أستكشاف أخطاء IPsec وإصلاحها الخاصة بأنفاق الخدمة على الحواف مع IKEv2

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء أكثر المشاكل شيوعا الخاصة بأنفاق أمان تبادل الإنترنت (IPsec) لأجهزة الطرف الثالث التي تم تكوين الإصدار 2 من بروتوكول الإنترنت (IKEv2) لها وإصلاحها. يشار إليها بشكل شائع باسم أنفاق الخدمة/النقل عبر وثائق Cisco SD-WAN. يشرح هذا المستند أيضا كيفية تمكين تصحيح أخطاء IKE وقراءتها وربطها بتبادل الحزم لفهم نقطة الفشل على تفاوض IPsec.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- IKEv2
- تفاوض IPsec
- تقنية SD-WAN من Cisco

المكونات المستخدمة

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.

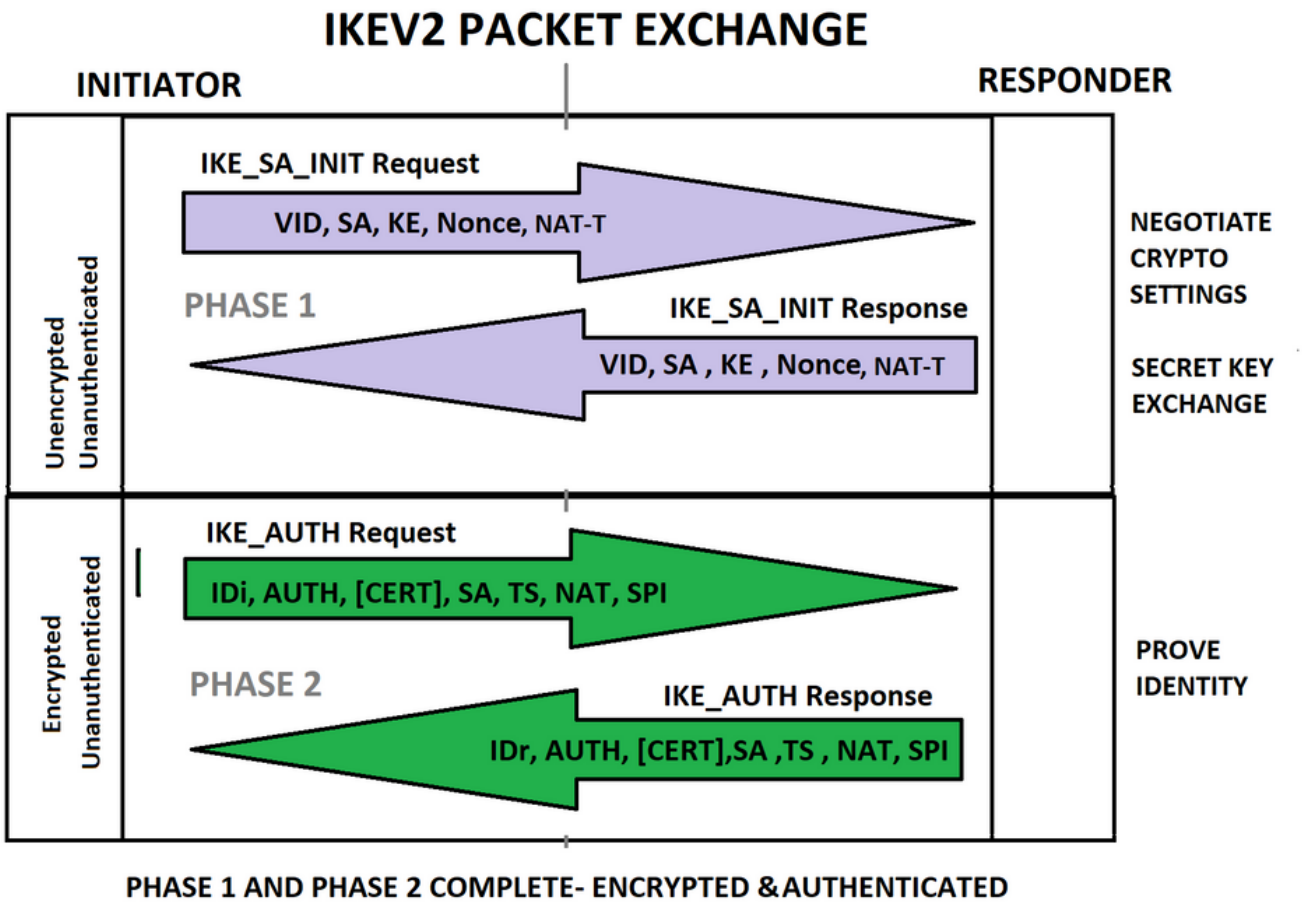
معلومات أساسية

مسرد إيك

- **أمان بروتوكول الإنترنت (IPsec)** هي مجموعة قياسية من البروتوكولات بين نقطتي اتصال عبر شبكة IP توفر مصادقة البيانات وسلامتها وسريتها.
- **Internet Key Exchange الإصدار 2 (IKEv2) هو البروتوكول المستخدم لإعداد اقتران أمان (SA) في مجموعة بروتوكولات IPsec.**
- **اقتران الأمان** (SA) هو إنشاء سمات أمان مشتركة بين كيانين على الشبكة لدعم الاتصال الآمن. يمكن أن تتضمن حالة الوصول (SA) سمات مثل خوارزمية التشفير والوضع ومفاتيح تشفير حركة المرور والمعلومات لبيانات الشبكة التي سيتم تمريرها عبر الاتصال.
- يتم إستخدام **معرفات المورد** (VID) لتحديد أجهزة النظير باستخدام تنفيذ المورد نفسه لدعم المميزات الخاصة بالمورد.
- **Nonce**: قيم عشوائية تم إنشاؤها في Exchange لإضافة العشوائية ومنع هجمات إعادة التشغيل.
- معلومات **تبادل المفاتيح (KE)** لعملية تبادل المفاتيح الآمنة Diffie-Hellman (DH).
- **يتم إستخدام Identity Initiator/Responder (IDi/IDr)** لإرسال معلومات المصادقة إلى النظير. يتم إرسال هذه المعلومات تحت حماية السر المشترك المشترك المشترك.
- يمكن اشتقاق المفاتيح المشترك IPSec باستخدام DH مرة أخرى لضمان **سرية إعادة التوجيه الكاملة (PFS)** أو تحديث السر المشترك المشتق من تبادل DH الأصلي.
- **تبادل مفاتيح Diffie-Hellman (DH) هو طريقة لتبادل خوارزميات التشفير بأمان عبر قناة عامة.**
- **محددات حركة المرور (TS)** هي هويات الوكيل أو حركة مرور البيانات المتبادلة على مفاوضات IPsec للمرور عبر النفق المشفر.

تبادل حزم IKEv2

تحتوي كل حزمة من حزم IKE على معلومات الحمولة لإنشاء النفق. يشرح مسرد IKE الاختصارات المعروضة على هذه الصورة كجزء من محتوى الحمولة لتبادل الحزم.

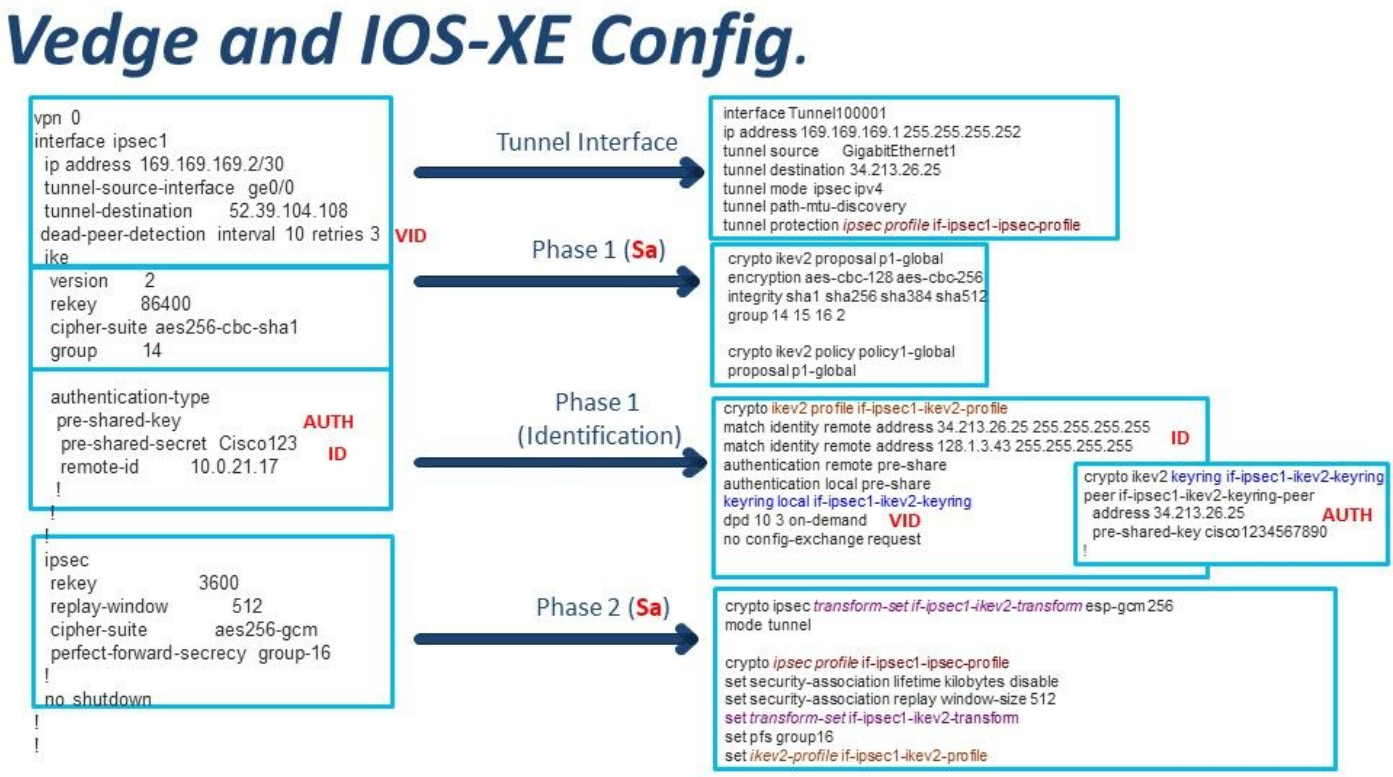


IKEv2-Exchange

ملاحظة: من المهم التحقق من تبادل الحزمة لمفاوضات IKE فشل نفق IPsec في التحليل السريع للتكوين المتضمن لمعالجة المشكلة بشكل فعال.

ملاحظة: لا يصف هذه المستند عملية تبادل حزم IKEv2 بشكل أعمق. لمزيد من المراجع، انتقل إلى [تبادل حزم IKEv2 وتصحيح أخطاء مستوى البروتوكول]

يلزم ربط تكوين vEdge مقابل تكوين Cisco IOS® XE. كما أنه من المفيد مطابقة مفاهيم IPsec ومحتوى الحمولة لعمليات تبادل حزم IKEv2 كما هو موضح في الصورة.



ملاحظة: يقوم كل جزء من التكوين بتعديل أحد جوانب تبادل تفاوض IKE. من المهم ربط الأوامر بتفاوض بروتوكول IPsec.

استكشاف الأخطاء وإصلاحها

تمكين تصحيح أخطاء IKE

يتيح تصحيح أخطاء InEdges IKED معلومات مستوى تصحيح الأخطاء إما IKEv1 أو IKEv2.

```
debug iked misc high
debug iked event high
```

من الممكن عرض معلومات تصحيح الأخطاء الحالية ضمن **vshell** وتشغيل الأمر **tail -f <debug path>**.

```
vshell
tail -f /var/log/message
```

في CLI يمكن أيضا أن يعرض السجلات الحالية/معلومات تصحيح الأخطاء للمسار المحدد.

```
monitor start /var/log/messages
```

تلميحات لبدء عملية أستكشاف أخطاء IPsec وإصلاحها

من الممكن فصل ثلاثة سيناريوهات IPsec مختلفة. وهي نقطة مرجعية جيدة لتحديد العوارض ان يكون هنالك نهج افضل لتعرف كيف تبدأ.

1. لم يتم إنشاء نفق IPsec.
2. نفق IPsec انخفض وعاد ليؤسس لوحده. (متصل)

3. تم تعطيل نفق IPsec ويبقى في حالة انخفاض.

بالنسبة لنفق IPsec الذي يسجل أعراض، يلزم تصحيح الأخطاء في الوقت الفعلي للتحقق من السلوك الحالي على مفاوضات IKE.

بالنسبة لنفق IPsec الذي أعراضه وإعادة تأسيسه على أعراض خاصة، والمعروف بشكل عام باسم Tunnel Flved وتحليل السبب الجذري (RCA) مطلوب. الـ بد من معرفة الطابع الزمني عند هبوط النفق أو تشخيص وقت محدد للنظر في تصحيح الأخطاء.

لأن نفق IPsec لن يستمر على أعراض الحالة المنخفضة، وهذا يعني النفق الذي عمل من قبل ولكن لأي سبب، تم وزنه وتحتاج إلى معرفة السبب والسلوك العادي الحالي الذي يمنع إنشاء النفق بجانب مرة أخرى.

تعرف على النقاط قبل بدء استكشاف الأخطاء وإصلاحها:

1. نفق IPsec (المقر) مع المشاكل والتكوين.
2. الطابع الزمني الذي تم فيه تنزيل النفق (إذا كان ذلك ممكنا).
3. عنوان IP لنظير IPsec (وجهة النفق).

بالنسبة للسجلات، يتم حفظ جميع السجلات والتصحيحات على ملفات **/var/log/messages**، بالنسبة للسجلات الحالية، يتم حفظها في ملف الرسائل ولكن هذا العرض المحدد يمكن تحديد الرفرفة بعد الرسائل على الصلة ذات التصحيح أخطاء أن تكون من المحتمل، والمشكلة من الأيام/الساعات من 1،2،3..إلخ. من المهم معرفة الطابع الزمني للنظر إلى ملف الرسالة الصحيح وتحليل تصحيح الأخطاء (charon) لمفاوضات IKE الخاصة بالنفق المرتبط ب IPsec.

تطبع معظم تصحيح الأخطاء مقر نفق IPsec. الطريقة الأكثر شيوعا للتعرف على التفاوض على الحالة. تمت فلترة النفق حيث يتم توفير عنوان IP للنظير البعيد وعنوان IP هي والحزم على الأمثلة بعض تصحيح أخطاء IKE:

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_IPsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
```

تظهر تصحيح أخطاء مفاوضات IKE Init مقر نفق IPsec، ومع ذلك، فإن المعلومات التالية لتبادل الحزم تستخدم عناوين IP الخاصة بنفق IPsec فقط.

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_ipsec2_1'
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1
Jun 18 00:31:22 vedge01 charon: 16[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jun 18 00:31:22 vedge01 charon: 16[NET] sending packet: from 10.132.3.92[500] to 10.10.10.1[500]
(464 bytes)
Jun 18 00:31:22 vedge01 charon: 12[NET] received packet: from 10.10.10.1[500] to
10.132.3.92[500] (468 bytes)
Jun 18 00:31:22 vedge01 charon: 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) N(HTTP_CERT_LOOK) N(FRAG_SUP) V ]
Jun 18 00:31:22 vedge01 charon: 12[ENC] received unknown vendor ID:
4f:85:58:17:1d:21:a0:8d:69:cb:5f:60:9b:3c:06:00
Jun 18 00:31:22 vedge01 charon: 12[IKE] local host is behind NAT, sending keep alives
```

تكوين نفق IPsec:

```
interface ipsec2 ip address 192.168.1.9/30 tunnel-source 10.132.3.92 tunnel-destination
10.10.10.1 dead-peer-detection interval 30 ike version 2 rekey 86400 cipher-suite aes256-cbc-
sha1 group 14 authentication-type pre-shared-key pre-shared-secret
$8$wgrs/Cw6tX0na34yF4Fga0B62mGBpHFdOzFaRmoYfnBioWVO3s3efFPBbkaZqvoN ! ! ! ipsec rekey 3600
replay-window 512 cipher-suite aes256-gcm perfect-forward-secrecy group-14 !
```

العرض 1. لم يتم إنشاء نفق IPsec

وبما أن المشكلة يمكن أن تكون التطبيق الأول للنفق، فإنها لم تكن في وضع التشغيل وأن تصحيح أخطاء IKE هو الخيار الأفضل.

العرض 2. نفق "IPsec" تم تخفيضه أو إعيد بناءه لوحده

وكما ذكر سابقا، يجري عادة تناول هذا العرض لمعرفة السبب الجذري لانهيار النفق. ومع معرفة تحليل السبب الجذري، في بعض الأحيان، يمنع مسؤول الشبكة حدوث المزيد من المشاكل.

تعرف على النقاط قبل بدء أستكشاف الأخطاء وإصلاحها:

1. نفق IPsec (الرقم) مع المشاكل والتكوين.
2. الطابع الزمني الذي نزل فيه النفق.
3. عنوان IPsec للنظير (وجهة النفق)

عمليات إعادة إرسال DPD

في هذا المثال، نزل النفق في 18 يونيو في 00:31:17.

```
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec2
DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-vedge01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

ملاحظة: السجلات الموجودة في أسفل نفق IPsec ليست جزءا من سجلات *FTMD*. لذلك الطابع الزمني و*IKE*.

ملاحظة: الا تتم عادة طباعة السجلات ذات الصلة معا، ويكون هناك المزيد من المعلومات فيما بينها غير مرتبطة بنفس العملية.

الخطوة 1. بعد تحديد الطابع الزمني وتارابط الوقت والسجلات، ابدأ مراجعة السجلات من الأسفل إلى الأعلى.

```
Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits

Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
```

```
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
```

يتم وصف آخر عملية تبادل حزم DPD ناجحة على أنها الطلب رقم 542.

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 13.51.17.190[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]
```

الخطوة 2. عتمت بتجميع عيمج المعلومات اعم بالترتيب الصحيح:

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
10.132.3.92[4500] (76 bytes)
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]

Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3,
timeout=30, exchange=37, state=2)
Jun 18 00:28:22 Lvedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to
10.10.10.1[4500] (76 bytes)

Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec2 DOWN
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"LONDSR01" system-ip:4.0.5.1 vpn-id:1 if-
name:"ipsec2" new-state:down
```

على سبيل المثال الموضح، يتم تقليل قيمة النفق بسبب عدم تلقي vEdge01 مزحل تادحو 3 لاسرإ ةداعإ دعب "دوقفم" ىلع IPsec ريظن نييعت عقوتملا نم .10.10.10.1 نم DPD بيانات DPD، كما يتم إغلاق النفق. هناك عدة أسباب محتملة لهذا السلوك، عادة، ويرتبط ب ISP ةقيرط دجوت الف ،ةدحاو ةرم ةلكشملا تثدح اذإ .راسملا يف تطقس وأ ترسخ طبرلا ثيح ةمزحلا بقعت نكمي ،ةلكشملا ترمتسا اذإ ،كلذ عمو ،ةدوقفملا رورملا ةكرح بقعتل باستخدام التقاط على vEdge، والأقران البعيد ل IPSec، و ISP.

العرض 3. تم تعطيل نفق IPsec ويبقى في حالة الإنزال

ولم يتم إنزال، بسبب أي لأن نكلو قباسلا يف اديج لمعي قفنلا ناك ،ضرعلا اذه يف اقباس ركذ امك يتمكن النفق من التأسيس بنجاح من جديد. في هذا السيناريو، هناك إضافة إلى الشبكة.

تعرف على النقاط قبل بدء أستكشاف الأخطاء وإصلاحها:

1. نفق IPsec (الرقم) مع المشاكل والتكوين.
2. الطابع الزمني الذي نزل فيه النفق.
3. عنوان IPsec للنظير (وجهة النفق)

عدم تطابق PFS

في هذا المثال، لا يبدأ أستكشاف الأخطاء وإصلاحها مع الطابع الزمني عند انخفاض النفق. مع إستمرار المشكلة، فإن تصحيح أخطاء IKE هو الخيار الأفضل.

```
interface ipsec1 description VWAN_VPN ip address 192.168.0.101/30 tunnel-source-interface ge0/0
tunnel-destination 10.10.10.1 ike version 2 rekey 28800 cipher-suite aes256-cbc-sha1 group 2
authentication-type pre-shared-key pre-shared-secret
"$8$njK2pLLjgKWNQu0KecNtY3+fo3hbTs0/7iJy6unNtersmCGjGB38kIPjsoqqXZdVmtizLu79\naQdjt2POM242Yw=="
! ! ! ipsec rekey 3600 replay-window 512 cipher-suite aes256-cbc-sha1 perfect-forward-secrecy
group-16 ! mtu 1400 no shutdown
```

تم تمكين تصحيح الأخطاء وتم عرض التفاوض.

```
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (508 bytes)
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] parsed CREATE_CHILD_SA request 557 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] failed to establish CHILD_SA, keeping
IKE_SA
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] generating CREATE_CHILD_SA response 557 [
N(NO_PROP) ]
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)

daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (76 bytes)
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] parsed INFORMATIONAL request 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] generating INFORMATIONAL response 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] sending packet: from 172.28.0.36[4500] to
10.10.10.1[4500] (76 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to
172.28.0.36[4500] (396 bytes)
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[ENC] parsed CREATE_CHILD_SA request 559 [ SA No
TSi TSr ]
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] received proposals:
ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
```

```
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
daemon.info: Apr 27 05:12:58 Avedge01 charon: 07[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[IKE] failed to establish CHILD_SA, keeping
IKE_SA
```

> **ملاحظة:** يتم تبادل حزم CREATE_CHILD_SA لكل rekey أو sa جديد. لمزيد من المراجع، انتقل إلى [مهم تبادل حزم IKEv2](#)

تظهر تصحيحات IKE نفس السلوك ويتم تكراراها باستمرار، لذلك من الممكن أخذ جزء من المعلومات وتحليلها:

CREATE_CHILD_SA يعني rekey، مع الغرض من SPIS الجديد أن يكون خلق وتبادلت بين نقاط نهاية IPsec.

- يستقبل vEdge حزمة طلب CREATE_CHILD_SA من 10.10.10.1.
- يعالج Vedge الطلب ويتحقق من الاقتراحات (SA) المرسلة من النظير 10.10.10.1
- يقوم vEdge بمقارنة الاقتراح الذي تم إرساله بواسطة النظير مقابل مقترحاته التي تم تكوينها.
- يفشل CREATE_CHILD_SA المبادل مع "لم يتم العثور على اقتراحات مقبولة".

عند هذه النقطة، السؤال هو: **<u>لماذا هناك عدم تطابق في التكوين إذا كان النفق يعمل سابقا ولم يتم إجراء أي تغييرات؟</u>**

التحليل بعمق، يوجد حقل إضافي في الاقتراحات التي تم تكوينها والتي لا يرسلها النظير.

الاقتراحات المكونة: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ

العروض التي تم تلقيها:
esp:AES_GCM_16_256/NO_EXT_SEQ،
ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ،
ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ،
ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ،
ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ،
ESP:3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ

MODP_4096 هي مجموعة DH 16، والتي قام الحواف بتكوينها لملفات PFS (السرية التامة لإعادة التوجيه) على المرحلة 2 (قسم IPsec).

PFS هو التكوين غير المتطابق الوحيد الذي يمكن إنشاء النفق فيه بنجاح أو لا وفقا لمن هو البادئ أو المستجيب في تفاوض IKE. ومع ذلك، عندما يبدأ المفتاح لا يكون قادرا على الاستمرار وهذا العرض يمكن تقديمه أو الربط به.

لا تتم إعادة تشغيل نفق vEdge IPSec/IKEv2 بعد تمزيقه بسبب حدث DELETE

راجع فرعم تصحيح الأخطاء من Cisco [CSCvx86427](#) للحصول على مزيد من المعلومات حول هذا السلوك.

بينما تستمر المشكلة، تعد تصحيح أخطاء IKE أفضل الخيارات. ومع ذلك، بالنسبة لهذا الخطأ الخاص إذا تم تمكين تصحيح الأخطاء، لا يتم عرض أي معلومات لا إلى الوحدة الطرفية ولا ملف الرسالة.

لتضييق هذه المشكلة والتحقق من إذا كان vEdge يصدم معرف تصحيح الأخطاء من Cisco CSCvx86427، يلزم العثور على اللحظة التي يتم فيها إسقاط النفق.

تعرف على النقاط قبل بدء أستكشاف الأخطاء وإصلاحها:

1. نفق IPsec (الرقم) مع المشاكل والتكوين.
2. الطابع الزمني الذي نزل فيه النفق.
3. عنوان IPsec للنظير (وجهة النفق)

بعد تحديد الطابع الزمني، وترابط الوقت والسجلات، راجع السجلات قبل وقت انخفاض النفق مباشرة.

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] received DELETE for IKE_SA ipsec1_1[217]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between
10.16.0.5[10.16.0.5]...10.10.10.1[10.10.10.1]
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
Apr 13 22:05:21 vedge01 charon: 12[ENC] generating INFORMATIONAL response 4586 [ ]
Apr 13 22:05:21 vedge01 charon: 12[NET] sending packet: from 10.16.0.5[4500] to 10.10.10.1[4500]
(80 bytes)
Apr 13 22:05:21 vedge01 charon: 12[KNL] Deleting SAD entry with SPI 00000e77
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-FTMD-6-INFO-1000001: VPN 1 Interface
ipsec1 DOWN
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-ftmd-6-INFO-1400002: Notification:
interface-state-change severity-level:major host-name:"vedge01" system-ip:4.1.0.1 vpn-id:1 if-
name:"ipsec1" new-state:down
```

ملاحظة: هناك حزم حذف متعددة على تفاوض IPsec، والحذف ل CHILD_SA هو حذف متوقع، والحذف ل IKE_SA دون أي نقية حذف حزمة تلقي عند هذه المشكلة وتشاهد، و REKEY لعملية تفاوض IPsec معين. يؤدي هذا الحذف إلى إزالة كافة نفق IPsec/IKE.

معلومات ذات صلة

- تصحيح أخطاء مستوى البروتوكول وتبادل حزم KEv2
- تبادل مفتاح الإنترنت (IKE) - RFC 2409
- IKEv2 - RFC 7296
- شبكة LAN من موقع إلى شبكة LAN IPSec بين vEdge و Cisco IOS
- 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).