排除SD-WAN cEdge IPsec防重播故障

目录

简介

本文档介绍适用于cEdge路由器的SD-WAN IPsec中的IPsec反重播行为，以及如何解决反重播问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- Internet协议安全(IPsec)

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

IPsec身份验证针对旧或重复的IPsec数据包提供内置的反重播保护，并在接收方上检查了ESP报头中的序列号。由于数据包在反重播窗口外按顺序传送，因此反重播数据包丢弃是IPsec最常见的数据平面问题之一。在IPsec Anti Replay Check Failures中可以找到用于IPsec反重播丢弃的常规故障排除方法，该常规技术也适用于SD-WAN。但是，在Cisco SD-WAN解决方案中使用的传统IPsec和IPsec之间存在一些实施差异。本文旨在解释这些差异以及采用Cisco IOS ®XE的cEdge平台上的方法。

SD-WAN重放检测注意事项

组密钥与成对密钥

与传统IPsec不同，SD-WAN使用IKE协议在两个对等体之间协商IPsec SA，SD-WAN使用组密钥概念。在此模式中，SD-WAN边缘设备定期生成每个TLOC的数据平面入站SA，并将这些SA发送到vSmart控制器，后者再将SA传播到SD-WAN网络中的其余边缘设备。有关SD-WAN数据平面操作的更详细说明，请参阅SD-WAN数据平面安全概述。

> **注**：自Cisco IOS ®XE起。 支持6.12.1a/SD-WAN 19.2,IPsec成对密钥。请参阅IPsec Pairwise密钥概述。使用Pairwise密钥，IPsec反重播保护的工作方式与传统IPsec完全相同。本文重点研究重播检查与组密钥模型的使用。

编码的SPI

在IPsec ESP报头中，SPI（安全参数索引）是一个32位值，接收方使用该值来标识入站数据包解密到的SA。使用SD-WAN，此入站SPI可以用**show crypto ipsec sa**标识：

```
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)
```

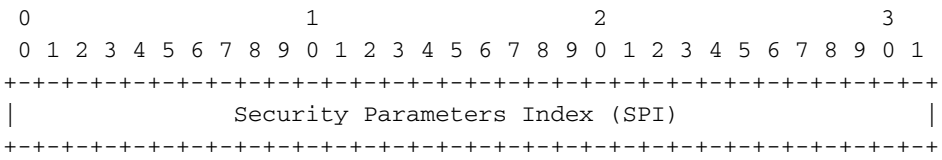
> **注意**：即使所有隧道的入站SPI相同，但接收方具有不同的SA以及与每个对等边缘设备的SA关联的对应重放窗口对象，因为SA由源、目标IP地址、源、目标端口4元组和SPI编号标识。因此，从本质上讲，每个对等体都有自己的反重播窗口对象。

在对等设备发送的实际数据包中，请注意SPI值与之前的输出不同。以下是启用数据包复制选项的packet-trace输出示例：

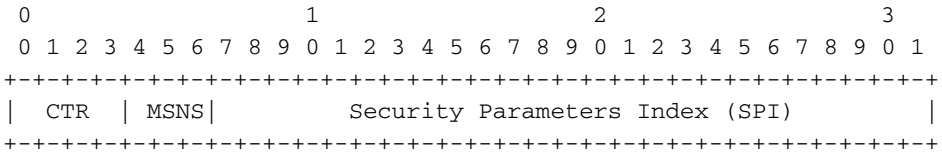
```
Packet Copy In
  45000102 0cc64000 ff111c5e ac127cd0 ac127cd1 3062303a 00eea51b 04000123
  00000138 78014444 f40d7445 3308bf7a e2c2d4a3 73f05304 546871af 8d4e6b9f
```

ESP报头中的实际SPI**为0x04000123。**原因是SD-WAN的SPI中的第一个位被编码为附加信息，并且只有低位的SPI字段被分配给实际SPI。

传统IPsec:



SD-WAN:



其中：

- **CTR**（前4位，0-3位）— 控制位，用于指示特定类型的控制数据包。例如，控制位0x80000000用于BFD。
- **MSN**（接下3位，4-6位）— 多序列号空间索引。这用于在序列计数器数组中定位正确的序列计数器，以检查给定数据包的重放。对于SD-WAN，MSNS的3位允许将8个不同的流量类映射到各自的序列号空间。这意味着可用于SA选择的有效SPI值是从字段的完整32位值中降低的25位。

QoS的多序列号空间

在数据包由于QoS（例如LLQ）而无序传送的环境中，通常观察IPsec重播故障，因为QoS始终在IPsec加密和封装之后运行。多序列号空间解决方案使用映射到给定安全关联的不同QoS流量类别的多个序列号空间来解决此问题。不同的序列号空间按所示的ESP数据包SPI字段中编码的MNS位进行索引。有关更详细的说明，请参阅QoS的IPsec反重播机制。

如前所述，此多序列号实施意味着可用于SA选择的有效SPI值是低位25位。使用此实现配置重播窗口大小时的另一个实际考虑事项是，配置的重播窗口大小用于聚合重播窗口，因此每个序列号空间的有效重播窗口大小是聚合的1/8。

配置示例：

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

> **注**：每个序列号空间的有效重播窗口大小为1024/8 = 128!

> **注**：自Cisco IOS ®XE起。17.2.1，聚合重播窗口大小已增加到8192，因此每个序列号空间的最大重播窗口为8192/8 = 1024个数据包。

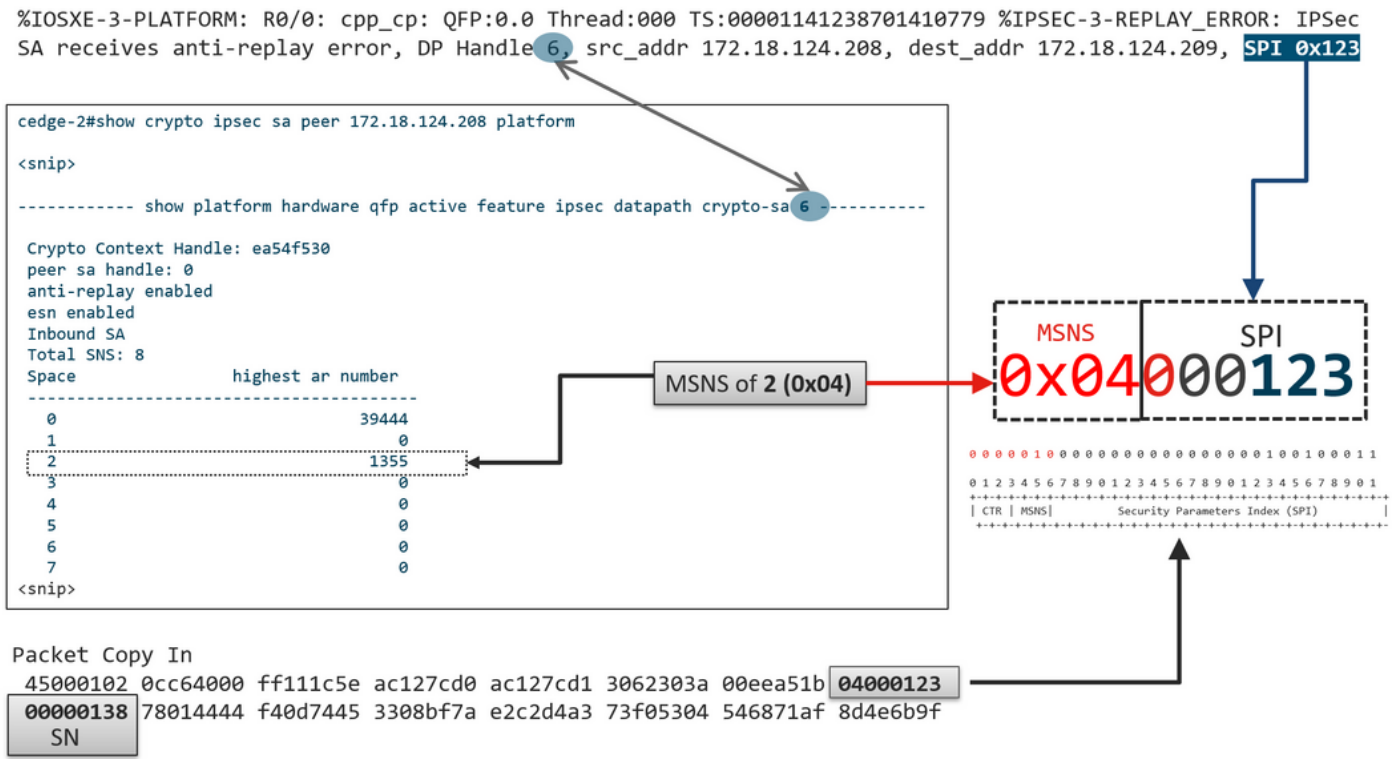
在cEdge设备上，从**show crypto ipsec sa peer x.x.x.x platform** IPsec数据平面输出可获得每个序列号空间收到的最后一个序列号：

```
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>
```

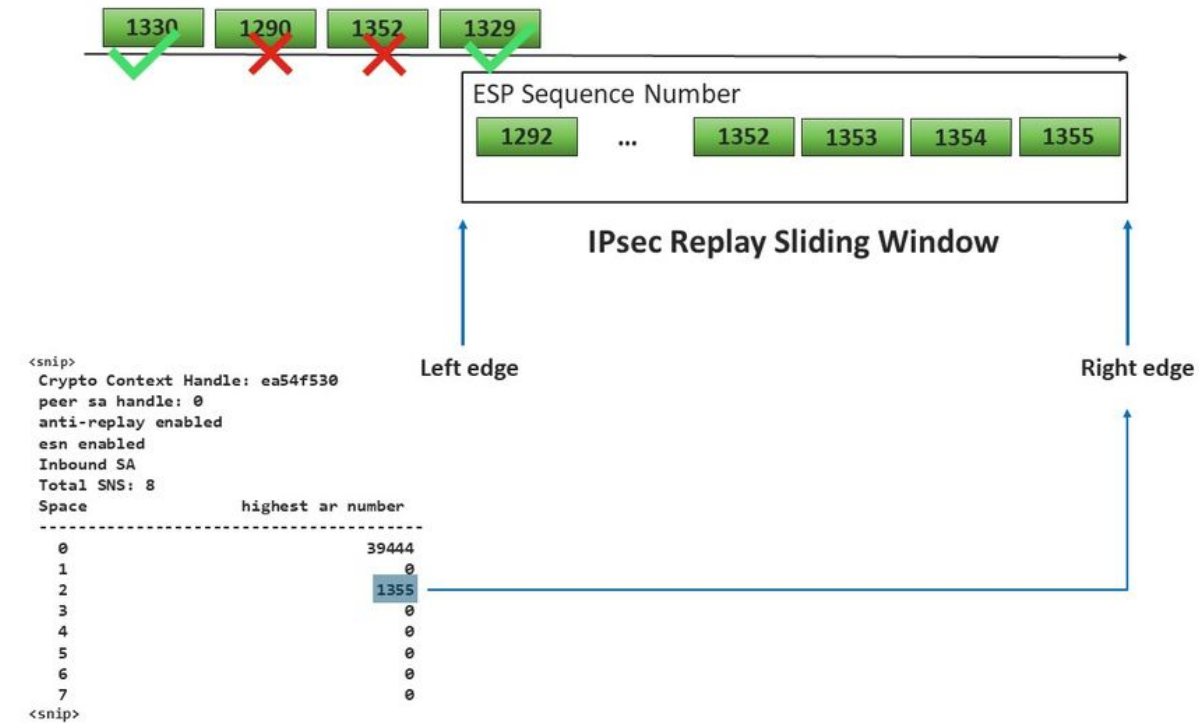
在本例中，0(0x00)的MSNS的最高反重播窗口（反重播滑动窗口的右边缘）是**39444**,**2(0x04)的MSNS的最高反重播窗口（反重播滑动窗口的右边缘）是1335**，这些计数器用于检查序列号是否位于相同序列号空间中的数据包的重播窗口内。

> **注意**：ASR1k平台与其他Cisco IOS ®XE路由平台(ISR4k、ISR1k、CSR1kv)之间存在实施差异。因此，这些平台的show命令及其输出存在一些差异。

可以将Anti-Replay错误与show输出关联以查找SPI和序列号索引，如图所示。



利用以前获得的信息，右边缘（顶部窗口）和滑动窗口的外观如图所示。



使已配置的重放窗口有效的命令

与常规IPsec（非SD-WAN）不同，rekey命令对反重播窗口无效。

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

这些命令会触发已配置的重播窗口生效：

警告：确保您了解任何命令的潜在影响，它们会影响控制连接和数据平面。

```
clear sdwan control connection
```

或

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

或

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

排除重播丢弃故障

数据收集故障排除

对于IPsec反重播丢包，了解问题的条件和潜在触发因素非常重要。至少要收集的信息集以提供情景：

- 重放数据包丢弃的发送方和接收方的设备信息，包括设备类型、cEdge与vEdge、软件版本和配置。
- 问题历史记录。部署已部署多久？ 问题从何时开始的？最近对网络或流量状况所做的任何更改。
- 例如，重播丢包的任何模式，是偶发模式还是恒定模式？问题和/或重大事件的时间，例如，它只发生在流量高峰生产时间或仅在重新生成密钥期间，依此类推？

在收集了之前的信息后，继续执行故障排除工作流程。

工作流故障排除

IPsec重播问题的常规故障排除方法类似于传统IPsec的故障排除方法，如所述，该方法考虑了每个对等体SA序列空间和多个序列号空间。然后执行以下步骤：

步骤1:首先确定系统日志中重放丢弃的对等设备和丢弃率。对于丢包统计信息，请始终收集输出的多个时间戳快照，以便确定丢包率：

```
*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：由于网络中的数据包传输重新排序，偶尔出现重放丢包的情况并不少见，但持续重放丢包会影响服务，因此可以调查这些丢包。

第 2a 步： 对于相对较低的流量速率，使用条件设置为具有**copy packet**选项的对等ipv4地址的数据包跟踪并检查与当前重放窗口右边缘和相邻数据包中的序列号相比丢弃的数据包的序列号，以确认它们是否确实是重复或位于重放窗口之外。

步骤2b. 对于没有可预测的触发器的高流量速率，请配置具有循环缓冲区和EEM的EPC捕获，以便在检测到重放错误时停止捕获。由于从19.3开始，vManage当前不支持EEM，这意味着在执行此故障排除任务时，cEdge必须处于CLI模式。

第三步：理想情况下，在收集数据包捕获或数据包跟踪的同时，在接收器上收集**show crypto ipsec sa peer x.x.x.x**平台。此命令包括入站和出站SA的实时数据平面重放窗口信息。

第四步：如果丢弃的数据包确实顺序混乱，则同时从发送方和接收方进行捕获，确定问题出在源还是底层网络传输层。

第五步：如果数据包被丢弃，即使它们既不重复也不在重放窗口之外，则通常表示接收方存在软件问题。

ASR1001-x故障排除示例

问题说明:

硬件：ASR1001-X
软件：17.06.03a

收到会话对等体10.62.33.91的多个反重播错误，因此BFD会话不断摆动，并且这两个站点之间的流量会受到影响。

```
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
```

步骤1:选中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"
```

注：在本示例中，每个序列号空间的有效重播窗口大小必须为8192/8= 1024。

第 2 步 验证对等10.62.33.91的有效重播窗口大小，以比较并确认配置的值。

```
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
```

此 **窗口大小：64** 输出中显示的内容与配置的重播窗口不匹配 **8192(8192//8=1024)**，这意味着即使已配置该命令，该命令也不会生效。

注：有效重放窗口仅在ASR平台上显示。为确保反重放窗口的实际大小与配置的大小相同，请应用section命令中的某个命令以有效配置重放窗口。

第三步：为来自会话源10.62.33.91、目标10.62.63.251的入站流量同时配置和启用数据包跟踪和监控捕获（可选）

```
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
```

第四步： 收集数据包跟踪摘要：

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

第五步： 展开捕获的一些已丢弃(IpsecInput)数据包。

(IpsecInput)数据包丢弃：

```
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封装的ESP:

- UDP报头是304f303b 00770000,
- 下一个是SPI(0400106)
- 因此00b6e00d是安全编号(SN)。
- 由于32位SPI(0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 1),MSNS指数为2(x 0 400106)。

第六步：检验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
```

MSNS的最大反重播窗口（反重播滑动窗口的右边缘）为2(0x04)0b65f00。

步骤 7. 展开一些转发的(FWD)捕获的数据包。

转发数据包：

```
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
```

数据包：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
```

步骤 8 收集并获取丢弃之前、之后和丢弃之后转发的多数据包(FWD)的序列号信息。

```
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
```

步骤 9 将SN转换为十进制并将它们重新排序为简单计算：

```
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
```

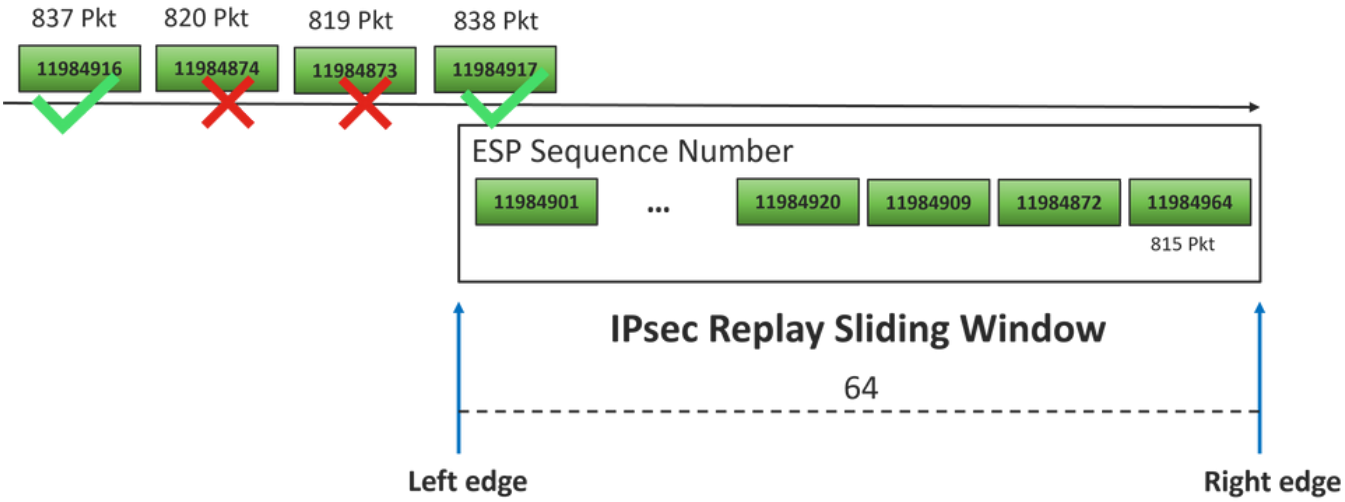
> **注意**:如果序列号大于窗口中的最高序列号，则检查数据包的完整性。如果数据包通过完整性验证检查，则滑动窗口将移至右侧。

步骤 10 将SN转换为十进制并将它们重新排序为简单计算：

```
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
```

对于此示例，可以用**窗口大小64**和右边缘**11984964**可视化滑动窗口，如图所示。



收到的丢弃数据包的序列号远远超出该序列空间的重放窗口的右边缘。

解决方案

由于窗口大小仍旧在前一个值64中（如步骤2所示），所以为了使用1024窗口大小生效，需要应用“使已配置的重放窗口生效”一节中的命令之一。

其他Wireshark捕获工具

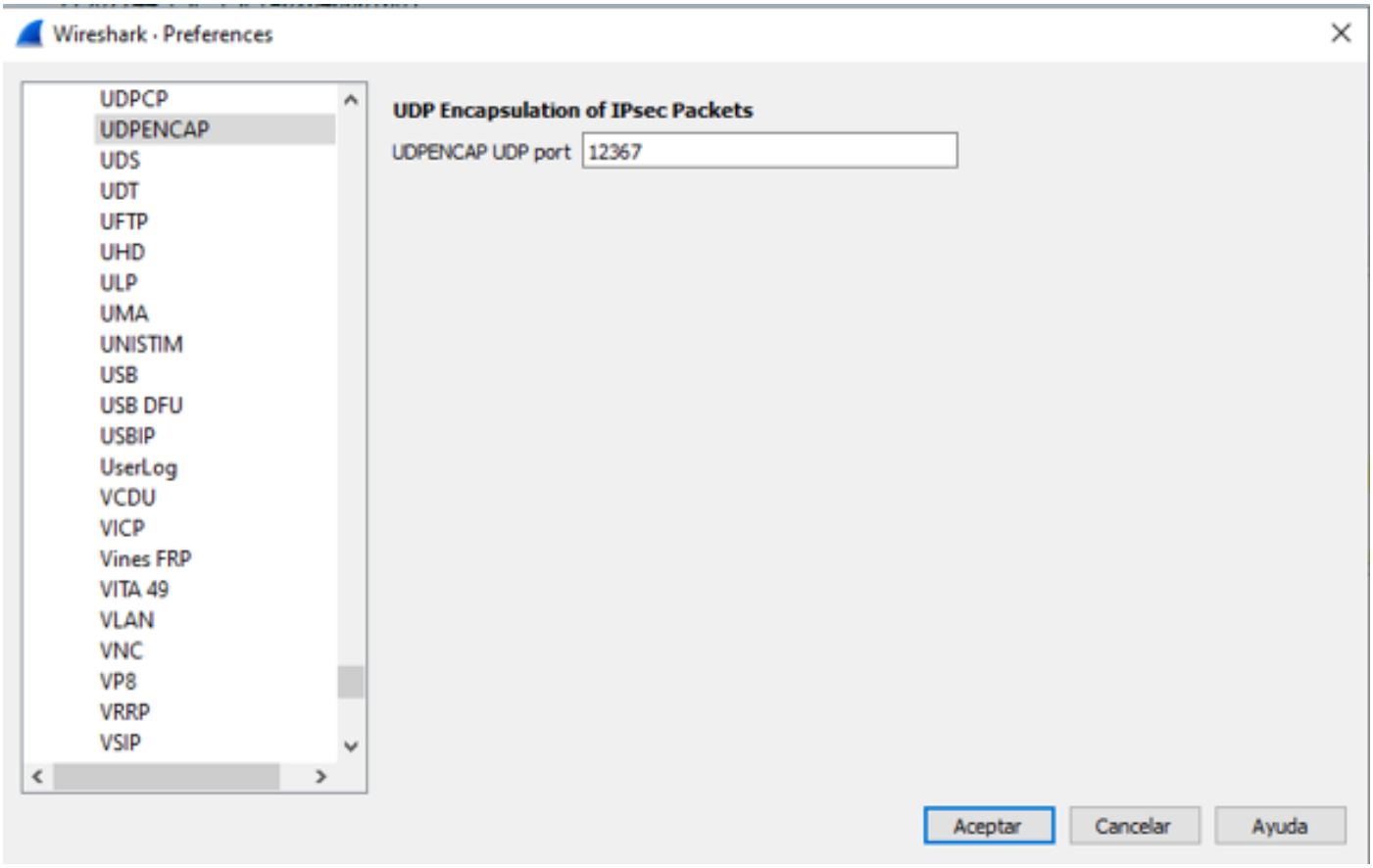
Wireshark软件是帮助关联ESP SPI和序列号的另一个有用工具。

注：出现问题时收集数据包捕获非常重要，如果可能的话，则同时按之前所述收集FIA跟踪

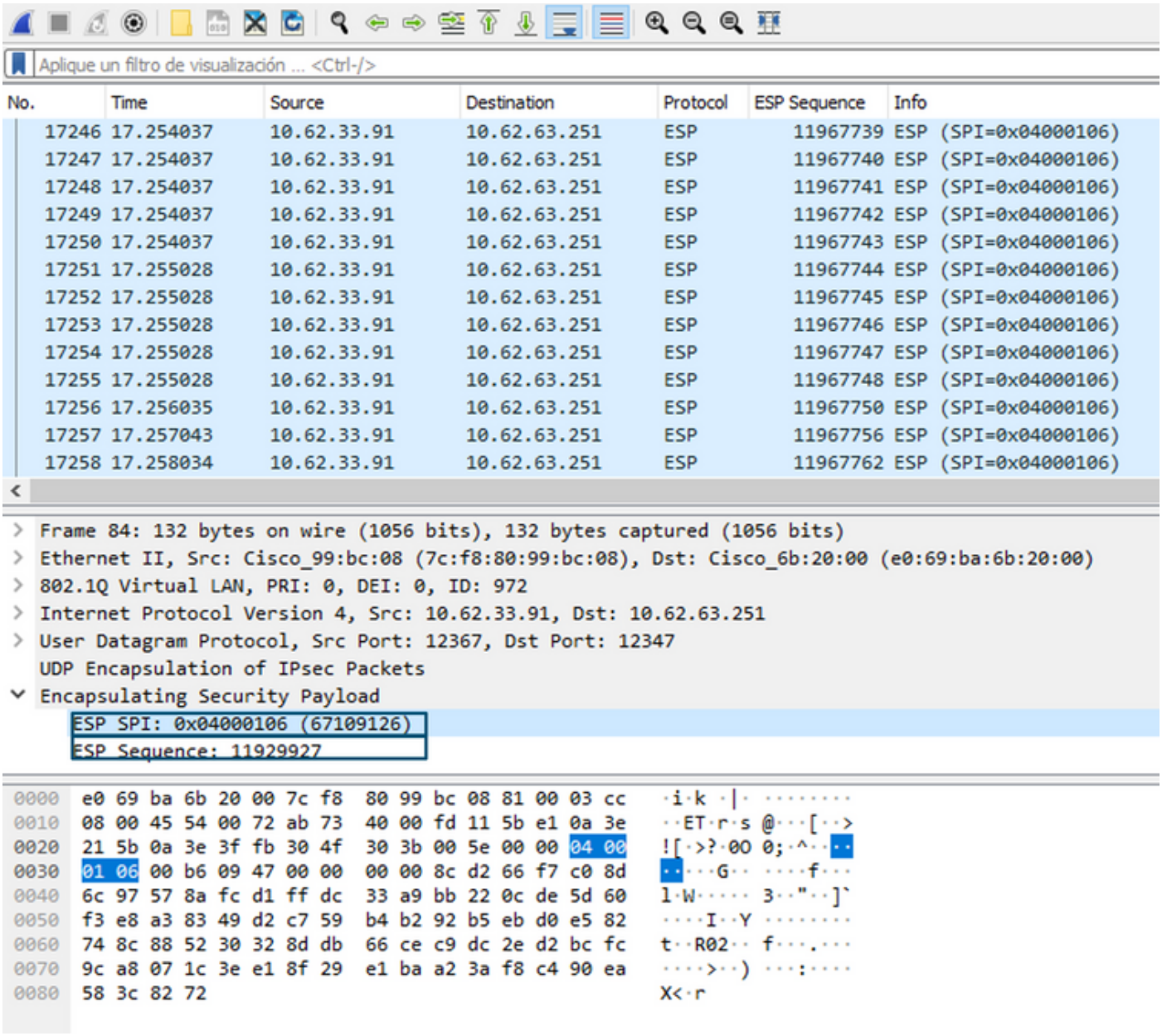
配置入站方向的数据包捕获并将其导出到pcap文件。

```
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中打开pcap结构时，为了能够查看ESP SPI和序列号，请展开一个数据包，右键单击并选择协议首选项，搜索**UDPENCAP**，并将默认端口更改为SD-WAN端口（源端口），如图所示。



UDPENCAP与正确的端口一起使用后，现在显示ESP信息，如图所示。



相关信息

- IPsec Anti-Replay Check Failures TechZone文章
- IPsec反重播窗口扩展和禁用
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。