أستكشاف أخطاء مكافحة إعادة تشغيل SD-WAN ل cEdge IPsec وإصلاحها

المحتويات

المقدمة

يصف هذا المستند السلوك المضاد لإعادة تشغيل IPsec في SD-WAN IPsec لموجهات cEdges وكيفية أستكشاف أخطاء مكافحة إعادة التشغيل وإصلاحها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة المنطقة الواسعة المعرفة من برنامج Cisco (SD-WAN)
- أمان بروتوكول الإنترنت (IPsec)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- C8000v، الإصدار 17.06.01
- ASR1001-X، الإصدار 17.06.03a
- vManage، الإصدار 20.7.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

توفر مصادقة IPsec حماية مضمنة ضد إعادة التشغيل ضد حزم IPsec القديمة أو المكررة مع رقم التسلسل في رأس ESP الذي تم فحصه على المستقبل. عمليات إسقاط الحزمة المضادة لإعادة التشغيل هي أحد أكثر مشاكل مستوى البيانات شيوعا مع IPsec بسبب الحزم التي يتم تسليمها خارج الترتيب خارج نافذة مكافحة إعادة التشغيل. يمكن العثور على نهج عام لاستكشاف الأخطاء وإصلاحها لعمليات الإسقاط المضادة لإعادة تشغيل IPsec في حالات فشل التحقق من عدم إعادة تشغيل IPsec، ويتم تطبيق التقنية العامة على SD-WAN أيضا. ومع ذلك، توجد بعض إختلافات التنفيذ بين IPsec التقليدي و IPsec المستخدم في حل Cisco SD-WAN. تهدف هذه المقالة إلى شرح هذه الاختلافات والنهج المتبع على الأنظمة الأساسية من Cisco IOS ®XE.

اعتبارات اكتشاف إعادة تشغيل SD-WAN

مفتاح المجموعة مقابل مفتاح Pairwise

على عكس IPsec التقليدي، حيث يتم التفاوض حول رسائل IPsec SAs بين نظامين باستخدام بروتوكول IKE، يستخدم SD-WAN مفهوم مفتاح مجموعة. في هذا النموذج، يقوم جهاز SD-WAN Edge بإنشاء مستوى بيانات SA الوارد بشكل دوري لكل TLOC وإرسال شبكات SA هذه إلى وحدة التحكم vSmart، والتي تقوم بدورها بنشر SA إلى بقية أجهزة الحواف في شبكة SD-WAN. للحصول على وصف أكثر تفصيل لعمليات مستوى بيانات SD-WAN، راجع نظرة عامة على أمان مستوى بيانات SD-WAN.

> **ملاحظة**: منذ Cisco IOS ®XE. 6.12.1a/SD-WAN 19.2، يتم دعم مفاتيح IPsec الجانبية. راجع نظرة عامة على مفاتيح IPsec Pairwise. باستخدام المفاتيح Pairwise، تعمل الحماية ضد إعادة التشغيل ل IPsec تماما مثل IPsec التقليدي. تركز هذه المقالة بشكل أساسي على التحقق من إعادة التشغيل باستخدام نموذج مفتاح المجموعة.

رمز SPI

في رأس IPsec ESP، يكون SPI (فهرس معلمات الأمان) عبارة عن قيمة 32 بت يستخدمها المستقبل لتعريف SA التي يتم فك تشفير الحزمة الواردة بها. باستخدام SD-WAN، يمكن تعريف واجهة برمجة التطبيقات (SPI) الواردة هذه باستخدام **show crypto ipSec**:

```
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)
```

> **ملاحظة**: على الرغم من أن SPI الوارد هو نفسه لجميع الأنفاق، إلا أن المستلم لديه SA

ارظن ريظن ةفاح زاهج لكل SA ب طبترملا لسارملا ليغشتلا ةداعإ ةذفان نئاك وكائن مختلف لأنه يتم تحديد SA بواسطة المصدر وعنوان IP للوجهة والمصدر والوجهة منافذ 4-لتك ورقم SPI. لذلك أساسا، كل نظير له كائن نافذة مكافحة إعادة التشغيل الخاص به.

في الحزمة الفعلية التي تم إرسالها بواسطة جهاز النظير، لاحظ أن قيمة SPI مختلفة عن الإخراج السابق. وفيما يلي مثال على إخراج تتبع الحزمة مع تمكين خيار نسخ الحزمة:

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

قيمة واجهة برمجة التطبيقات (SPI) الفعلية في رأس ESP هي **0x04000123.** السبب وراء ذلك هو أن وحدات البت الأولى في SPI ل SD-WAN يتم ترميزها بمعلومات إضافية، ويتم تخصيص وحدات البت المنخفضة فقط من حقل SPI لواجهة SPI الفعلية.

بروتوكول IPsec التقليدي:

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

شبكة WAN المعرفة عن طريق البرامج:

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

أين:

- **CTR** (أول 4 وحدات بت، وحدات بت 0-3) - وحدات بت التحكم، المستخدمة للإشارة إلى النوع المحدد لحزم التحكم. على سبيل المثال، يتم إستخدام وحدة بت التحكم 0x800000 لبروتوكول BFD.
- **MSNS** (وحدات بت 3 التالية، وحدات بت 4-6) - فهرس مساحة رقم تسلسل متعدد. يتم إستخدام هذا لتحديد موقع عداد التسلسل الصحيح في صفيف عداد التسلسل للتحقق من إعادة التشغيل للحزمة المحددة. بالنسبة ل SD-WAN، تتيح وحدات MSNS ذات الإصدار 3 بت إمكانية تعيين 8 فئات مختلفة من فئات حركة المرور في مساحة أرقام التسلسل الخاصة بها. هذا يعني أن قيمة SPI الفعالة التي يمكن إستخدامها لتحديد SA هي 25 بت منخفضة الترتيب من قيمة 32 بت الكاملة للحقل.

مساحة رقمية تسلسلية متعددة لجودة الخدمة

من الشائع ملاحظة حالات فشل إعادة تشغيل IPsec في بيئة يتم فيها تسليم الحزم بشكل غير راس بسبب جودة الخدمة (QoS)، على سبيل المثال، LLQ، نظرا لأنه يتم تشغيل جودة الخدمة دائما بعد تشفير IPsec وتضمينه. يحل حل "مساحة الرقم التسلسلي المتعدد" هذه المشكلة باستخدام مساحات أرقام تسلسلية متعددة تم تعيينها إلى فئات حركة مرور جودة الخدمة المختلفة لاقتران أمان معين. تتم فهرسة مساحة رقم التسلسل المختلفة بواسطة وحدات بت MSNS المرمزة في حقل SPI لحزمة ESP كما هو موضح. للحصول على وصف أكثر تفصيلا، الرجاء مراجعة آلية مكافحة إعادة تشغيل IPsec لجودة الخدمة.

وكما تمت الإشارة مسبقا، فإن تنفيذ رقم التسلسل المتعدد هذا يعني ضمنا قيمة SPI الفعالة التي يمكن إستخدامها لتحديد SA هي 25 بت منخفضة الترتيب. هناك إعتبار عملي للتشغيل إعادة نافذة حجم أن وهو قيبطتلا اذهب ليغشتلا ةداعإ ةذفان مجح نيوكت دنع رخآ التشغيل إعادة نافذة حجم نوكي ثيحب ،التجميع لتشغيل إعادة نافذة هو هنيوكت مت يذلا الفعال لكل مساحة رقم تسلسل هو 1/8 من التجميع.

مثال التكوين:

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

> **ملاحظة**: حجم نافذة إعادة التشغيل الفعال لكل مساحة رقم تسلسل هو 1024/8 = 128!

> **ملاحظة**: منذ Cisco IOS ®XE. 17.2.1، تمت زيادة حجم نافذة إعادة التشغيل الإجمالي إلى 8192 حتى يمكن أن تحتوي كل مساحة رقم تسلسل على نافذة إعادة تشغيل قصوى من 8192/8 = 1024 حزمة.

على جهاز cEdge، يمكن الحصول على آخر رقم تسلسل تم تلقيه لكل مساحة رقم تسلسل من خرج مستوى بيانات **show crypto ipSec** نظير **x.x.x.x للنظام الأساسي** IPsec:

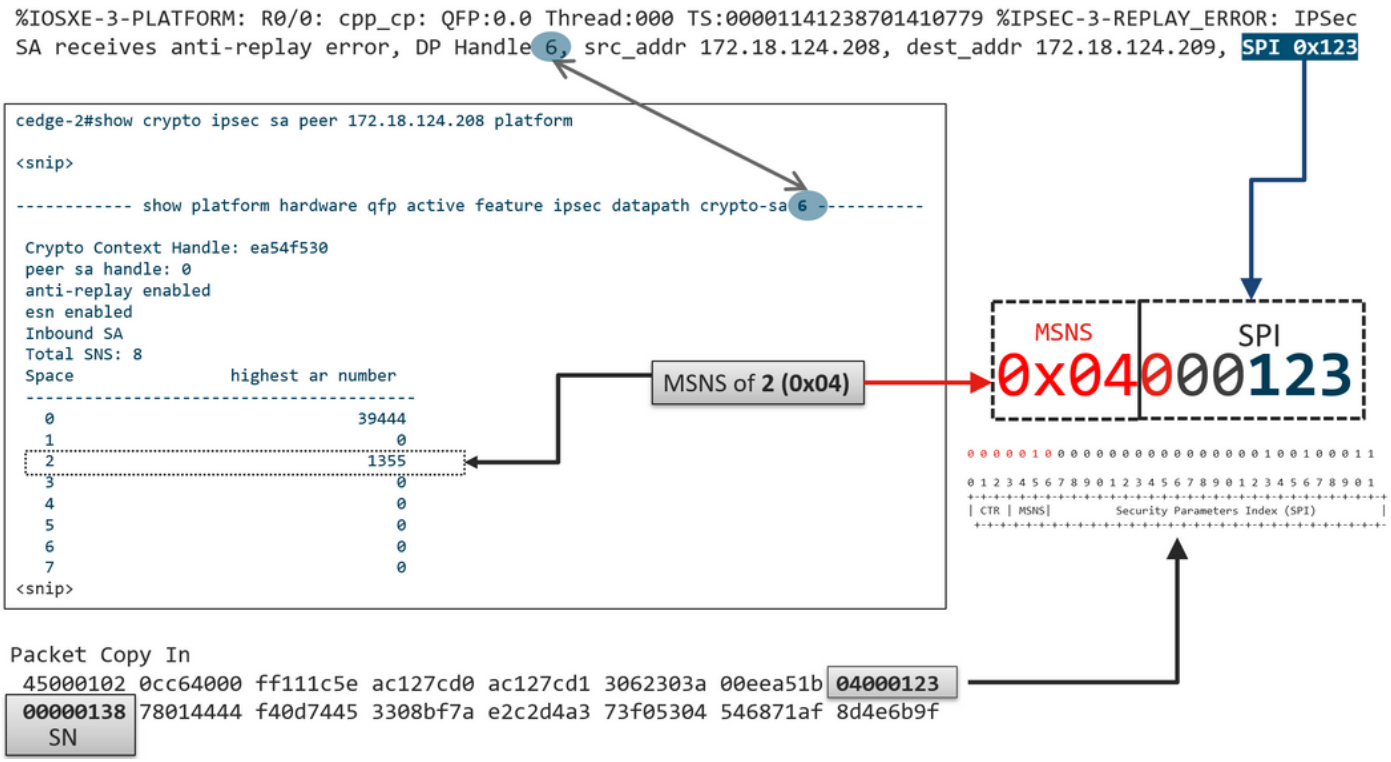
```
cedge-2#show crypto ipsec sa peer 172.18.124.208 platform

<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>
```

في المثال، فإن أعلى نافذة مواقع إعادة التشغيل (الحافة اليمنى من نافذة الانزلاق مكافحة إعادة التشغيل) ل MSN **(0x00)** هي **3944**، وكذلك ل MSNS ل **2 (0x04)** هو **1335**، وتستخدم في مزحل للتشغيل إعادة نافذة لخاد لسلستلا مقر ناك اذإ ام نم ققحتلل تادادعلا هذه التسلسل رقم مساحة سفن.

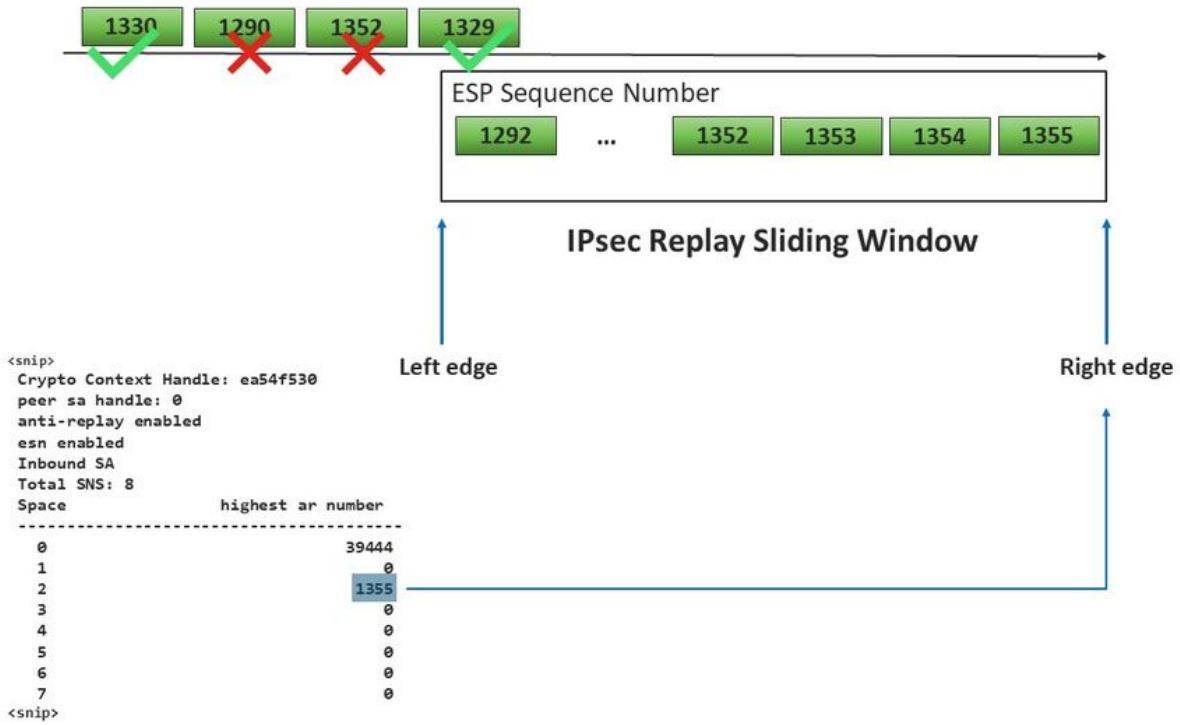
> **ملاحظة**: هناك إختلافات في التنفيذ بين منصة ASR1k وبقية منصات توجيه Cisco IOS ®XE (ISR4k، ISR1k، CSR1kv). ونتيجة لذلك، هناك بعض الاختلافات من حيث أوامر

show ومخرجاتها لهذه الأنظمة الأساسية.

من الممكن إجراء مقارنة بين عمليات مقاومة إعادة التشغيل ومخرجات العرض للعثور على SPI، وفهرس رقم التسلسل كما هو موضح في الصورة.



باستخدام المعلومات السابقة تم الحصول على الحافة اليمنى (الإطار العلوي) ويبدو الإطار المنزلق كما هو موضح في الصور.



أوامر للحصول على فعالية إطار إعادة التشغيل الذي تم

تكوينه

بخلاف IPsec العادي (بخلاف SD-WAN)، لا يرسي الأمر rekey على انفاذة منع إعادة التشغيل.

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

تقوم هذه الأوامر بتشغيل نافذة إعادة التشغيل التي تم تكوينها لتفعيل:

> **تحذير**: تأكد من فهمك للتأثير المحتمل لأي أمر، أنه يؤثر على اتصالات التحكم ومستوى البيانات.

```
clear sdwan control connection
```

أو

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

أو

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

أستكشاف أخطاء إعادة التشغيل وإصلاحها وإصلاحها

أستكشاف أخطاء تجميع البيانات وإصلاحها

بالنسبة لعمليات إسقاط مواقع إعادة تشغيل IPsec، من المهم فهم ظروف المشكلة والعوامل المحتملة التي أدت إلى حدوث المشكلة. قم على الأقل بتحديد مجموعة المعلومات لتوفير السياق:

- معلومات الجهاز لكل من المرسل والمستلم لعمليات إسقاط حزمة إعادة التشغيل، وتتضمن نوع الجهاز و cEdge مقابل vEdge وإصدار البرنامج والتكوين.
- محفوظات المشكلة. كم من الوقت كان الإنتشار هناك؟ متى بدأت المشكلة؟ أي تغييرات حديثة في الشبكة أو شروط حركة المرور.
- على سبيل المثال، أي نمط للرسائل المسقطة، هل هو متقطع أم ثابت؟ وقت المشكلة و/ أو الحدث المهم، مثل، هل يحدث فقط خلال ساعات الإنتاج العالية لذروة حركة المرور، أو فقط خلال وقت حدوث المشكلة، وهكذا.؟

مع جمع المعلومات السابقة، تابع سير عمل أستكشاف الأخطاء وإصلاحها.

أستكشاف أخطاء سير العمل وإصلاحها

نهج أستكشاف الأخطاء وإصلاحها العام لمشكلات إعادة تشغيل IPsec يشبه تماما طريقة تنفيذه ل IPsec التقليدي، وتأخذ في الاعتبار مسار تسلسل SA لكل نظير ومسار تسلسل متعدد كما هو موضح. ثم انتقل عبر هذه الخطوات:

الخطوة 1. أولا تعين النظير ل replay drop من ال syslog والمعدل الإسقاط. إلإحصائيات الإسقاط، قم دائما بجمع لقطات متعددة مختومة بالوقت للمخرجات بحيث يمكن تحديد معدل الإسقاط:

```
*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
```

ملاحظة: ليس من غير الشائع رؤية حالات سقوط إعادة التشغيل العرضية بسبب إعادة ترتيب الحزم في الشبكة، ولكن عمليات إسقاط إعادة التشغيل المستمرة قد تؤثر على الخدمة ويمكن التحقق فيها.

الخطوة 2أ. بالنسبة لمعدل حركة المرور المنخفض نسبيا، قم بأخذ تتبع الحزمة مع الشرط **ونسخ الحزمة** مع خيار النظير IPv4 عناوين لكي يكون المعين للحزمة وأصح أرقام التسلسل الحالية وأرقام التسلسل في الحافة إعادة التشغيل المرفوضة التي تسقط إعادة تشغيل التشغيل. ما إذا كانت بالفعل مكررة أو خارج نافذة إعادة التشغيل لتأكيد ما إذا كانت الحزم المجاورة.

الخطوة الثانية ب. بالنسبة لمعدل حركة المرور المرتفع مع عدم وجود مشغل يمكن التنبؤ به، قم بتكوين التقاط EPC باستخدام المخزن المؤقت الدائري و IM لإيقاف الالتقاط عند اكتشاف أخطاء إعادة التشغيل. نظرا لأن EEM غير مدعوم حاليا على vManage اعتبارا من 19.3، فإن هذا يعني أنه يجب أن يكون cEdge في وضع واجهة سطر الأوامر (CLI) عند تنفيذ مهمة استكشاف الأخطاء وإصلاحها هذه.

الخطوة 3. تجمع **العرض crypto ipSec ننظير x.x.x** بالجهاز المستقبل بشكل مثالي في الأمر هذا متضمنة. الحزمة أو تتبع الحزمة التقاط تجميع فيه يتم الذي الوقت نفس من لكل sa الوارد والصادر. معلومات نافذة إعادة تشغيل مستوى البيانات الوقت الفعلي.

الخطوة 4. إذا كانت الحزمة التي تم إسقاطها خارج الترتيب بالفعل، فعليك التقاط صور مع المصدر أو مع المشكلة كانت إذا ما لتحديد سواء على حد المستلم والمرسل من متزامنة ضبط تسليم الشبكة الأساسية.

الخطوة 5. إذا تم إسقاط الحزم على الرغم من أنها ليست مكررة أو خارج نافذة إعادة التشغيل، فإنها تشير عادة إلى مشكلة في البرنامج على المستقبل.

استكشاف أخطاء ASR1001-X وإصلاحها

وصف المشكلة:

hw: ASR1001-X
البرامج: 17.06.03a

تتلقى العديد من الأخطاء المضادة لإعادة التشغيل لنظير جلسة العمل 10.62.33.91، وبالتالي فإن جلسة عمل BFD تستمر في التدفق وتتأثر حركة مرور البيانات بين هذين الموقعين.

```
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
```

الخطوة 1. تحقق من تكوين إطار مكافحة إعادة التشغيل 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"
```

ملاحظة: يجب أن يكون حجم نافذة إعادة التشغيل الفعال لكل مسار رقم تسلسل 8192/8= 1024 في هذا المثال.

الخطوة 2. تحقق من حجم نافذة إعادة التشغيل الفعال للنظير 10.62.33.91 لمقارنة القيم التي تم تكوينها وتأكيدها.

```
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
```

يعرض الأمر **حجم النافذة: 64** معروض في المخرجات التي تم تكوينها في نافذة إعادة التشغيل 8192 (8192//8=1024)، يعني حتى الأمر لم تسري.

ملاحظة: تظهر نافذة إعادة التشغيل الفعالة فقط على الأنظمة الأساسية ASR. in order to ضمنت الحجم حقيقي للنافذة مكافحة إعادة التشغيل ال نفسه مثل ال يشكل لإعادة تشغيل كل يشكل من ةيلعافلا يأخذ أن أمر مسقل في الأمر نم داحو تقبط، مجح نافذة.

الخطوة 3. تكوين تتبع الحزمة والتقاط الشاشة وتمكينها (اختياري) بشكل متزامن لحركة المرور الواردة من مصدر الجلسة: 10.62.33.91، الوجهة: 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
```

الخطوة 4. تجميع ملخص تتبع الحزم:

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

الخطوة 5. قم بتوسيع بعض الحزم التي تم إسقاطها (IPSecInput) التي تم التقاطها.

(عمليات إسقاط حزم IPSecInput):

```
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
```

يستخدم SD-WAN بروتوكول UDP المضمن ESP:

- رأس UDP هو 304f303b 0077000،
- التالي هو SPI (**04000106**)
- لذلك **00b6e00d** هو رقم الأمان (SN).
- يكون مؤشر MSNS هو **2** (**x04**00106) تتيجة اولاجهة برمجة التطبيقات (SPI) إصدار 32 بت (**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 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 1 1).

الخطوة 6. التحقق من فهرس MSNS

```
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
```

أعلى نافذة مقاومة لإعادة التشغيل (الحافة اليمنى للنافذة المنزلقة لمقاومة إعادة التشغيل) لـ MSNS رقم 2 (0x04) هي **0b65f00.**

الخطوة 7. مددت بعض يحول (FWD) على قبض ربط.

الحزم الإضافية:

```
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
```

الحزمة: 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
```

الخطوة 8. تجميع معلومات رقم التسلسل والحصول عليها من الحزم المتعددة المعاد توجيهها (FWD) قبل وبعد عمليات الإسقاط.

```
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
```

الخطوة 9. تحويل إلى رقم عشري لـ SN وإعادة ترتيبهم إلى حساب بسيط:

```
REORDERED:
813 PKT: 00b6e00d FWD --- Decimal: 11984909
814 PKT: 00b6dfe8 FWD --- Decimal: 11984872
```

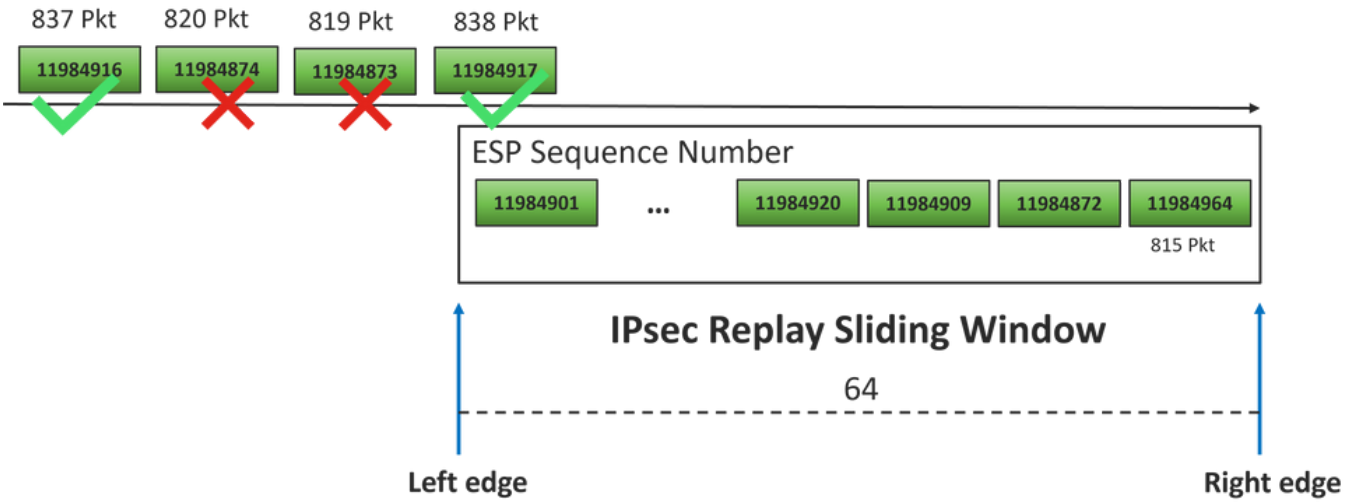
```
815 PKT: 00b6e044 FWD --- Decimal: 11984964 ***** Highest Value
816 PKT: 00b6dfed DROP--- Decimal: 11984877
817 PKT: 00b6dfec DROP--- Decimal: 11984876
818 PKT: 00b6dfeb DROP--- Decimal: 11984875
819 PKT: 00b6dfe9 DROP--- Decimal: 11984873
820 PKT: 00b6dfea DROP--- Decimal: 11984874
<snip>
837 PKT: 00b6e014 FWD --- Decimal: 11984916
838 PKT: 00b6e015 FWD --- Decimal: 11984917
839 PKT: 00b6e016 FWD --- Decimal: 11984918
```

ملاحظة: إذا كان الرقم التسلسلي أكبر من أعلى رقم تسلسلي في النافذة، فإن الحزمة يتم التحقق من تكاملها. إذا تجاوزت الحزمة التحقق من السلامة، فإن الإطار المنزلق يتم نقله إلى اليمين.

الخطوة 10. تحويل إلى رقم عشري ل SN وإعادة ترتيبهم إلى حساب بسيط:

```
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
```

لهذا المثال، من الممكن عرض النافذة المنزلقة **بحجم النافذة 64** والحافة **اليمنى11984964** كما هو موضح في الصورة.



الرقم التسلسلي المستلم للحزم المسقطة يسبق كثيرا الحافة اليمنى لنافذة إعادة التشغيل لمساحة التسلسل تلك.

الحل

بما أن حجم النافذة ال يزال في القيمة السابقة 64 كما يرى في الخطوة 2، فإن أحد الأوامر في

القسم أن أي أخذ فعالية ال يشكل إعادة تشغيل نافذة يحتاج أن يكون طبقت in order ال 1024 نافذة حجم أي أخذ تأثير.

أداة التقاط Wireshark الإضافية

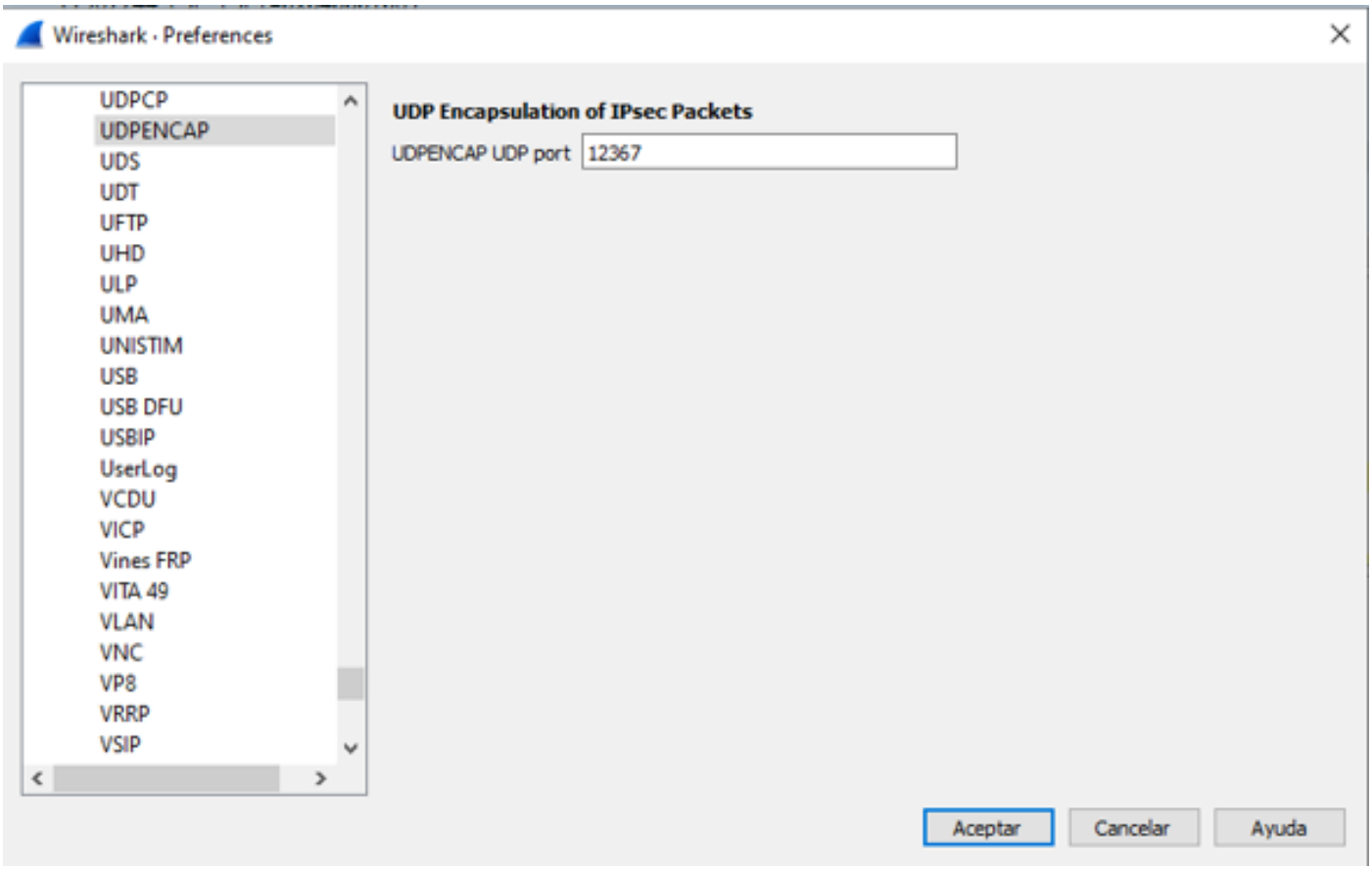
هناك أداة أخرى مفيدة للمساعدة في ربط ESP SPI والرقم التسلسلي وهو برنامج Wireshark.

> **ملاحظة**: من المهم تجميع التقاط الحزمة عند حدوث المشكلة وإذا كان من الممكن في نفس الوقت تجميع تتبع FIA كما هو موضح مسبقا

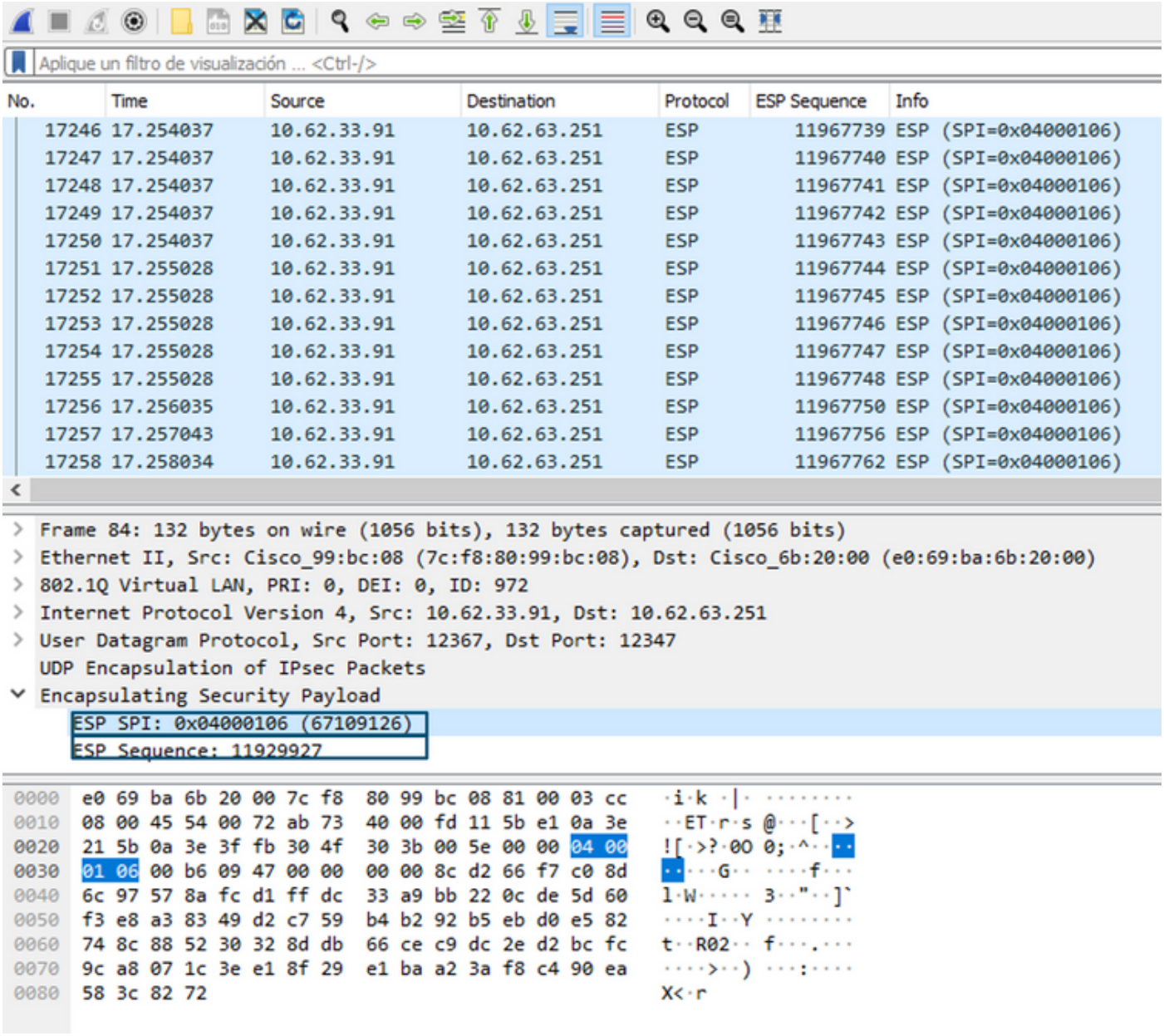
قم بتكوين التقاط الحزمة للاتجاه الوارد وتصديره إلى ملف PCAP.

```
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
```

عند فتح معرف فئة PCAP في Wireshark، لتتمكن من رؤية ESP SPI والرقم التسلسلي، قم بتوسيع حزمة واحدة، وانقر بزر الماوس الأيمن وحدد **تفضيلات البروتوكول**، ثم ابحث عن **UDPENCAP** وقم بتغيير المنفذ الافتراضي إلى منفذ SD-WAN (منفذ المصدر) كما هو موضح في الصورة.



بعد أن يكون UDPnap في مكانه مع المنفذ الأيمن، يتم عرض معلومات ESP الآن كما هو موضح في الصورة.



معلومات ذات صلة

- مقالة TechZone للتحقق من عدم إعادة تشغيل IPsec
- توسيع وتعطيل النافذة المضادة لإعادة التشغيل لـ IPsec
- الدعم التقني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).