أستكشاف أخطاء التحقق من عدم إعادة تشغيل IPsec وإصلاحها

المحتويات

المقدمة

يصف هذا المستند مشكلة تتعلق بفشل التحقق من عدم إعادة تشغيل أمان بروتوكول الإنترنت (IPsec) ويوفر الحلول الممكنة.

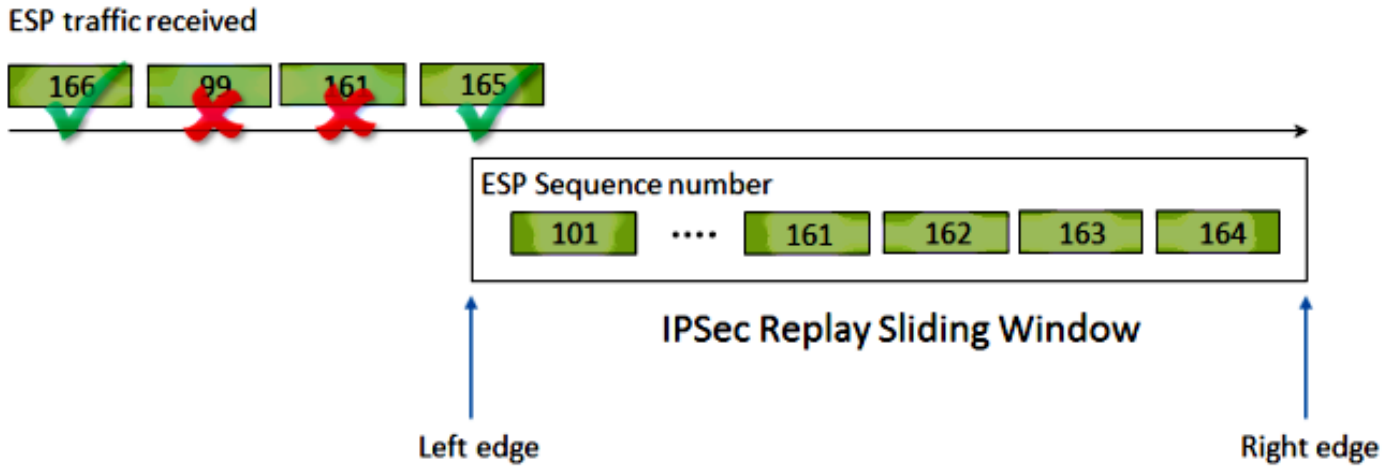
معلومات أساسية

نظرة عامة على هجمات إعادة التشغيل

هجوم إعادة التشغيل هو شكل من أشكال هجوم الشبكة يتم فيه تسجيل إرسال البيانات الصحيحة بشكل خبيث وأو إحتيالي ثم تكرارها لاحقا. إنها محاولة لتخريب الأمن من قبل شخص يقوم بتسجيل إتصالات مشروعة ويكررها من أجل انتحال شخصية مستخدم صالح وإعاقة الاتصالات الشرعية أو إحداث تأثير سلبي عليها.

حماية التحقق من إعادة تشغيل IPsec

يتم تعيين رقم تسلسل يتزايد بشكل متكرر لكل حزمة مشفرة بواسطة IPsec لتوفير الحماية ضد إعادة التشغيل ضد الهجوم. تحافظ نقطة نهاية IPsec المتلقية على تعقب الحزم التي قامت بمعالجتها بالفعل عند إستخدام هذه الأرقام ونافذة منزلقة لأرقام التسلسل المقبولة. الحجم الافتراضي للنافذة المضادة لإعادة التشغيل في تطبيق Cisco IOS® هو 64 حزمة، كما هو موضح في هذه الصورة:



عند تمكين حماية ضد إعادة التشغيل لنقطة نهاية نفق IPsec، تتم معالجة حركة مرور IPsec الواردة كما يلي:

- إذا كان رقم التسلسل يقع داخل النافذة ولم يتم إستلامه من قبل، فإن الحزمة يتم التحقق من تكاملها. إذا تجاوزت الحزمة فحص التحقق من السلامة، يتم قبولها ويلاحظ الموجه أن رقم التسلسل هذا قد تم إستلامه. على سبيل المثال، حزمة مع تضمين حمولة الأمان (ESP) الرقم التسلسلي 162.
- إذا كان رقم التسلسل يقع داخل النافذة ولكنه تم إستقباله مسبقا، فسيتم إسقاط الحزمة. يتم تجاهل هذه الحزمة المكررة ويتم تسجيل الإسقاط في عداد إعادة التشغيل.

- إذا كان رقم التسلسل أكبر من أعلى رقم تسلسل في النافذة، فإن الحزمة يتم التحقق من تكاملها. إذا تجاوزت الحزمة التحقق من السلامة، فإن الإطار المنزلق يتم نقله إلى اليمين. على سبيل المثال، إذا تم تلقي حزمة صالحة برقم تسلسلي 189، فسيتم تعيين الحافة اليمنى الجديدة للنافذة على 189، والحافة اليسرى على 125 (189 - 64 [حجم النافذة]).

- إذا كان رقم التسلسل أقل من الحافة اليسرى، فإن الحزمة يتم إسقاطها وتسجيلها داخل عداد إعادة التشغيل. تعتبر هذه حزمة خارج الترتيب.

في الحالات التي يحدث فيها فشل التحقق من إعادة التشغيل وإسقاط الحزمة، يقوم الموجه بإنشاء رسالة syslog مماثلة لهذا:

```
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle n, src_addr x.x.x.x, dest_addr y.
```

ملاحظة: يستند اكتشاف إعادة التشغيل إلى افتراض وجود اقتران أمان IPsec (SA) بين نظراء فقط. تستخدم Group Encrypted Transport VPN (GETVPN) رسالة SA واحدة من IPsec بين العديد من الأقران. وتتيجة لذلك، يستخدم GETVPN آلية تحقق ضد إعادة التشغيل مختلفة تماما تسمى فشل مكافحة إعادة التشغيل المستند إلى الوقت. يغطي هذا المستند فقط مكافحة إعادة التشغيل المستندة إلى العداد لأنفاق IPsec من نقطة إلى نقطة.

ملاحظة: تعد الحماية ضد إعادة التشغيل خدمة أمان مهمة يقدمها بروتوكول IPsec. يترتب على تعطيل مكافحة إعادة تشغيل IPsec تبعات أمان ويجب القيام به بفطنة.

المشاكل التي يمكن أن تتسبب في عمليات إسقاط إعادة تشغيل IPsec

وكما تم وصفه مسبقا، فإن الغرض من عمليات التحقق من إعادة التشغيل هو الحماية من التكرارات الضارة للحزم. ومع ذلك، هناك بعض السيناريوهات التي قد لا يكون فيها التحقق من إعادة التشغيل الفاشل راجعا إلى سبب ضار:

- قد ينتج الخطأ من حزمة كافية تم إعادة ترتيبها في مسار الشبكة بين نقاط نهاية النفق. من المحتمل أن يحدث ذلك إذا كان هناك مسارات شبكة متعددة بين الأقران.
- قد يحدث الخطأ بسبب مسارات معالجة الحزم غير المتساوية داخل Cisco IOS. على سبيل المثال، قد يتم تأجيل حزم IPsec المجزأة التي تتطلب إعادة تجميع IP قبل فك التشفير بشكل كاف، وأنها تقع خارج نافذة إعادة التشغيل عند وقت معالجتها.
- قد يرجع سبب الخطأ إلى جودة الخدمة (QoS) التي تم تمكينها على نقطة نهاية IPsec المرسلة أو داخل مسار الشبكة. مع تنفيذ Cisco IOS، يحدث تشفير IPsec قبل QoS في إتجاه المخرج. قد تتسبب بعض ميزات جودة الخدمة، مثل قوائم انتظار تقليل التأخير (LLQ)، في جعل تسليم حزم IPsec خارج الترتيب وإفالتها من قبل نقطة نهاية الاستلام بسبب فشل التحقق من إعادة التشغيل.
- قد تقوم مشكلة تكوين الشبكة/التشغيل بتكرار الحزم أثناء نقلها للشبكة.

- يمكن للمهاجم (الدخيل) تأجيل حركة مرور ESP وإفالتها وتكرار تكرارها.

أستكشاف أخطاء إعادة تشغيل IPsec وإصلاحها

يتمثل المفتاح لاستكشاف أخطاء عمليات إسقاط إعادة تشغيل IPsec وإصلاحها في تحديد ما الحزم التي تم إسقاطها بسبب إعادة التشغيل، واستخدام عمليات التقاط الحزم لتحديد إذا كانت هذه الحزم هي بالفعل حزم أو حزم تمت إعادة تشغيلها بالفعل والتي وصلت إلى موجه الاستقبال خارج نافذة إعادة التشغيل. لمطابقة الحزم المسقطة بشكل صحيح مع ما تم التقاطه في تتبع sniffer، تتمثل الخطوة الأولى في تحديد النظير وتدفق IPsec الذي تنتمي إليه الحزم المسقطة ورقم تسلسل ESP للحزمة.

إستخدام ميزة تتبع حزم البيانات Cisco IOS XE

على الأنظمة الأساسية للموجه التي تشغل Cisco IOS® XE، يتم طباعة معلومات حول إسقاط، النظير بالإضافة إلى فهرس معلمات أمان IPsec (SPI) في رسالة syslog عند حدوث إعادة تشغيل. ومع ذلك، هناك معلومة للمساعدة في أستكشاف أخطاء منع إعادة التشغيل وإصلاحها. يتم إستخدام رقم تسلسل ESP (ESP). وهي رقم تسلسل موفر خدمة الإنترنت، وهي رئيسية لا تزال تفتقد. بدون رقم تسلسل ESP لتحديد حزمة IPsec بشكل فريد داخل تدفق IPsec معين.

التسلسل، يصبح من الصعب تحديد الحزمة التي يتم إسقاطها في التقاط الحزمة بالضبط.

يمكن إستخدام ميزة تتبع حزم بيانات Cisco IOS XE في هذه الحالة عند ملاحظة إسقاط إعادة التشغيل، باستخدام رسالة syslog هذه:

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:060 TS:00000001132883828011
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3, src_addr 10.2.0.200, dest_addr
```

للمساعدة في تحديد رقم تسلسل ESP للحزمة التي تم إسقاطها، أكمل الخطوات التالية باستخدام ميزة تعقب الحزمة:

1. قم بإعداد مرشح تصحيح الأخطاء الشرطي للنظام الأساسي لمطابقة حركة المرور من جهاز النظير:

```
debug platform condition ipv4 10.2.0.200/32 ingress
debug platform condition start
```

1. قم بتمكين تتبع الحزمة باستخدام خيار النسخ لنسخ معلومات رأس الحزمة:

```
debug platform packet enable
debug platform packet-trace packet 64
debug platform packet-trace copy packet input l3 size 100
```

1. عند اكتشاف أخطاء إعادة التشغيل، أستخدم المخزن المؤقت لتتبع الحزمة لتحديد الحزمة التي سقطت بسبب إعادة التشغيل، ويمكن العثور على رقم تسلسل ESP في الحزمة التي تم نسخها:

```
<#root>

Router#

show platform packet-trace summary


Pkt   Input           Output          State  Reason
0     Gi4/0/0         Tu1             CONS   Packet Consumed
1     Gi4/0/0         Tu1             CONS   Packet Consumed
2     Gi4/0/0         Tu1             CONS   Packet Consumed
3     Gi4/0/0         Tu1             CONS   Packet Consumed
4     Gi4/0/0         Tu1             CONS   Packet Consumed
5     Gi4/0/0         Tu1             CONS   Packet Consumed

6     Gi4/0/0         Tu1             DROP   053 (IpsecInput)
```

```
7     Gi4/0/0          Tu1              DROP   053 (IpsecInput)

8     Gi4/0/0          Tu1              CONS   Packet Consumed
9     Gi4/0/0          Tu1              CONS   Packet Consumed
10    Gi4/0/0          Tu1              CONS   Packet Consumed
11    Gi4/0/0          Tu1              CONS   Packet Consumed
12    Gi4/0/0          Tu1              CONS   Packet Consumed
13    Gi4/0/0          Tu1              CONS   Packet Consumed
```

يظهر الإخراج السابق أن رقمي الحزمة 6 و 7 تم إسقاطهما، لذلك يمكن فحصهما بالتفصيل الآن:

<#root>

```
Router#
```

show platform packet-trace packet 6

```
/>Packet: 6           CBUG ID: 6
Summary
  Input     : GigabitEthernet4/0/0
  Output    : Tunnel1
  State     : DROP 053 (IpsecInput)
  Timestamp : 3233497953773
Path Trace
  Feature: IPV4
    Source      : 10.2.0.200
    Destination : 10.1.0.100
    Protocol    : 50 (ESP)
  Feature: IPSec
    Action    : DECRYPT
    SA Handle : 3
    SPI       :
```

0x4c1d1e90

```
    Peer Addr :
```

10.2.0.200

```
    Local Addr: 10.1.0.100
  Feature: IPSec
    Action    : DROP
    Sub-code  :
```

019 - CD_IN_ANTI_REPLAY_FAIL

```
Packet Copy In
  45000428 00110000 fc329575 0a0200c8 0a010064 4c1d1e90
```

00000006

```
790aa252
 e9951cd9 57024433 d97c7cb8 58e0c869 2101f1ef 148c2a12 f309171d 1b7a4771
 d8868af7 7bae9967 7d880197 46c6a079 d0143e43 c9024c61 0045280a d57b2f5e
 23f06bc3 ab6b6b81 c1b17936 98939509 7aec966e 4dd848d2 60517162 9308ba5d
```

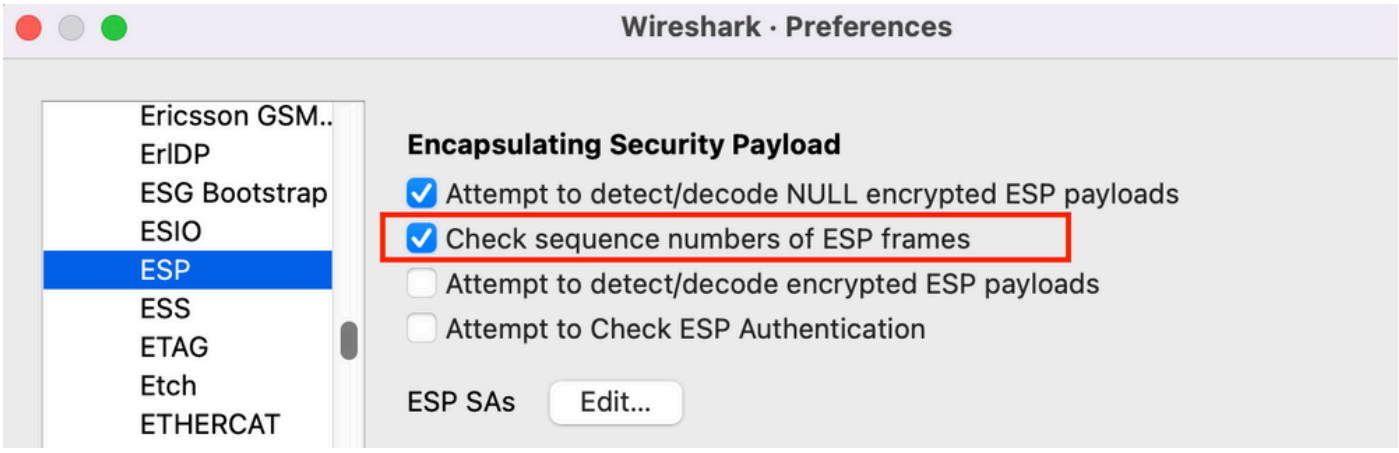
يحتوي رقم تسلسل ESP على إزاحة مقدارها 24 بايت تبدأ من رأس IP (أو 4 بايت من بيانات حمولة حزمة IP)، كما تم التأكيد عليه بالأسود في الإخراج السابق. في هذا المثال الخاص، يكون رقم تسلسل ESP للحزمة المسقطة هو 0x6.

تجميع التقاط الحزم

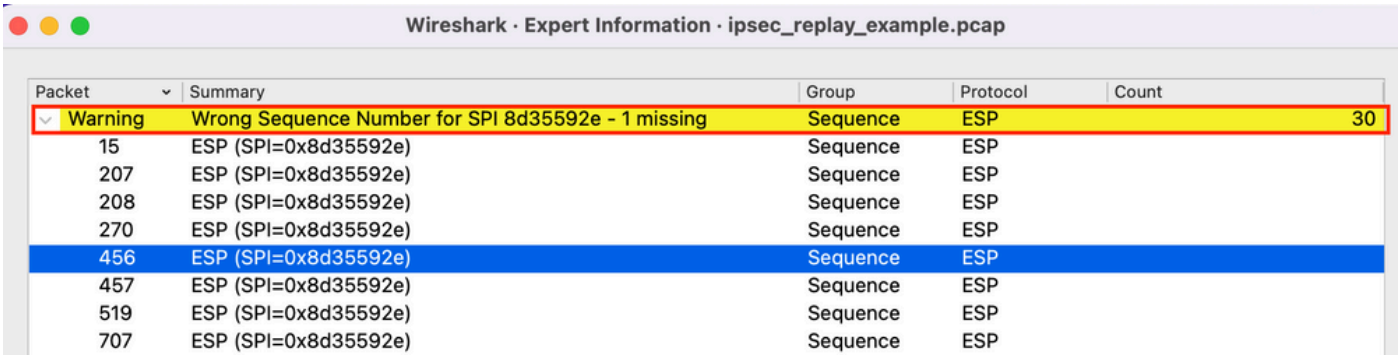
بالإضافة إلى تعريف معلومات الحزمة للحزمة التي سقطت بسبب فشل التحقق من إعادة التشغيل، يلزم تجميع التقاط حزمة لتدفق IPsec المعني في نفس الوقت. وهذا يساعد في فحص نمط رقم تسلسل ESP داخل نفس تدفق IPsec للمساعدة في تحديد سبب إسقاط إعادة التشغيل. للحصول على تفاصيل حول كيفية إستخدام التقاط الحزمة المضمنة (EPC) على موجهات Cisco IOS XE، راجع [التقاط الحزمة المضمنة لمثال تكوين Cisco IOS و Cisco IOS XE](#).

إستخدام تحليل رقم تسلسل Wireshark

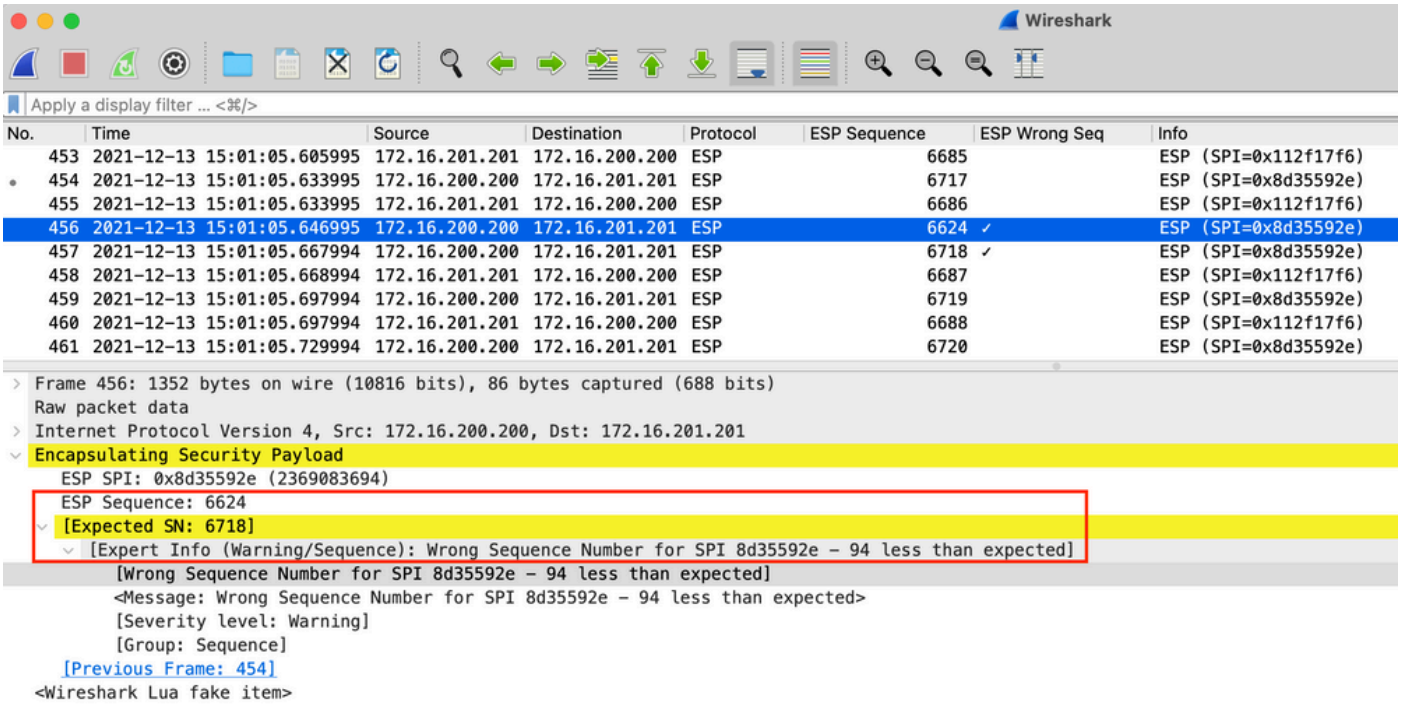
بمجرد تجميع التقاط الحزمة للحزم المشفرة (ESP) على واجهة WAN، يمكن إستخدام Wireshark لإجراء تحليل رقم تسلسل ESP لأي شذوذ في رقم التسلسل. أولا، تأكد من تمكين التحقق من الرقم التسلسلي تحت تفضيلات > بروتوكولات > ESP كما هو موضح في الصورة:



تحقق بعد ذلك من أي مشاكل متعلقة برقم تسلسل ESP في التحليل > معلومات الخبراء كما يلي:



انقر على أي من الحزم التي تحتوي على رقم تسلسل خاطئ للحصول على تفاصيل إضافية كما يلي:



الحل

بعد تحديد النظير وتجميع التقاط الحزمة لعمليات إسقاط إعادة التشغيل، يمكن لثلاثة سيناريوهات محتملة شرح حالات فشل إعادة التشغيل:

1. إنها حزمة صالحة تم إرجاؤها:
   يساعد التقاط الحزمة على تأكيد ما إذا كانت الحزمة صحيحة بالفعل، وإذا كانت المشكلة غير مهمة (بسبب زمن وصول الشبكة أو مشاكل مسار الإرسال) أو تتطلب استكشاف أخطاء المسار وإصلاحها بشكل أكثر عمقا. على سبيل المثال، يظهر التقاط حزمة ذات رقم تسلسلي من X يصل خارج الترتيب، ويضبط حجم نافذة إعادة التشغيل حاليا على 64. إذا وصلت حزمة صالحة برقم تسلسلي (X + 64) قبل الحزمة X، يتم تحويل النافذة إلى اليمين ثم يتم إسقاط الحزمة X بسبب فشل إعادة التشغيل.

   في مثل هذه السيناريوهات، من الممكن زيادة حجم نافذة إعادة التشغيل أو تعطيل التحقق من إعادة التشغيل لضمان أن مثل هذا التأخير يعتبر مقبولا ولا يتم تجاهل

الحزم الشرعية. بشكل افتراضي، يكون حجم نافذة إعادة التشغيل صغير إلى حد ما (حجم النافذة 64). إذا قمت بزيادة الحجم، فإنه لا يزيد بشكل كبير من خطر حدوث هجوم. لمزيد من المعلومات حول كيفية تكوين نافذة مكافحة إعادة تشغيل IPsec، ارجع إلى كيفية تكوين نافذة مكافحة إعادة تشغيل IPsec: توسيع المستند وتعطيله.

تلميح: إذا تم تعطيل نافذة إعادة التشغيل أو تعديله في ملف تعريف IPSec المستخدم على واجهة النفق الظاهرية (VTI)، فلن تصبح التغييرات نافذة المفعول حتى تتم إزالة ملف تعريف الحماية وإعادة تطبيقه أو إعادة تعيين واجهة النفق. هذا سلوك متوقع لأن ملفات تعريف IPsec عبارة عن قالب يتم إستخدامه لإنشاء خريطة ملف تعريف نفق عند إظهار واجهة النفق. إذا كانت الواجهة قيد التشغيل بالفعل، فإن التغييرات التي يتم إجراؤها على ملف التعريف لا تؤثر على النفق حتى تتم إعادة تعيين الواجهة.

ملاحظة: لم تدعم طرز موجه خدمات التجميع المبكرة (ASR) 1000 (مثل ASR1000 مع ESP5 و ESP10 و ESP20 و ESP40، بالإضافة إلى ASR1001) حجم نافذة يبلغ 1024 على الرغم من أن واجهة سطر الأوامر (CLI) سمحت بهذا التكوين. ونتيجة لذلك، قد لا يكون حجم النافذة الذي تم الإعلام عنه في إخراج الأمر show crypto ipSec صحيحا. أستخدم الأمر show crypto ipSec sa peer ip-address platform للتحقق من حجم النافذة المضادة لإعادة التشغيل بالجهاز. الحجم الافتراضي للنافذة هو 64 حزمة على كل الأنظمة الأساسية. أحلت ل كثير معلومة، cisco بق id CSCso45946. تدعم منصات توجيه Cisco IOS XE الأحدث (مثل ASR1K مع ESP100 و ESP200، ASR1001-X و ASR1002-X، موجهات سلسلة موجه الخدمة المتكاملة (ISR) 4000، وموجهات سلسلة Catalyst8000) حجم نافذة من 1024 حزمة في الإصدارات 15.2(2)S والإصدارات الأحدث.

---

2. وذلك بسبب تكوين جودة الخدمة على نقطة نهاية الإرسال:
ويتطلب هذا الوضع فحصا دقيقا ومعايرة بعض جودة الخدمة من أجل تخفيف الحالة. للحصول على وصف أكثر عمقا لهذا الموضوع والحل المحتمل، ارجع إلى الاعتبارات المضادة لإعادة التشغيل في مقالة خاصة ب IPSec VPN (V3PN) تم تمكين IPSec مع.

3. هي حزمة مكررة تم تلقيها مسبقا:
إذا كان هذا هو الحال، يمكن ملاحظة حزمتين أو أكثر لهما رقم تسلسل ESP نفسه داخل تدفق IPsec نفسه في التقاط الحزمة. في هذه الحالة، يتوقع إسقاط الحزمة حيث تعمل حماية إعادة تشغيل IPsec كما هو متوقع لمنع هجمات إعادة التشغيل في الشبكة، و syslog عبارة عن معلومات فقط. إذا إستمرت هذه الحالة، فيجب التحقيق فيها كتهديد أمني محتمل.

ملاحظة: لا يتم عرض حالات فشل التحقق من إعادة التشغيل إلا عند تمكين خوارزمية المصادقة في مجموعة تحويل IPsec. طريقة أخرى لمنع رسالة الخطأ هذه هي تعطيل المصادقة وإجراء التشفير فقط، ومع ذلك، يتم تثبيط هذا بشدة بسبب التأثيرات الأمنية للمصادقة المعطلة.

معلومات إضافية

أستكشاف أخطاء إعادة التشغيل وإصلاحها على الموجهات القديمة باستخدام برنامج Cisco IOS التقليدي

تسقط إعادة تشغيل IPsec على موجهات سلسلة ISR G2 القديمة التي تستخدم CISCO IOS مختلفة عن الموجهات التي تستخدم Cisco IOS XE، كما هو موضح هنا:

```
<#root>

%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed

connection id=529, sequence number=13
```

الحظ أن إخراج الرسالة ال يوفر عنوان IP للنظير وأو معلومات SPI. الاستكشاف الأخطاء وإصلاحها على هذا النظام الأساسي، أستخدم "conn-id" في رسالة الخطأ. قم بتعريف "conn-id" في رسالة الخطأ، وابحث عنه في إخراج show crypto ipSec، نظرا لأن إعادة التشغيل هي لكل SA (مقارنة بكل نظير). توفر رسالة syslog أيضا رقم تسلسل ESP، والذي يمكن أن يساعد في التعرف بشكل فريد على الحزمة المسقطة في التقاط الحزمة.

ملاحظة: مع إصدارات مختلفة من الرمز، يكون "conn-id" وهو معرف conn أو flow_id ل SA الوارد.

وهذا موضح هنا:

```
<#root>

%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed

connection id=529, sequence number=13


Router#

show crypto ipsec sa | in peer|conn id


   current_peer 10.2.0.200 port 500

conn id: 529

, flow_id: SW:529, sibling_flags 80000046, crypto map: Tunnel0-head-0
        conn id: 530, flow_id: SW:530, sibling_flags 80000046, crypto map: Tunnel0-head-0
Router#

Router#

show crypto ipsec sa peer 10.2.0.200 detail
```

```
   interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.0.100

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 10.2.0.200 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27
    #pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
    #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
    #pkts invalid prot (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
```

##pkts replay failed (rcv): 21

```
    #pkts internal err (send): 0, #pkts internal err (recv) 0

     local crypto endpt.: 10.1.0.100, remote crypto endpt.: 10.2.0.200
     path mtu 2000, ip mtu 2000, ip mtu idb Serial2/0
     current outbound spi: 0x8B087377(2332586871)
     PFS (Y/N): N, DH group: none

               inbound esp sas:
```

spi: 0xE7EDE943(3891128643)

```
        transform: esp-gcm ,
        in use settings ={Tunnel, }
        conn id: 529, flow_id: SW:529, sibling_flags 80000046, crypto map:
        Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4509600/3223)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

<SNIP>
```

10.2.0.200 ريظنلا ناونع نم ليغشتلا ةداعإ طاقسإ متي ،جارخإلا اذه نم هتظحالم نكمي امك عم ESP SA SPI الوارد نم 0xE7EDE943. امك نكمي ةظحالم نأ مقر لسلست ESP ةمزحلل يتلا SPI مقرو ريظنلا ناونع ةعومجم مادختسإ نكمي .اهسفن لجسلا ةلاسر نم 13 وه اهطاقسإ مت لسلست مقرو ESP ديدحتل ةمزحلا يتلا مت اهطاقسإ يف طاقتلا ةمزحلا لكشب ديرف.

ةظحالم: نوكت ةلاسر Cisco IOS Syslog ةدودحم لدعمل ةمزحل ىوتسم تانايبلا يتلا طقست ىلإ دحاو يف ةقيقدلا. للوصحلل ىلع ددع قيقد نم مزحلا يتلا مت اهطاقسإ، مدختسأ رمألا show crypto ipSec detail امك وه حضوم اقبسم.

العمل باستخدام برنامج Cisco IOS XE السابق

في الموجهات التي تشغل إصدارات Cisco IOS XE السابقة، قد يقوم "replay_error" التي تم الإعلام عنها في Syslog بطباعة تدفق IPsec الفعلي باستخدام معلومات النظير حيث يتم إسقاط الحزمة التي تمت إعادة تشغيلها، كما هو موضح هنا:

```
%IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread: 095 TS:00000000240306197890
%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 3
```

لتحديد معلومات نظير IPsec الصحيحة وتدفق البيانات، أستخدم مؤشر مستوى البيانات (DP) المطبوع في رسالة syslog كمؤشر معلمة الإدخال SA في هذا الأمر، لاسترداد معلومات تدفق IPsec على معالج تدفق الكم (QFP):

<#root>

```
Router#
```

show platform hardware qfp active feature ipsec sa 3

```
QFP ipsec sa Information

         QFP sa  id: 3
          pal sa id: 2
         QFP spd id: 1
          QFP sp id: 2
            QFP spi:
```

0x4c1d1e90(1276976784)

```
         crypto ctx: 0x000000002e03bfff
              flags: 0xc000800
                   : src:IKE  valid:Yes  soft-life-expired:No  hard-life-expired:No
                   :
```

replay-check:Yes

```
  proto:0  mode:0  direction:0
                   : qos_preclassify:No  qos_group:No
                   : frag_type:BEFORE_ENCRYPT  df_bit_type:COPY
                   : sar_enable:No  getvpn_mode:SNDRCV_SA
                   : doing_translation:No  assigned_outside_rport:No
                   : inline_tagging_enabled:No
          qos_group: 0x0
                mtu: 0x0=0
          sar_delta: 0
         sar_window: 0x0
         sibling_sa: 0x0
             sp_ptr: 0x8c392000
            sbs_ptr: 0x8bfbf810
```

local endpoint: 10.1.0.100
remote endpoint: 10.2.0.200

```
   cgid.cid.fid.rid: 0.0.0.0
               ivrf: 0
               fvrf: 0
    trans udp sport: 0
    trans udp dport: 0
    first intf name: Tunnel1
  <SNIP>
```

يمكن أيضا إستخدام برنامج نصي مضمن لإدارة الأحداث (EEM) لأتمتة مجموعة البيانات:

```
event manager applet Replay-Error
 event syslog pattern "%IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error"
 action 1.0 regexp "([0-9]+)$" "$_syslog_msg" dph
 action 2.0 cli command "enable"
 action 3.0 cli command "show platform hardware qfp active feature ipsec sa $dph |
 append bootflash:replay-error.txt"
```

في هذا المثال، تتم إعادة توجيه المخرجات التي تم تجميعها إلى ذاكرة التمهيد المؤقتة (bootflash). لعرض هذا الإخراج، أستخدم الأمر more bootflash:replay-error.txt.

معلومات ذات صلة

- تصميم شبكة مرجع حل IPSec VPN (V3PN) الذي تم تمكين الصوت والفيديو
- كيفية تكوين نافذة مكافحة إعادة تشغيل IPsec: التوسيع والتعطيل.
- الدعم التقني والمستندات - Cisco Systems

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).