Troubleshoot SD-WAN cEdge IPsec Anti Replay Failures

Contents

Introduction

This document describes the IPsec Anti-Replay behavior in SD-WAN IPsec for cEdges routers and how to troubleshoot Anti-Replay issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- C8000V Version17.06.01
- ASR1001-X Version 17.06.03a
- vManage Version 20.7.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

IPsec authentication provides built-in anti-replay protection against old or duplicated IPsec packets with the sequence number in the ESP header checked on the receiver. Anti-replay packet drops is one of the most common data-plane issues with IPsec due to packets delivered out of order outside of the anti-replay window. A general troubleshoot approach for IPsec anti-replay drops can be found in IPsec Anti Replay Check Failures, and the general technique applies to SD-WAN as well. However, some implementation differences exist between traditional IPsec and IPsec used in the Cisco SD-WAN solution. This article is intended to explain these differences and the approach on the cEdge platforms with Cisco IOS ®XE.

SD-WAN Replay Detection Considerations

Group Key vs. Pairwise Key

Unlike traditional IPsec, where IPsec SAs are negotiated between two peers with the use of the IKE protocol, SD-WAN uses a group key concept. In this model, an SD-WAN edge device periodically generates data plane inbound SA per TLOC and sends these SAs to the vSmart controller, which in turn propagates the SA to the rest of the edges devices in the SD-WAN network. For a more detailed description of the SD-WAN data plane operations, see SD-WAN Data Plane Security Overview.

> **Note**: Since Cisco IOS ®XE. 6.12.1a/SD-WAN 19.2, IPsec pairwise keys are supported. See IPsec Pairwise Keys Overview. With Pairwise keys, IPsec anti-replay protection works exactly like traditional IPsec. This article primarily focuses on replay check with the use of the group key model.

Encoded SPI

In the IPsec ESP header, the SPI (Security Parameter Index) is a 32-bit value that the receiver uses to identify the SA to which an inbound packet is decrypted with. With SD-WAN, this inbound SPI can be identified with **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)
```

> **Note**: Even though the inbound SPI is the same for all the tunnels, the receiver has a different SA and the correspondent replay-window object associated with the SA for each

peer edge device since the SA is identified by the source, destination IP address, source, destination ports 4-tuple, and the SPI number. So essentially, each peer has its own anti-replay window object.

In the actual packet sent by the peer device, notice the SPI value is different from the previous output. Here is an example from the packet-trace output with the packet copy option enabled:

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

The actual SPI in the ESP header is **0x04000123.** The reason for this is that the first bits in the SPI for SD-WAN are encoded with additional information, and only the low bits of the SPI field are allocated for the actual SPI.

Traditional 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)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

- **CTR** (first 4 bits, bits 0-3) - Control Bits, used to indicate the specific type of control packets. For example control bit 0x80000000 is used for BFD.
- **MSNS** (next 3 bits, bits 4-6) - Multiple Sequence Number Space Index. This is used to locate the correct sequence counter in the sequence counter array to check for replay for the given packet. For SD-WAN, the 3-bit of MSNS allows for 8 different traffic classes to be mapped into their own sequence number space. This implies the effective SPI value that can be used for SA selection is the reduced low order 25 bits from the full 32-bit value of the field.

Multiple Sequence Number Space for QoS

It is common to observe IPsec replay failures in an environment where packets are delivered out of order due to QoS, for example, LLQ, since QoS is always run after IPsec encryption and encapsulation. The Multiple Sequence Number Space solution solves this problem with the use of multiple sequence number spaces mapped to different QoS traffic classes for a given Security Association. The different sequence number space is indexed by the MSNS bits encoded in the ESP packet SPI field as depicted. For a more detailed description, please see IPsec Anti Replay Mechanism for QoS.

As noted previously, this Multiple Sequence Number implementation implies the effective SPI value that can be used for SA selection is the reduced low order 25 bits. Another practical consideration when the replay window size is configured with this implementation is that the configured replay-window size is for the aggregate replay window, so the effective replay window size for each Sequence Number Space is 1/8 of the aggregate.

Configuration example:

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

> **Note**: The effective replay window size for each Sequence Number Space is 1024/8 = 128!

> **Note**: Since the Cisco IOS ®XE. 17.2.1, the aggregate replay window size has been increased to 8192 so that each Sequence Number Space can have a maximum replay window of 8192/8 = 1024 packets.

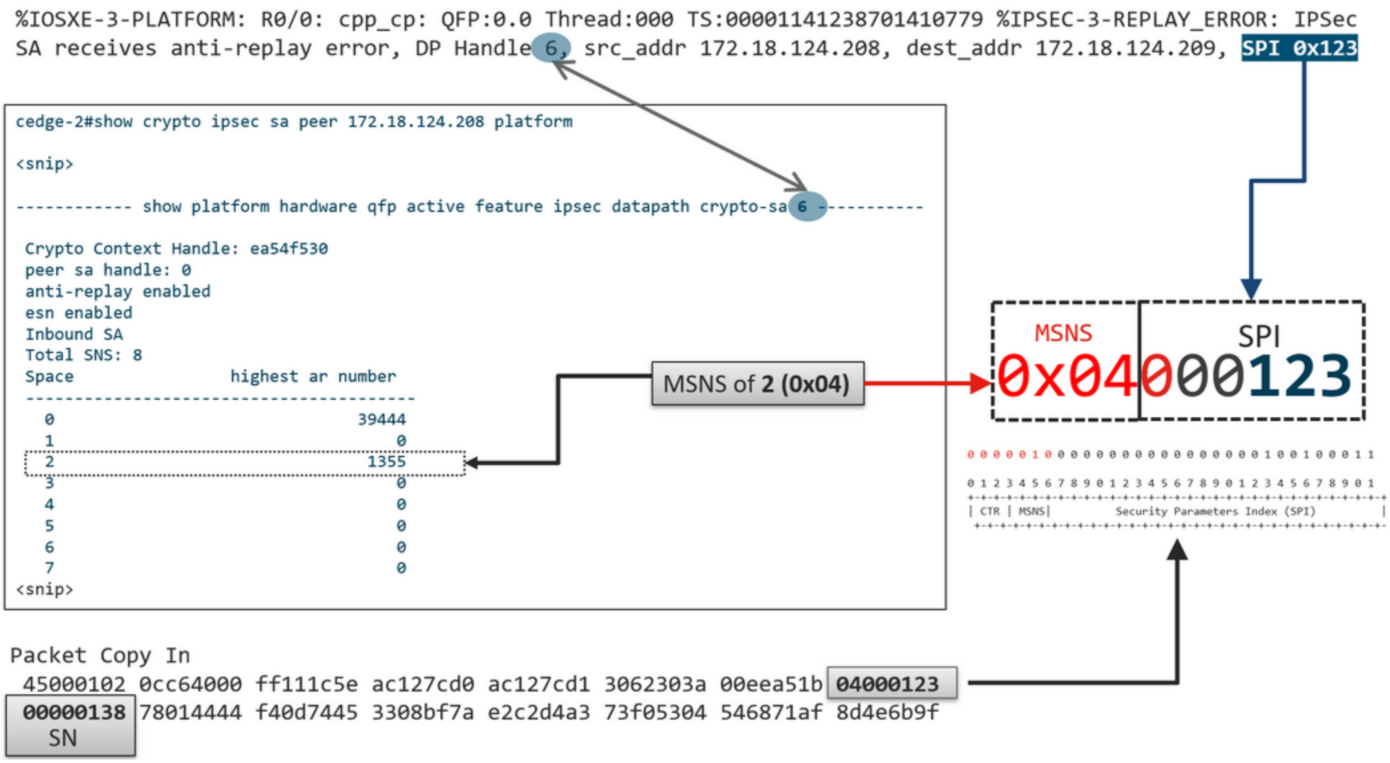
On a cEdge device, the last sequence number received for each sequence number space can be obtained from the **show crypto ipsec sa peer x.x.x.x platform** IPsec dataplane output:

```
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 the example, the highest anti-replay window (Right edge of the anti-replay sliding window) for MSNS of 0 **(0x00)** is **39444**, and that for MSNS of **2 (0x04)** is **1335**, and these counters are used to check if the sequence number is inside of the replay window for packets in the same sequence number space.

> **Note**: There are implementation differences betweem the ASR1k platform and the rest of the Cisco IOS ®XE routing platforms (ISR4k, ISR1k, CSR1kv). As a result, there are some discrepancies in terms of the show commands and their output for these platforms.

It is possible corralate the Anti-Replay erros and the show outputs to find the SPI, and the Sequence number index as shown in the image.

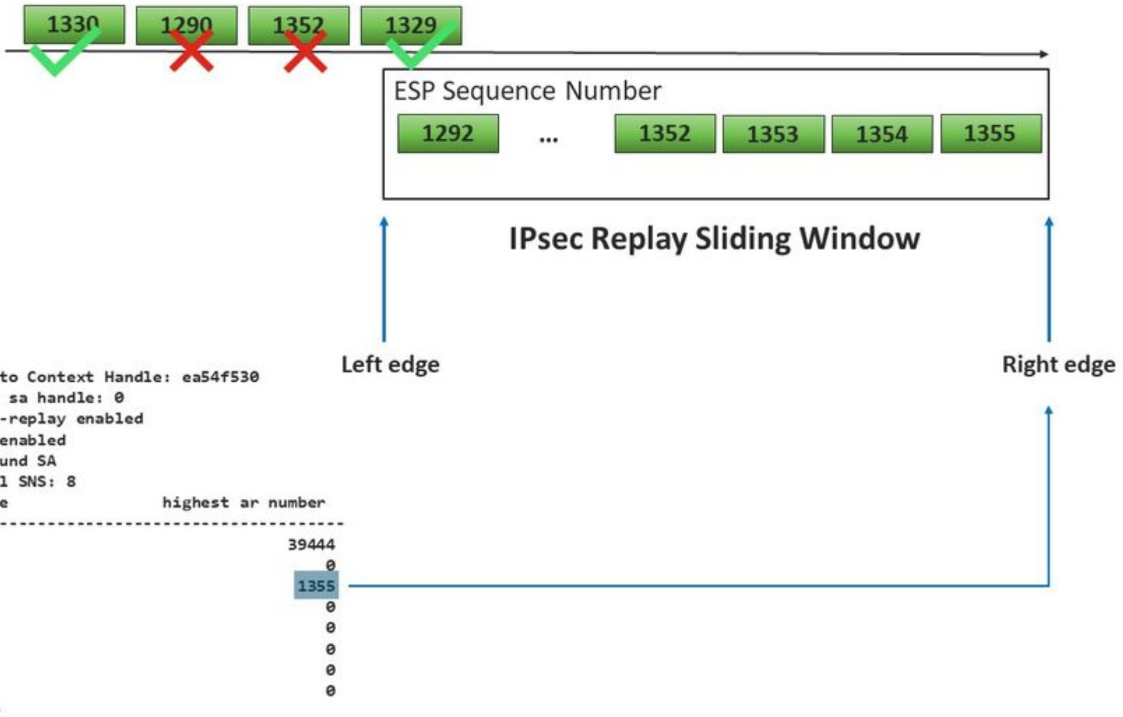


```
%IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00001141238701410779 %IPSEC-3-REPLAY_ERROR: IPSec
SA receives anti-replay error, DP Handle 6, src_addr 172.18.124.208, dest_addr 172.18.124.209, SPI 0x123
```

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

<snip>

----------- show platform hardware qfp active feature ipsec datapath crypto-sa 6 ----------

 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>
```

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

With the previous information obtained the right edge (Top window) and the sliding window looks as shown in the imagen.



```
<snip>
 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>
```

Commands to Take Effectiveness of the Configured Replay Window

Unlike the regular IPsec (non SD-WAN), the rekey command does not takes effect for the anti replay window.

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

These commands triggers the configured replay window to take effect:

> **Warning**: Ensure that you understand the potential impact of any command, they affect the control connections and data plane.

```
clear sdwan control connection
```

or

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

or

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

Troubleshoot Replay Drop Failures

Troubleshoot Data Collection

For the IPsec anti-replay drops, it is important to understand the conditions and potential triggers of the problem. At a minimum, collect the set of information for to provide the context:

- Device information for both the sender and receiver for the replay packet drops, it includes type of device, cEdge vs. vEdge, software version, and configuration.
- Problem history. How long has the deployment been in place? When did the problem start? Any recent changes to the network or traffic conditions.
- Any pattern to the replay drops, for example., is it sporadic or constant? Time of the problem and/or significant event, for example, does it only happen during high traffic peak production hours, or only during rekey, and so on.?

With the previous information collected, proceed with the troubleshoot workflow.

Troubleshoot Workflow

The general troubleshooting approach for IPsec replay issues is just like how it is performed for traditional IPsec, take into account the per-peer SA sequence space and Multiple Sequence Number Space as explained. Then go through these steps:

Step 1. First identify the peer for the replay drop from the syslog and the drop rate. For drop statistics, always collect multiple timestamped snapshots of the output so that the drop rate can be quatified:

```
*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
```

> **Note**: It is not uncommon to see occasional replay drops due to packet delivery reordering in the network, but persistent replay drops impact the service and they can be investigated.

Step 2a. For relatively low traffic rate, take a packet-trace with the condition set to be the peer ipv4 address with the ***copy packet*** option and examine the sequence numbers for the packet dropped against the current replay window right edge and sequence numbers in the adjacent packets to confirm if they are indeed duplicate or outside of the replay window.

Step 2b. For high traffic rate with no predictable trigger, configure an EPC capture with circular buffer and EEM to stop the capture when replay errors are detected. Since EEM is currently not supported on vManage as of 19.3, this implies the cEdge would have to be in CLI mode when this troubleshooting task is performed.

Step 3. Collect the **show crypto ipsec sa peer x.x.x.x platform**on the receiver ideally at the same time the packet capture or packet-trace is collected. This command includes the realtime dataplane replay window information for both the inbound and outbound SA.

Step 4. If the packet dropped is indeed out of order, then take simultaneous captures from both the sender and receiver to identify if the problem is with the source or with the underlay network delivery layer.

Step 5. If the packets are dropped even though they are neither duplicate nor outside of the replay window, then it is usually indicative of a software problem on the receiver.

Troubleshoot Example for ASR1001-x

Problem description:

HW: ASR1001-X
SW: 17.06.03a

Multiple Anti-replay errors receive for the session peer 10.62.33.91, therefore the BFD session constantly flaps and the traffic between these two sites is affected.

```
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
```

Step 1. Check 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"
```

> **Note**: The effective replay window size for each Sequence Number Space must be 8192/8= 1024 in this example.

Step2. Verify the effective replay window size for peer 10.62.33.91 to compare and confirm the configured value.

```
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
```

The **window Size: 64** displayed in the output does not match what the configured replay window **8192 (8192//8=1024)**, wich it means even it was configured the command did not take effect.

> **Note**: The effective replay window is only displayed on the ASR platforms. In order to ensure

the actual size for the anti replay window is the same as the configured size, apply one of the commands in the section commands to take the effectiveness of the configured replay window.

Step 3. Configure and enable packet trace and monitor capture (optional) simultaneously for inbound traffic from session source: 10.62.33.91, destination: 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
```

Step 4. Collect packet trace summary:

```
cEdge#show platform packet summay
<snip>
811 Te0/0/0.972 Te0/0/1.301 FWD
812 Te0/0/0.972 Te0/0/1.301 FWD
813 Te0/0/0.972 Te0/0/1.301 FWD
814 Te0/0/0.972 Te0/0/1.301 FWD
815 Te0/0/0.972 Te0/0/1.301 FWD
816 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
817 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
818 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
819 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
820 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
821 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
822 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
823 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
824 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
825 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
826 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
827 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
828 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
829 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
830 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
831 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
832 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
833 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
834 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
835 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
836 Te0/0/0.972 Te0/0/0.972 DROP 56 (IpsecInput)
837 Te0/0/0.972 Te0/0/1.301 FWD
838 Te0/0/0.972 Te0/0/1.301 FWD
```

Step 5. Expand some dropped (IpsecInput) packets captured.

(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 uses UDP encapsulated ESP:

- The UDP header is 304f303b 00770000,
- The next is SPI (**04000106**)
- Therefore **00b6e00d** is the secuence number (SN).
- The MSNS index is **2** (**x04**00106) due to 32-bit SPI (**0 0 0 0 0 1 0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 1 1.)

Step 6. Verify the 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
```

The highest anti-replay window (Right edge of the anti-replay sliding window) for MSNS of 2 (0x04) is **0b65f00.**

Step 7. Expand some forwarded (FWD) captured packets.

Fowarded packets:

```
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
```

Step 8. Collect and obtain the sequence number information from multipe packets forwarded (FWD) before, after and the drops.

```
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
```

Step 9. Convert to Decimal the SN and re order them to simple calculation:

```
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
```

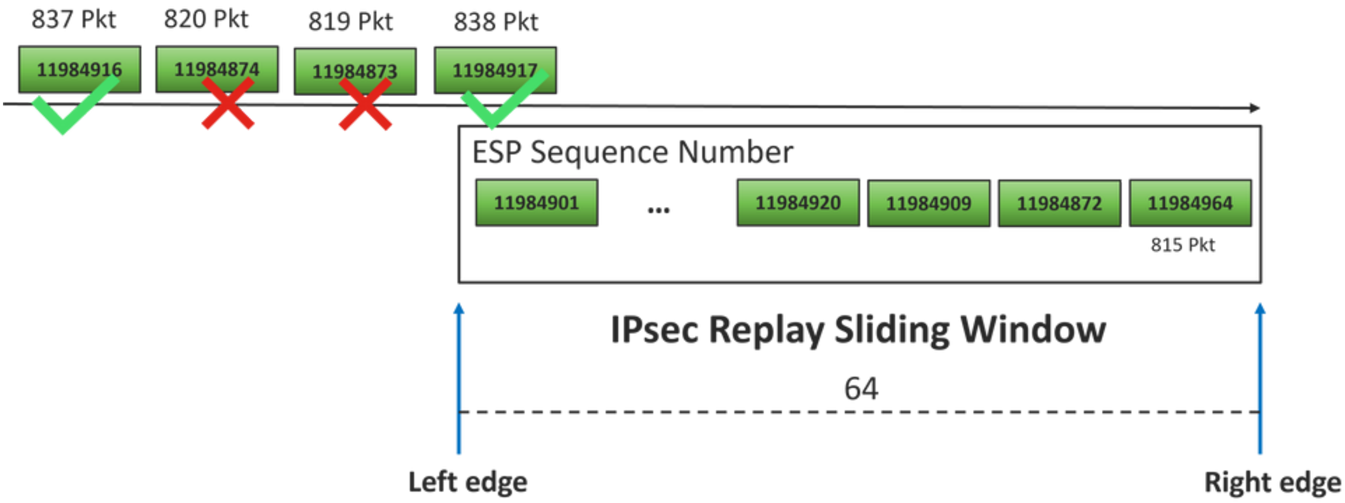
```
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

> **Note**: If the sequence number is greater than the highest sequence number in the window, the packet has its integrity checked. If the packet passes the integrity verification check, the sliding window is then moved to the right.

Step 10. Convert to Decimal the SN and re order them to simple calculation:

```
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
```

For this example, it is possible to visualize the sliding window with the **window size 64** and the **right edge11984964** as shown in the image.



The received sequence number for drop packets is way ahead of the right edge of the replay window for that sequence space.

Solution

Since the window size is still in the previous value 64 as seen in the step 2, one of the commands in the section Commands to Take Effectiveness of the Configured Replay Window need to be applied in order the 1024 window size takes affect.

Additional Wireshark Capture Tool

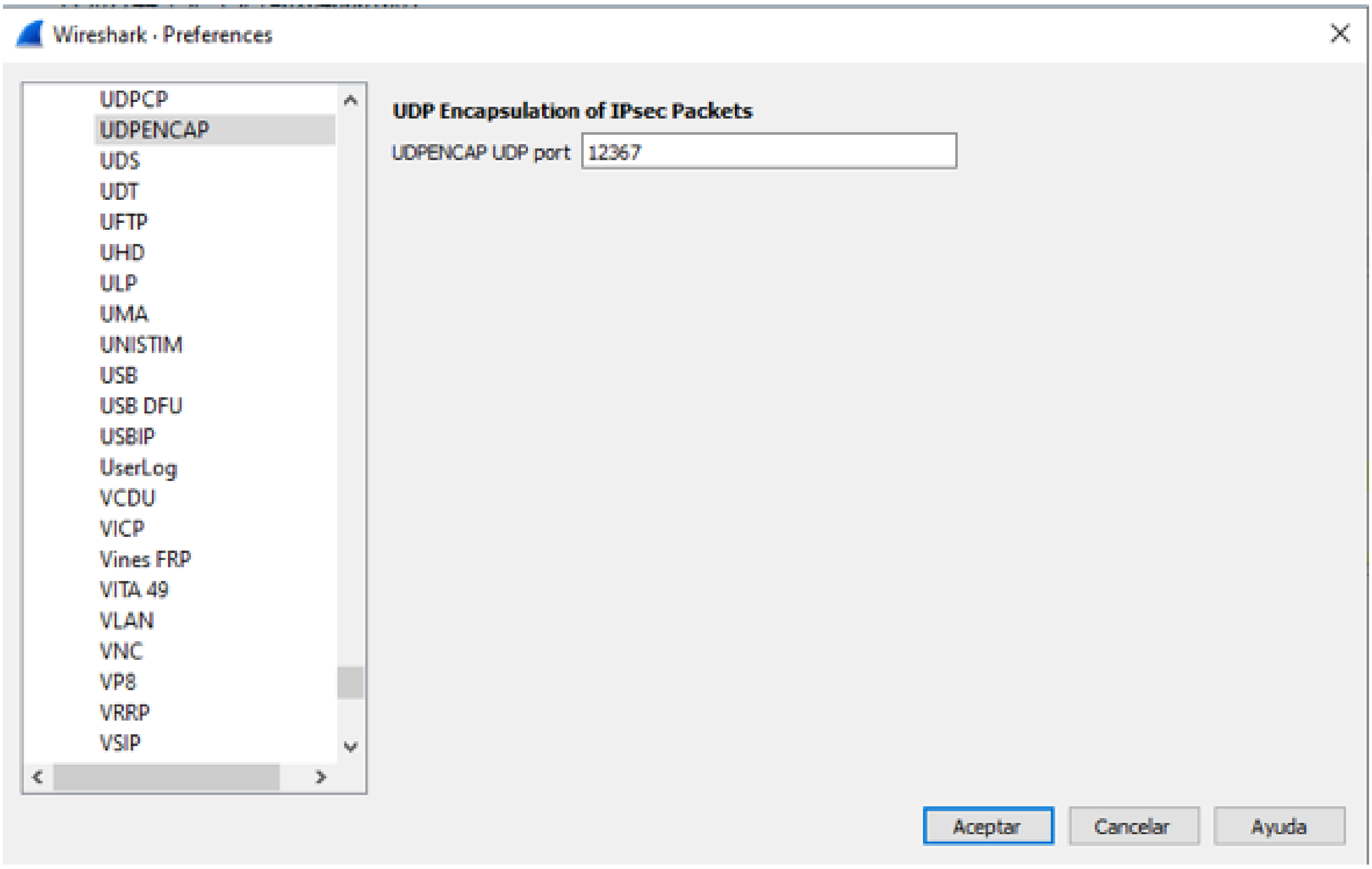
Another useful tool to help to correlate the ESP SPI and Sequence number is the Wireshark software.

> **Note**: It is important to collect the packet capture when the issue occurs and if it is possible at the same time the fia trace is collected as described previously

Configure the packet capture for inbound direction and export it to pcap file.

```
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
```

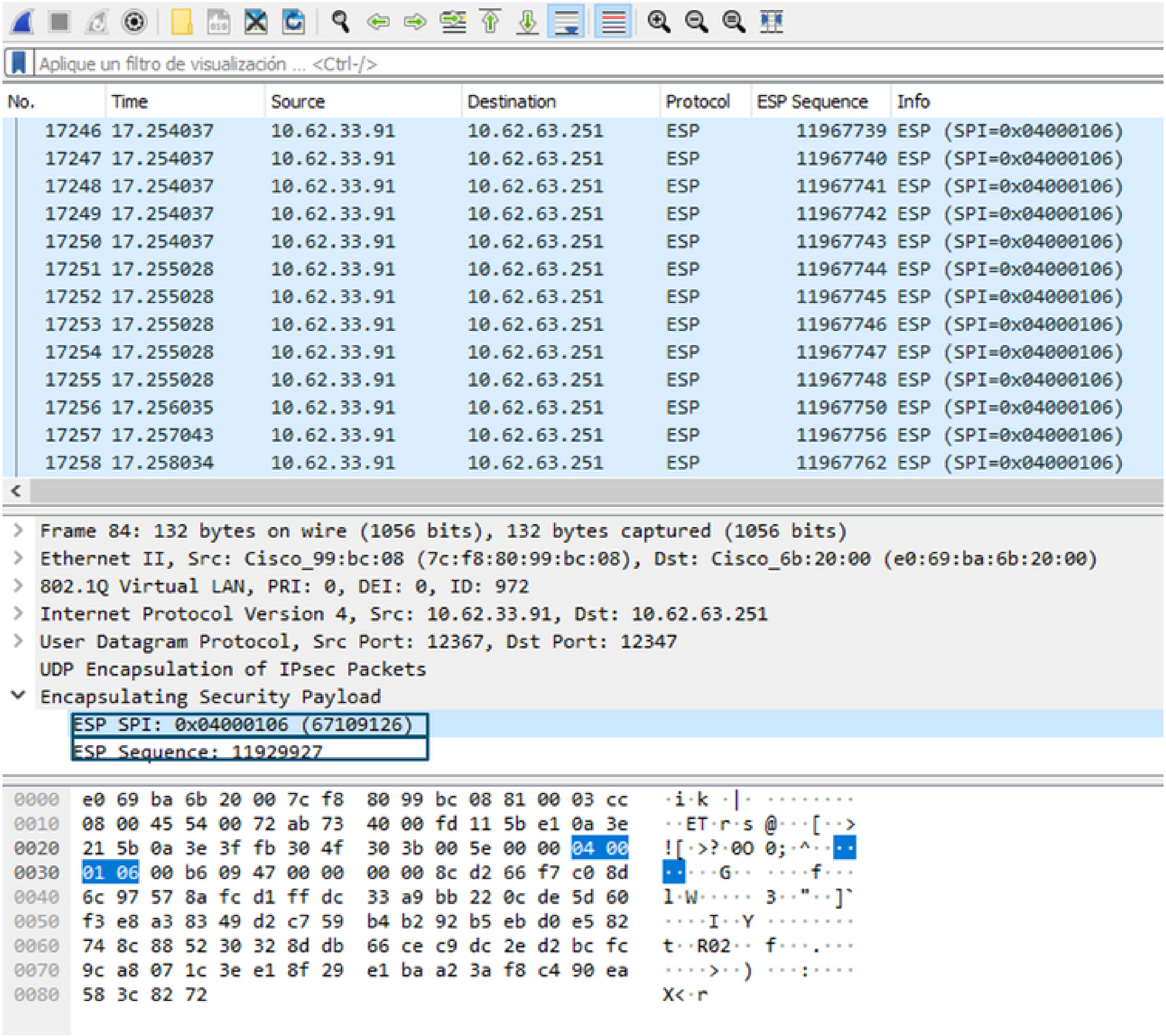
When pcap caoture is opened in Wireshark, in order to be able to see the ESP SPI and sequence number, expand one packet, right click and select **protocol preferences**, search for **UDPENCAP** and change the default port to SD-WAN port (Source port) as shown in the picture.



UDP Encapsulation of IPsec Packets

UDPENCAP UDP port 12367

After UDPENCAP is in place with the right port, the ESP information is now displayed as shown in the image.



```
No.    Time        Source        Destination    Protocol  ESP Sequence  Info
 17246 17.254037   10.62.33.91   10.62.63.251   ESP          11967739 ESP (SPI=0x04000106)
 17247 17.254037   10.62.33.91   10.62.63.251   ESP          11967740 ESP (SPI=0x04000106)
 17248 17.254037   10.62.33.91   10.62.63.251   ESP          11967741 ESP (SPI=0x04000106)
 17249 17.254037   10.62.33.91   10.62.63.251   ESP          11967742 ESP (SPI=0x04000106)
 17250 17.254037   10.62.33.91   10.62.63.251   ESP          11967743 ESP (SPI=0x04000106)
 17251 17.255028   10.62.33.91   10.62.63.251   ESP          11967744 ESP (SPI=0x04000106)
 17252 17.255028   10.62.33.91   10.62.63.251   ESP          11967745 ESP (SPI=0x04000106)
 17253 17.255028   10.62.33.91   10.62.63.251   ESP          11967746 ESP (SPI=0x04000106)
 17254 17.255028   10.62.33.91   10.62.63.251   ESP          11967747 ESP (SPI=0x04000106)
 17255 17.255028   10.62.33.91   10.62.63.251   ESP          11967748 ESP (SPI=0x04000106)
 17256 17.256035   10.62.33.91   10.62.63.251   ESP          11967750 ESP (SPI=0x04000106)
 17257 17.257043   10.62.33.91   10.62.63.251   ESP          11967756 ESP (SPI=0x04000106)
 17258 17.258034   10.62.33.91   10.62.63.251   ESP          11967762 ESP (SPI=0x04000106)
```

```
> Frame 84: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
> Ethernet II, Src: Cisco_99:bc:08 (7c:f8:80:99:bc:08), Dst: Cisco_6b:20:00 (e0:69:ba:6b:20:00)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 972
> Internet Protocol Version 4, Src: 10.62.33.91, Dst: 10.62.63.251
> User Datagram Protocol, Src Port: 12367, Dst Port: 12347
  UDP Encapsulation of IPsec Packets
v Encapsulating Security Payload
      ESP SPI: 0x04000106 (67109126)
      ESP Sequence: 11929927
```

```
0000  e0 69 ba 6b 20 00 7c f8  80 99 bc 08 81 00 03 cc   ·i·k ·|· ········
0010  08 00 45 54 00 72 ab 73  40 00 fd 11 5b e1 0a 3e   ··ET·r·s @···[··>
0020  21 5b 0a 3e 3f fb 30 4f  30 3b 00 5e 00 00 04 00   ![·>?·0O 0;·^····
0030  01 06 00 b6 09 47 00 00  00 00 8c d2 66 f7 c0 8d   ·····G·· ····f···
0040  6c 97 57 8a fc d1 ff dc  33 a9 bb 22 0c de 5d 60   l·W····· 3··"··]`
0050  f3 e8 a3 83 49 d2 c7 59  b4 b2 92 b5 eb d0 e5 82   ····I··Y ········
0060  74 8c 88 52 30 32 8d db  66 ce c9 dc 2e d2 bc fc   t··R02·· f···.···
0070  9c a8 07 1c 3e e1 8f 29  e1 ba a2 3a f8 c4 90 ea   ····>··) ···:····
0080  58 3c 82 72                                        X<·r
```

Related Information

- **IPsec Anti-Replay Check Failures TechZone Article**
- **IPsec Anti-Replay Window Expanding and Disabling**
- **Cisco Technical Support & Downloads**