SD-WAN cEdge IPsecアンチリプレイ障害のトラブルシューティング

内容

概要

このドキュメントでは、cEdgeルータ用のSD-WAN IPsecでのIPsecアンチリプレイの動作と、アンチリプレイの問題のトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- IPSec（Internet Protocol Security）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.06.01
- ASR1001-Xバージョン17.06.03a
- vManageバージョン20.7.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

IPsec認証では、古いIPsecパケットや重複したIPsecパケットに対するアンチリプレイ保護が組み込まれています。この保護では、受信側でESPヘッダーのシーケンス番号がチェックされます。アンチリプレイパケットのドロップは、アンチリプレイウィンドウの外で順序が入れ替わって配信されるパケットが原因で、IPsecのデータプレーンで最も一般的な問題の1つです。IPSecアンチリプレイドロップの一般的なトラブルシューティング方法については、『IPSecアンチリプレイチェックの失敗』を参照してください。この一般的な手法はSD-WANにも適用されます。ただし、Cisco SD-WANソリューションで使用される従来のIPsecとIPsecには、実装の違いがいくつかあります。この記事では、Cisco IOS ®XEを使用するcEdgeプラットフォームにおけるこれらの相違点とアプローチについて説明することを目的としています。

SD-WANリプレイ検出の考慮事項

グループキーとペアワイズキー

IKEプロトコルを使用して2つのピア間でIPsec SAがネゴシエートされる従来のIPsecとは異なり、SD-WANではグループキーの概念が使用されます。このモデルでは、SD-WANエッジデバイスがTLOCごとにデータプレーン着信SAを定期的に生成し、これらのSAをvSmartコントローラに送信します。これにより、SAはSD-WANネットワーク内の残りのエッジデバイスに伝搬されます。SD-WANデータプレーン動作の詳細については、『SD-WANデータプレーンセキュリティの概要』を参照してください。

> **注**:Cisco IOS ®XE以降。 6.12.1a/SD-WAN 19.2、IPsecペアワイズキーがサポートされます。「IPsecペアワイズキーの概要」を参照してください。ペアワイズキーを使用すると、IPsecアンチリプレイ保護は従来のIPsecとまったく同じように機能します。この記事では、主にグループキーモデルを使用したリプレイチェックに焦点を当てています。

エンコードされたSPI

IPsec ESPヘッダーでは、SPI(Security Parameter Index)は32ビットの値で、着信パケットが復号化される先のSAを受信側が識別するために使用されます。SD-WANでは、この着信SPIは**show crypto ipsec sa**で識別できます。

```
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：着信SPIがすべてのトンネルで同じであっても、受信側では異なるSAがあり、各ピアエッジデバイスのSAに関連付けられた対応するリプレイウィンドウオブジェクトがあります。これは、SAが送信元、宛先IPアドレス、送信元、宛先ポート4タプル、およびSPI番号によって識別されるためです。つまり、各ピアには独自のアンチリプレイウィンドウオブジェクトが存在します。

ピアデバイスから送信された実際のパケットでは、SPI値が前の出力と異なることに注意してください。パケットコピーオプションを有効にしたパケットトレースの出力例を次に示します。

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

ESPヘッダーの実際のSPIは**0x04000123です。**この理由は、SD-WAN用のSPIの最初のビットが追加情報を使用して符号化され、SPIフィールドの下位ビットのみが実際のSPIに割り当てられるためです。

従来の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)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

場所：

- **CTR**（最初の4ビット、ビット0 ~ 3）：制御ビット。特定のタイプの制御パケットを示すために使用されます。たとえば、制御ビット0x80000000はBFDに使用されます。
- **MSNS**（次の3ビット、ビット4 ~ 6）：複数シーケンス番号空間インデックス。これは、シーケンスカウンタ配列で正しいシーケンスカウンタを見つけて、特定のパケットのリプレイを確認するために使用されます。SD-WANでは、3ビットのMSNSにより、8つの異なるトラフィッククラスを独自のシーケンス番号空間にマッピングできます。これは、SAの選択に使用できる有効なSPI値が、フィールドの完全な32ビット値から下位25ビットに減らされることを意味します。

QoS用の複数のシーケンス番号スペース

QoSは常にIPsecの暗号化とカプセル化の後に実行されるため、QoSのためにパケットが順不同で配信される環境（LLQなど）では、IPsecのリプレイ障害を観察するのが一般的です。Multiple Sequence Number Spaceソリューションは、特定のセキュリティアソシエーションに対して異なるQoSトラフィッククラスにマッピングされた複数のシーケンス番号空間を使用することで、この問題を解決します。図に示すように、異なるシーケンス番号空間は、ESPパケットSPIフィールドでエンコードされたMSNSビットによってインデックスされます。詳細については、「

QoSのIPsecアンチリプレイメカニズム」を参照してください。

前述したように、このマルチプルシーケンス番号(MST)の実装は、SAの選択に使用できる効果的なSPI値が下位25ビットに減少することを意味します。この実装でリプレイ・ウィンドウ・サイズを構成する場合のもう1つの実用的な考慮事項は、リプレイ・ウィンドウのサイズを集約ウィンドウ用に構成し、各シーケンス番号スペースの有効なリプレイ・ウィンドウ・サイズを集約の1/8に設定することです。

設定例：

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

注：各シーケンス番号スペースの有効なリプレイウィンドウサイズは1024/8 = 128です。

注:Cisco IOS ®XE以降。17.2.1では、各シーケンス番号スペースに最大8192/8 = 1024パケットのリプレイウィンドウを設定できるように、リプレイウィンドウの合計サイズが8192に増加されました。

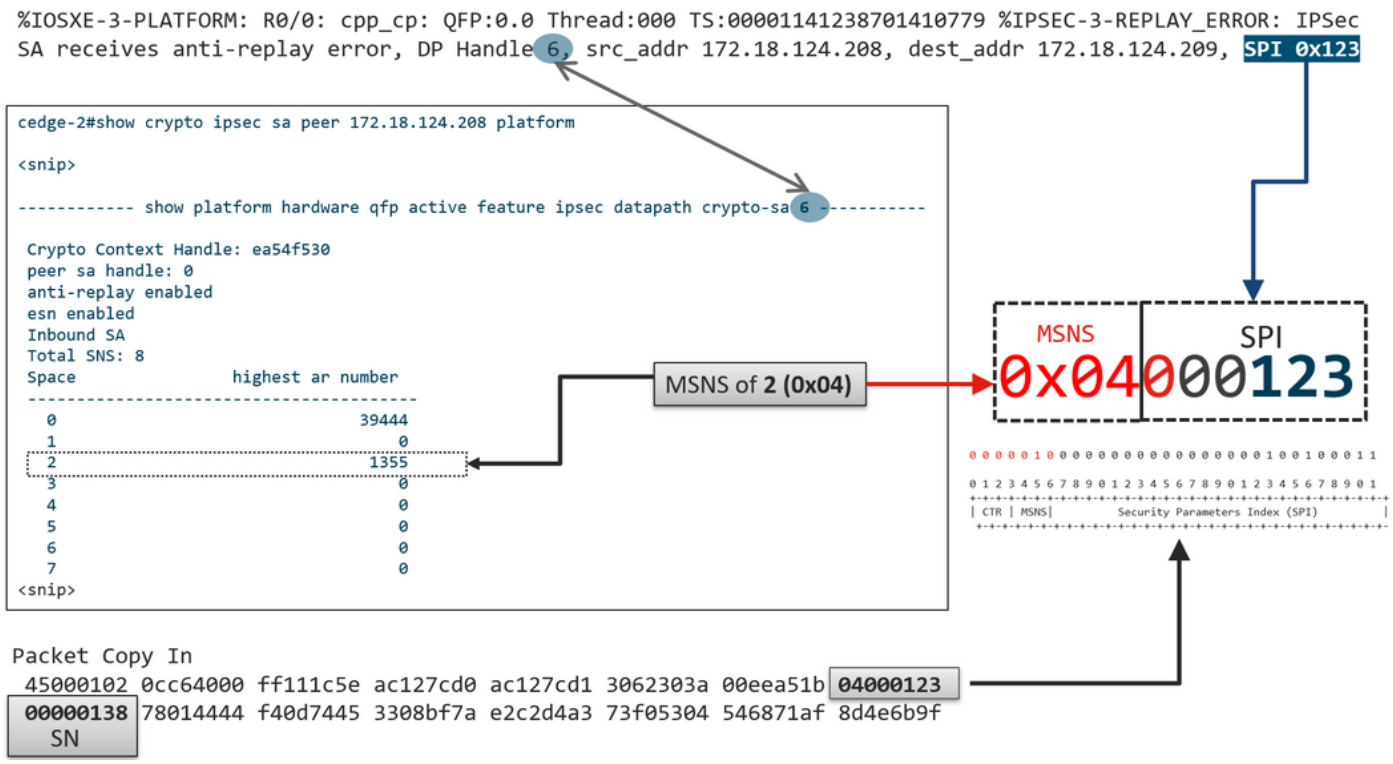
cEdgeデバイスでは、各シーケンス番号空間で受信された最後のシーケンス番号は、**show crypto ipsec sa peer x.x.x.x platform** IPSecデータプレーンの出力から取得できます。

```
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>
```

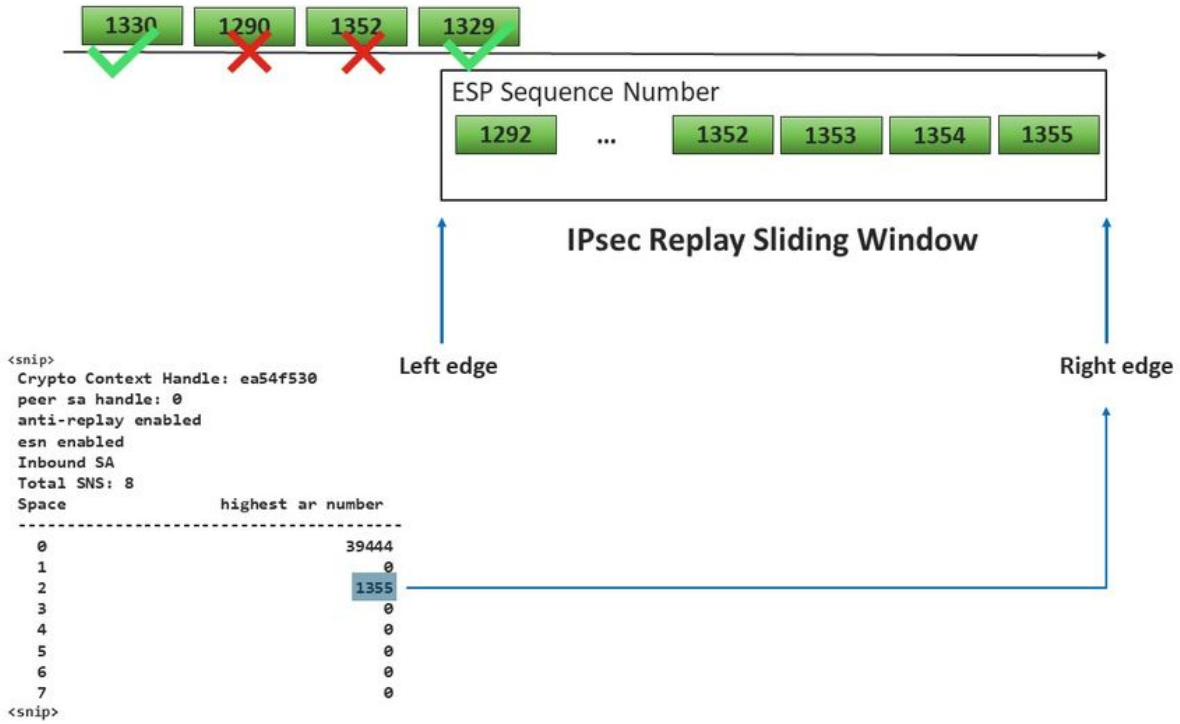
この例では、0 (0x00)のMSNSに対する最も高いアンチリプレイウィンドウ（アンチリプレイスライディングウィンドウの右端）は3944で、2 (0x04)のMSNSに対する最も高いアンチリプレイウィンドウは1335です。これらのカウンタを使用して、同じシーケンス番号空間にあるパケットのリプレイウィンドウ内にシーケンス番号番号番号がかどうかを確認します。

注:ASR1kプラットフォームとその他のCisco IOS ®XEルーティングプラットフォーム(ISR4k、ISR1k、CSR1kv)には実装の違いがあります。その結果、これらのプラットフォームでは、showコマンドとその出力の点でいくつかの不一致があります。

図に示すように、アンチリプレイエラーとshow出力を照合して、SPIとシーケンス番号のインデックスを見つけることができます。



前の情報を取得すると、右端（トップウィンドウ）とスライドウィンドウは、画像に示すように見えます。



設定されたリプレイウィンドウを有効にするためのコマンド

通常のIPsec（非SD-WAN）とは異なり、キー再生成コマンドはアンチリプレイウィンドウには適用されません。

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

次のコマンドは、設定されたリプレイウィンドウをトリガーして有効にします。

> **警告**：コマンドがコントロール接続とデータプレーンに影響を与える可能性のある影響を確実に理解してください。

```
clear sdwan control connection
```

または

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

または

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

リプレイドロップ障害のトラブルシューティング

データ収集のトラブルシューティング

IPSecアンチリプレイドロップの場合は、問題の状態と潜在的なトリガーを理解することが重要です。少なくとも、の一連の情報を収集して、コンテキストを提供します。

- リプレイパケットのドロップに関する送信側と受信側の両方のデバイス情報。これには、デバイスのタイプ、cEdgeとvEdge、ソフトウェアバージョン、および設定が含まれます。
- 問題履歴。導入はいつから行われていますか。 問題はいつ発生しましたか。ネットワークまたはトラフィック条件に対する最近の変更。
- 例えば、リプレイのドロップに対するパターンは散発的ですか、それとも一定ですか。問題や重要なイベントが発生した時間。たとえば、トラフィックのピーク時やキー再生成時などにのみ発生しますか。

前の情報を収集した後、トラブルシューティングワークフローに進みます。

ワークフローのトラブルシューティング

IPSecのリプレイ問題に対する一般的なトラブルシューティングアプローチは、説明したように、ピアごとのSAシーケンス空間と複数のシーケンス番号空間を考慮して、従来のIPSecで実行される方法と似ています。次の手順を実行します。

ステップ 1：最初に、syslogからのリプレイドロップのピアとドロップレートを特定します。ドロップ統計情報の場合は、常に出力の複数のタイムスタンプ付きスナップショットを収集して、ドロップレートを定量化できるようにします。

```
*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：ネットワーク内でのパケット配信の並べ替えによるリプレイドロップが散見されることは珍しくありませんが、リプレイドロップが続くとサービスに影響を与えるため、調査が可能です。

ステップ 2a 比較的低いトラフィックレートの場合は、条件を**copy packet**オプションを使用してピアipv4アドレスに設定したパケットトレースを取得し、現在のリプレイウィンドウの右端に対してドロップされたパケットのシーケンス番号と、隣接するパケットのシーケンス番号を調べて、それらが実際に重複しているか、リプレイウィンドウの外側にあるかを確認します。

ステップ2b: 予測可能なトリガーがない高トラフィックレートの場合は、循環バッファとEEMを使用してEPCキャプチャを設定し、リプレイエラーが検出されたときにキャプチャを停止します。EEMは現在19.3の時点ではvManageでサポートされていないため、このトラブルシューティングタスクを実行する際には、cEdgeをCLIモードにする必要があります。

ステップ 3：パケットキャプチャまたはパケットトレースの収集と同時に、受信側で**show crypto ipsec sa peer x.x.x.x**プラットフォームを収集するのが理想的です。このコマンドには、インバウンドSAとアウトバウンドSAの両方のリアルタイムデータプレーンリプレイウィンドウ情報が含まれます。

ステップ 4：ドロップされたパケットが実際に故障している場合は、送信側と受信側の両方から同時にキャプチャを取得し、問題が送信元にあるのか、アンダーレイのネットワーク配信層にあるのかを特定します。

ステップ 5：パケットが重複しておらず、リプレイウィンドウ外でもなくてもドロップされる場合は、通常は受信側のソフトウェアの問題を示しています。

ASR1001-xのトラブルシューティング例

問題の説明:

HW:ASR1001-X
SW:17.06.03a

セッションピア10.62.33.91に対して複数のアンチリプレイエラーが受信されるため、BFDセッションが常にフラップし、これら2つのサイト間のトラフィックが影響を受けます。

```
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
```

ステップ 1：設定されているアンチリプレイウィンドウが8192であることを確認します。

```
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**：この例では、各シーケンス番号スペースの有効なリプレイウィンドウサイズは8192/8=1024である必要があります。

ステップ 2 ピア10.62.33.91の有効なリプレイウィンドウサイズを確認し、設定値を比較して確認します。

```
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
```

「**ウィンドウサイズ：64** 出力に表示される内容が、設定されているリプレイウィンドウと一致しない **8192(8192//8=1024)**コマンドが有効になっていなかったことを意味します。

注：有効なリプレイウィンドウは、ASRプラットフォームでのみ表示されます。アンチリプレイウィンドウの実際のサイズが設定されたサイズと同じであることを確認するには、「コマンド」セクションのコマンドのいずれかを適用して、設定されたリプレイウィンドウの効果を有効にします。

ステップ 3：セッション送信元：10.62.33.91、宛先：10.62.63.251からのインバウンドトラフィックに対して、パケットトレースを設定し、同時にキャプチャをモニタする（オプション）

```
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
```

ステップ 4： パケットトレースの要約の収集：

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

ステップ 5： キャプチャされたドロップされた(IpsecInput)パケットを展開します。

(IpsecInput)パケットドロップ：

```
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はUDPカプセル化ESPを使用します。

- UDPヘッダーは304f303b 00770000、
- 次はSPI(**04000106**)です
- したがって、**00b6e00d**はセキュリティ番号(SN)です。
- 00106 MSNSインデックスは、32ビット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 1 0 0 1 1)により、**2(x04)**です。

手順 6：MSNSインデックスの確認

```
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のMSNS (0x04)の最も高いアンチリプレイウィンドウ (アンチリプレイスライディングウィンドウの右端) は**0b65f00です。**

手順 7： 転送(FWD)でキャプチャされたパケットを展開します。

転送パケット：

```
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
```

パケット：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
```

ステップ 8： ドロップの前、後、およびドロップ後に転送される複数のパケット(FWD)からシーケンス番号情報を収集して取得します。

```
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
```

ステップ 9： SNを10進数に変換し、単純な計算に並べ替えます。

```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
```

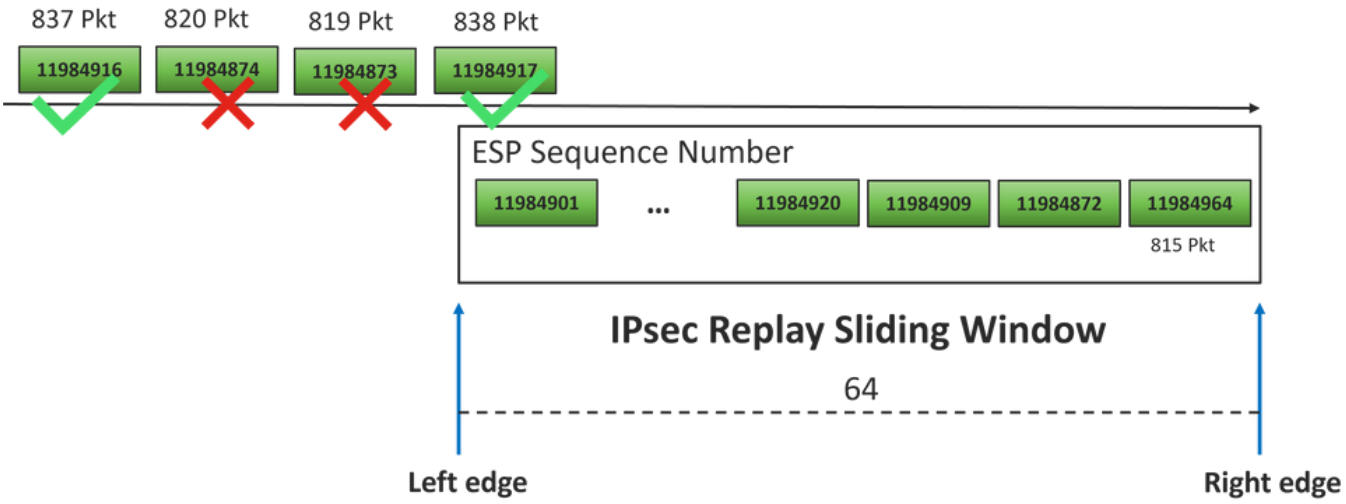
```
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

注：シーケンス番号がウィンドウ内の最も大きいシーケンス番号よりも大きい場合、パケットの整合性がチェックされます。パケットが整合性検証チェックに合格すると、スライディングウィンドウが右に移動します。

ステップ 10： SNを10進数に変換し、単純な計算に並べ替えます。

```
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
```

この例では、図に示すように、**ウィンドウサイズ64**と**右端**11984964でスライドウィンドウを視覚化できます。



ドロップ・パケットに対して受信したシーケンス番号は、そのシーケンス空間のリプレイ・ウィンドウの右端よりずっと先にあります。

解決方法

ウィンドウサイズはステップ2で見たように以前の値64のままであるため、「設定されたリプレイウィンドウの有効性を確保するためのコマンド」セクションにあるコマンドの1つを、1024ウ

ィンドウサイズを有効にするために適用する必要があります。

追加のWiresharkキャプチャツール

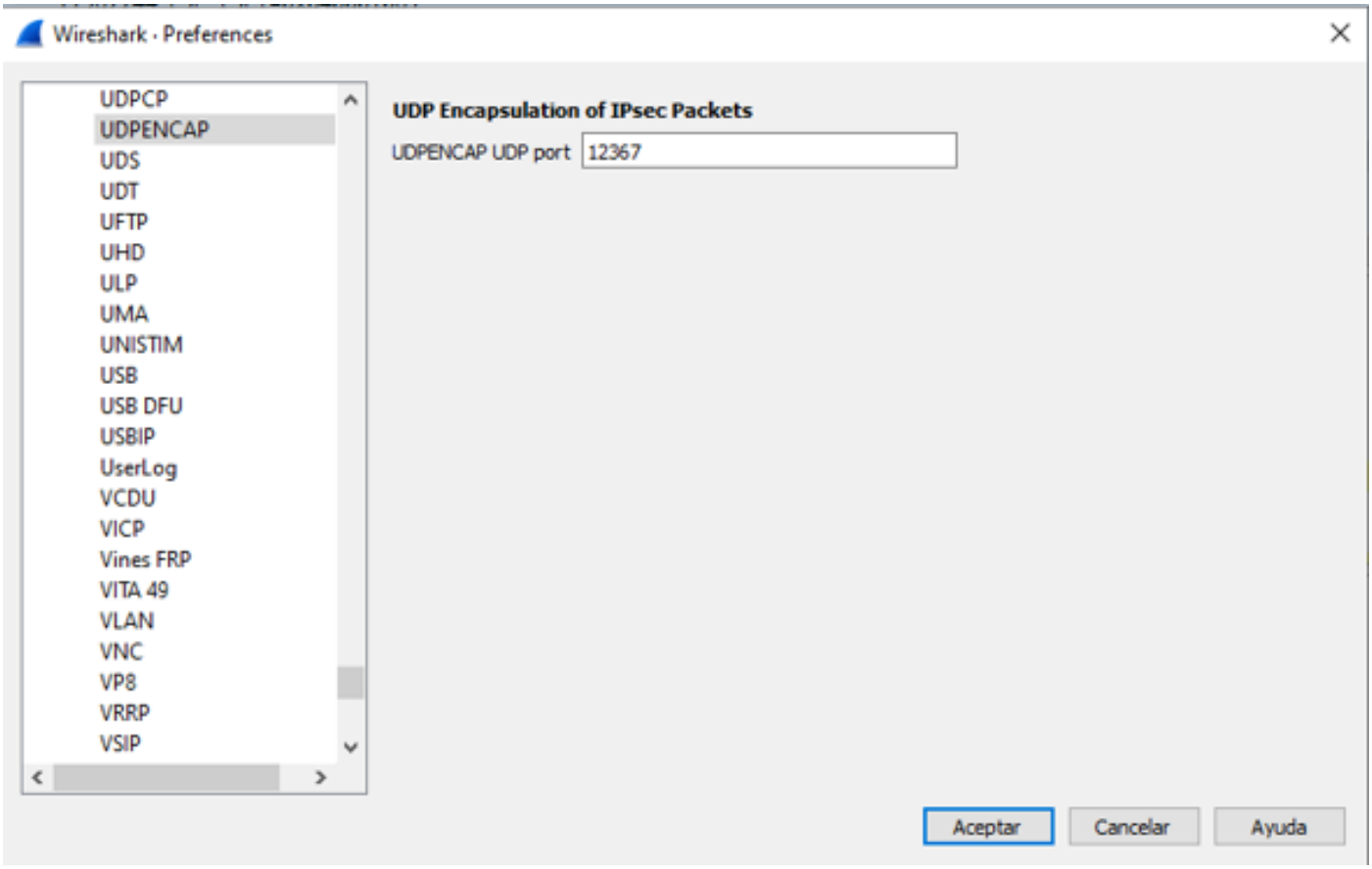
ESP SPIとシーケンス番号の関連付けに役立つもう1つの便利なツールは、Wiresharkソフトウェアです。

> **注**：問題が発生したときにパケットキャプチャを収集することが重要です。可能であれば、前述のようにfiaトレースも収集します

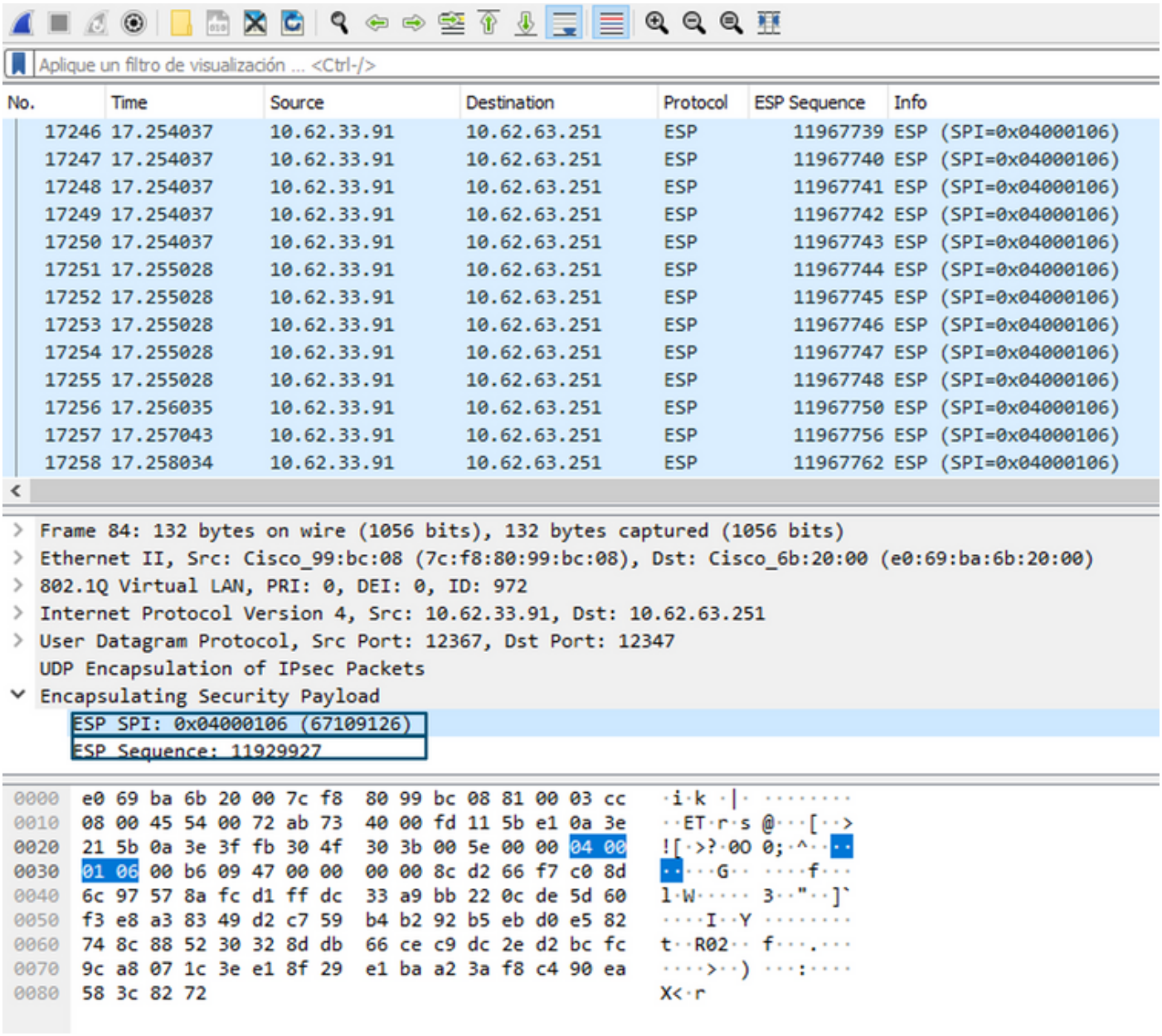
インバウンド方向のパケットキャプチャを設定し、pcapファイルにエクスポートします。

```
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
```

pcap機能がWiresharkで開かれると、ESP SPIとシーケンス番号を表示するために、1つのパケットを展開し、右クリックして**protocol preferences**を選択し、**UDPENCAP**を検索して、デフォルトポートを図に示すようにSD-WANポート（送信元ポート）に変更します。



UDPENCAPが適切なポートに設定されると、図に示すようにESP情報が表示されます。



関連情報

- [IPSecアンチリプレイチェックの失敗に関するTechZone記事]
- [IPsecアンチリプレイウィンドウの展開と無効化]
- [シスコテクニカルサポートおよびダウンロード]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。