的SA以及與該SA關聯的對應重放視窗對象，因為SA由源、目標IP地址、源、目標埠4元組和SPI編號標識。因此，本質上，每個對等體都有自己的反重放視窗對象。

在對等裝置傳送的實際資料包中，請注意SPI值不同於先前的輸出。以下是已啟用packet copy選項的packet-trace輸出範例：

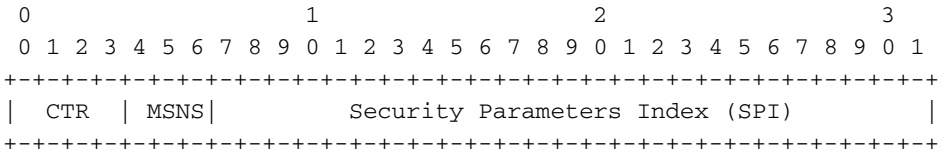
```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

ESP報頭中的實際SPI為0x04000123。其原因在於SD-WAN的SPI中的第一個位被附加資訊編碼，並且只有該SPI欄位的低位被分配給實際的SPI。

傳統IPsec:



SD-WAN:



其中：

- **CTR**（前4位，0-3位）— 控制位，用於指示特定型別的控制資料包。例如，控制位0x80000000用於BFD。
- **MNS**（接下來的3位，4-6位）— 多序號空間索引。這用於在序列計數器陣列中定位正確的序列計數器，以檢查給定資料包的重放。對於SD-WAN，MNS的3位允許將8個不同的流量類對映到它們自己的序列號空間。這表示可用於SA選擇的有效SPI值是欄位的完整32位值中低位25位。

用於QoS的多序列號空間

在由於QoS（例如LLQ）而亂序傳送資料包的環境中，通常觀察IPsec重放故障，因為QoS始終在IPsec加密和封裝之後運行。多序號空間解決方案通過使用對映到給定安全關聯的不同QoS流量類別的多個序號空間來解決該問題。不同的序列號空間按所示的ESP資料包SPI欄位中編碼的MSNS位索引。有關更詳細的說明，請參閱適用於QoS的IPsec反重播機制。

如前所述，此多序列號實現意味著可用於SA選擇的有效SPI值是低位25位。使用此實現配置重放視窗大小時的另一個實際考慮是，配置的重放視窗大小用於聚合重放視窗，因此每個序列號空間的有效重放視窗大小是聚合的1/8。

組態範例:

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

> **註**：每個序列號空間的有效重放視窗大小為1024/8 = 128!

> **附註**：自Cisco IOS ®XE起。17.2.1聚合重放視窗大小已增加到8192，因此每個序列號空間的最大重放視窗為8192/8 = 1024資料包。

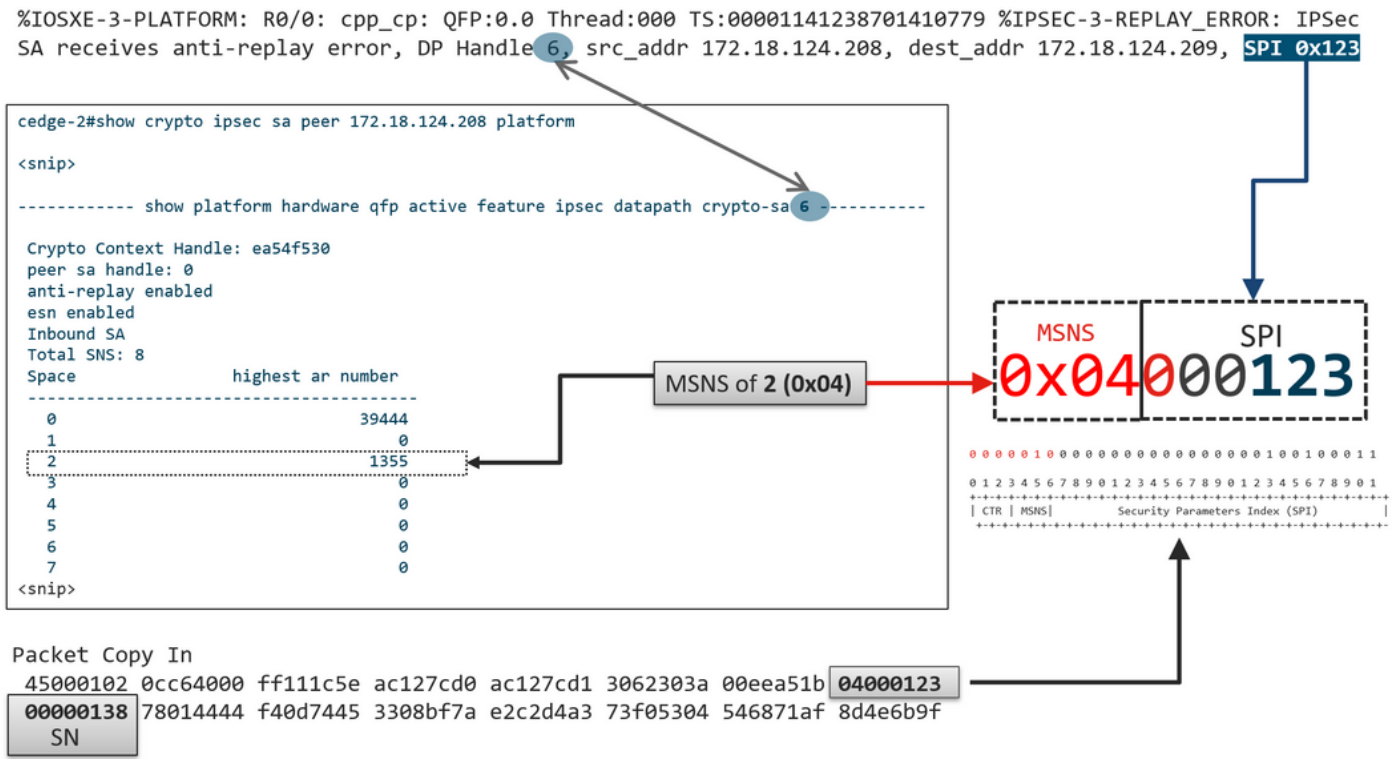
在cEdge裝置上，可從**show crypto ipsec sa peer x.x.x.x platform** IPsec資料平面輸出獲取每個序列號空間接收的最後一個序列號：

```
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>
```

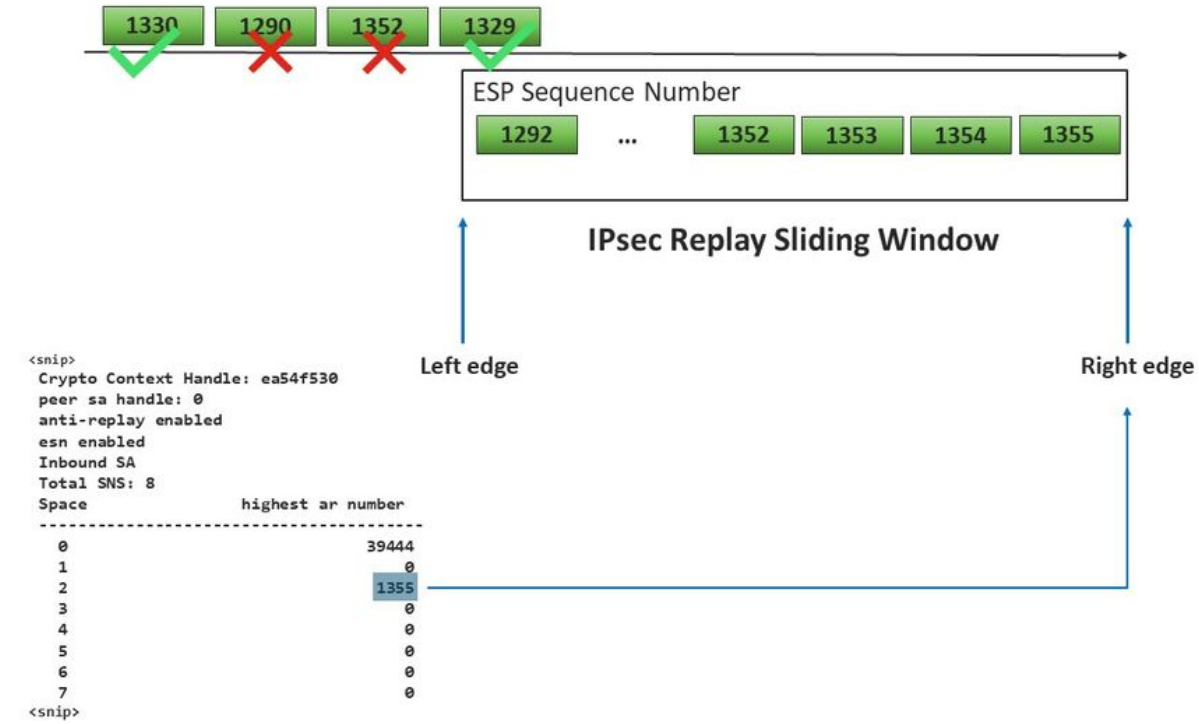
在本示例中，MNS為0(0x00)的最高反重放視窗（反重放滑動視窗的右邊緣）是**39444**，而**2(0x04)的MNS的最高反重放視窗（反重放滑動視窗的右邊緣）是1335**，這些計數器用於檢查序列號是否在同一個序列號空間中的資料包位於重放視窗內。

> **註**:ASR1k平台與其他Cisco IOS ®XE路由平台(ISR4k、ISR1k、CSR1kv)之間存在實施差異。因此，這些平台的show命令及其輸出存在一些差異。

可以將Anti-Replay錯誤與show輸出關聯以查詢SPI和序列號索引，如圖所示。



利用以前獲得的資訊，右邊緣（頂部視窗）和滑動視窗的外觀如圖所示。



使已配置的重放視窗有效的命令

與常規IPsec（非SD-WAN）不同，rekey命令對反重放視窗無效。

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

這些命令將觸發已配置的重播視窗生效：

警告：確保您瞭解任何命令的潛在影響，它們將影響控制連線和資料平面。

```
clear sdwan control connection
```

或

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

或

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

排除重播丟棄故障

資料收集故障排除

對於IPsec反重播丟包，瞭解問題的條件和潛在觸發因素非常重要。至少要收集的一組資訊以提供上下文：

- 重放資料包丟棄的傳送方和接收方的裝置資訊，包括裝置型別、cEdge與vEdge、軟體版本和配置。
- 問題歷史記錄。部署已部署多長時間？ 問題是什麼時候開始的？網路或流量條件最近的任何更改。
- 重播丟棄的任何模式，例如，它是零星的還是恆定的？問題和/或重要事件的時間，例如，它是否僅在高流量高峰生產時間發生，還是僅在重新生成金鑰期間發生，以此類推？

在收集了上述資訊後，繼續執行故障排除工作流程。

工作流故障排除

針對IPsec重播問題的常規故障排除方法類似於針對傳統IPsec執行此故障排除的方法，如說明的那樣，該方法考慮了每個對等體的SA序列空間和多序列號空間。然後執行以下步驟：

步驟1。首先確定系統日誌中重放丟棄的對等項和丟棄率。對於刪除統計資訊，請始終收集輸出的多個帶有時間戳的快照，以便可以驗證刪除率：

```
*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
```

注意：由於網路中的資料包傳輸重新排序，偶爾出現重放丟棄並不罕見，但持續重放丟棄會影響服務，可以對這些問題進行調查。

步驟 2a. 對於相對較低的通訊速率，請執行條件設定為具有**copy packet**選項的對等ipv4地址的資料包跟蹤，並根據當前重放視窗右邊緣和相鄰資料包中的序列號檢查被丟棄的資料包的序列號，以確認它們確實是重複的資料包還是在重放視窗之外。

步驟2b。 對於沒有可預測的觸發器的高流量速率，請配置帶有循環緩衝區和EEM的EPC捕獲，以便在檢測到重放錯誤時停止捕獲。由於從19.3開始，vManage目前不支援EEM，因此在執行此故障排除任務時，cEdge必須處於CLI模式。

步驟3.在收集封包擷取或封包追蹤的同時，理想地在接收者上收集**show crypto ipsec sa peer x.x.x.x**平台。此命令包括入站和出站SA的即時資料平面重放視窗資訊。

步驟4.如果丟棄的資料包確實順序有誤，則同時從傳送方和接收方進行捕獲，確定問題出在源還是底層網路傳輸層。

步驟5.如果資料包被丟棄，即使它們既不重複也不在重放視窗之外，則通常指示接收方存在軟體問題。

ASR1001-x故障排除示例

問題描述：

硬體：ASR1001-X
軟體：17.06.03a

收到會話對等體10.62.33.91的多個反重播錯誤，因此BFD會話不斷波動，並且這兩個站點之間的流量會受到影響。

```
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
```

步驟1.檢查Configured Anti Replay Window 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"
```

註：在本例中，每個序列號空間的有效重放視窗大小必須為8192/8= 1024。

步驟2. 驗證對等10.62.33.91的有效重放視窗大小，以比較並確認配置值。

```
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
```

其 **視窗大小：64** 輸出中顯示的內容與配置的重播視窗不匹配 **8192(8192//8=1024)**，這意味著即使配置了該命令，該命令也不會生效。

註：有效重放視窗僅顯示在ASR平台上。為了確保反重放視窗的實際大小與配置的大小相同，請應用section命令中的某個命令以使configured replay視窗生效。

步驟3.為來自會話源10.62.33.91、目標10.62.63.251的入站流量同時配置並啟用資料包跟蹤和監控捕獲（可選）

```
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
```

步驟4. 收集資料包跟蹤摘要：

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

步驟5. 展開捕獲的一些丟棄(IpsecInput)資料包。

(IpsecInput)Packet drops:

```
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使用UDP封裝的ESP:

- UDP報頭是304f303b 00770000,
- 下一個是SPI(**04000106**)
- 因此**00b6e00d**是安全編號(SN)。
- 由於32位SPI(**0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1),MSNS索引為**2(x 04**00106)。

步驟6.驗證MNS索引

```
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
```

對於MSNS為2(0x04)的最高防重放視窗（防重放滑動視窗的右邊緣）是**0b65f00。**

步驟7. 展開一些已轉發(FWD)捕獲的資料包。

轉發資料包：

```
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
```

資料包：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
```

步驟8. 在丟棄之前、之後和丟棄之前從多個轉發的資料包(FWD)收集並獲取序列號資訊。

```
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
```

步驟9. 將SN轉換為十進位制，並將它們重新排序為簡單計算：

```
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
```

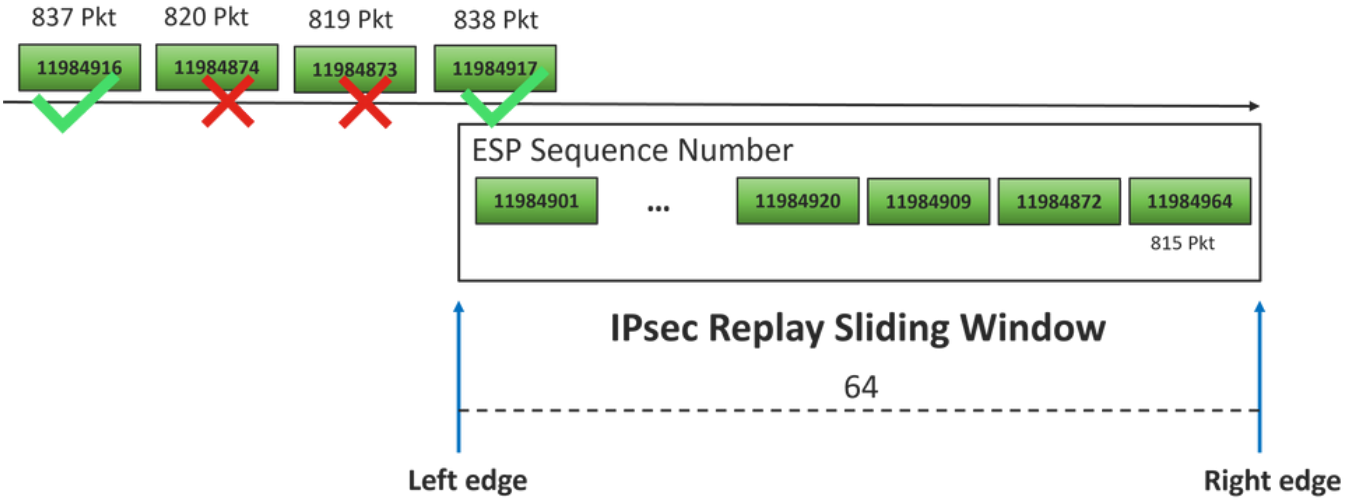
> **注意**:如果序列號大於視窗中的最高序列號，則檢查資料包的完整性。如果資料包通過完整性驗證檢查，則滑動視窗將移動到右側。

步驟10. 將SN轉換為十進位制，並將它們重新排序為簡單計算：

```
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
```

11984964在本例中，可以將**視窗大小64**和**右邊緣**的滑動視窗視覺化，如下圖所示。



所接收的丟棄資料包的序列號遠遠超出該序列空間的重放視窗的右邊緣。

解決方案

由於視窗大小仍位於先前值64中（如步驟2所示），所以為了使用1024視窗大小生效，需要應用「使已配置的重放視窗生效」一節中的命令之一。

其他Wireshark捕獲工具

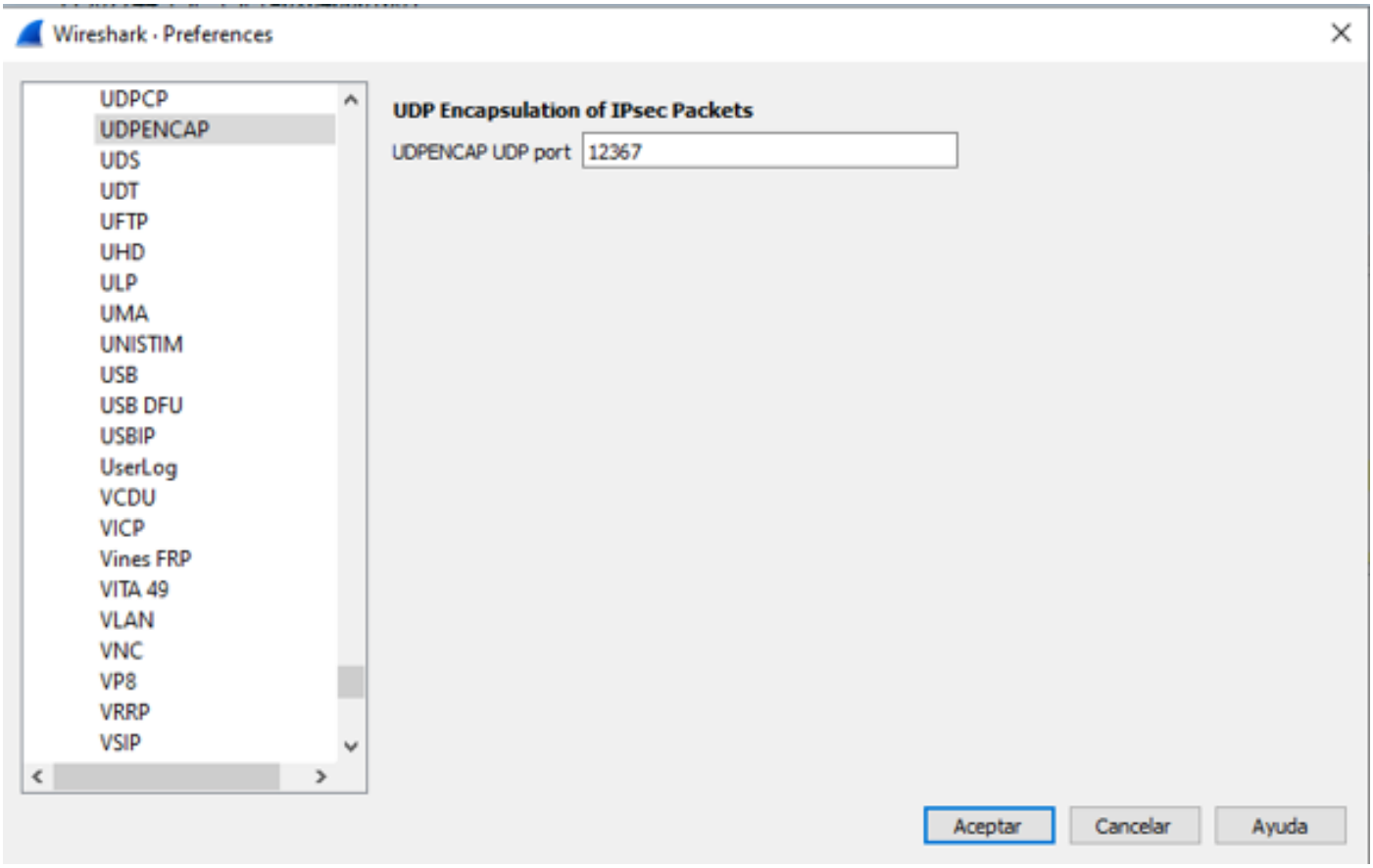
Wireshark軟體是幫助關聯ESP SPI和序列號的另一個有用工具。

> **註**：出現問題時收集資料包捕獲是非常重要的，如果可能的話，則同時按前面所述收集FIA跟蹤

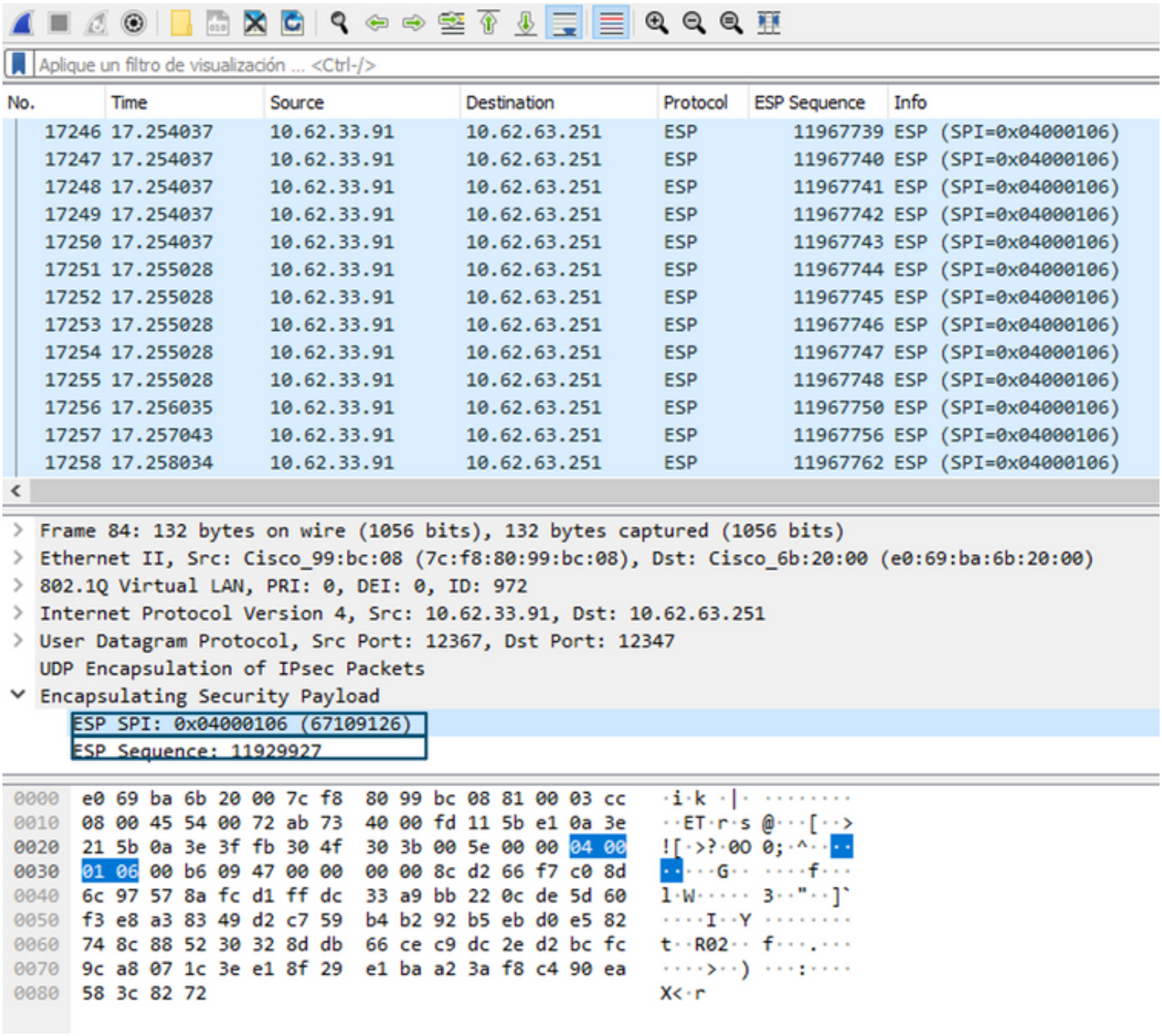
配置入站方向的資料包捕獲並將其匯出到pcap檔案。

```
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
```

在Wireshark中開啟pcap結構時，為了能夠檢視ESP SPI和序列號，請展開一個資料包，按一下右鍵並選擇協定首選項，搜尋**UDPENCAP**，並將預設埠更改為SD-WAN埠（源埠），如下圖所示。



在正確的埠設定了UDPENCAP後，現在將顯示ESP資訊，如下圖所示。



相關資訊

- [IPsec Anti-Replay Check Failures TechZone文章]
- [IPsec Anti-Replay視窗正在擴展和禁用]
- [思科技術支援與下載]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。