أستكشاف أخطاء أنفاق IPsec ومشكلات مستوى التحكم الشائعة مع عمليات التقاط الحزم وإصلاحها

المحتويات

المقدمة

يصف هذا المستند كيفية التقاط الحزمة، والأدوات الأخرى، والمساعدة في مشاكل مستوى التحكم عند التفاوض على شبكة VPN من موقع إلى موقع على موجهات Cisco IOS® XE.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين Cisco IOS® CLI.
- معرفة أساسية ب IKEv2 و IPsec.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- CSR1000V - برنامج Cisco IOS XE الإصدار 16.12.0.

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

لقطات الحزم هي أداة قوية لمساعدتك في التحقق مما إذا كانت الحزم يتم إرسالها/استقبالها بين أجهزة نظير VPN. كما أنها تؤكد ما إذا كان السلوك الذي يتم مشاهدته مع تصحيح أخطاء IPsec يتوافق مع الإخراج الذي يتم تجميعه على عمليات الالتقاط نظرا لأن عمليات تصحيح الأخطاء هي تفسير منطقي، ويمثل الالتقاط التفاعل المادي بين الأجهزة النظيرة. ولهذا السبب، يمكنك تأكيد مشاكل الاتصال أو تجاهلها.

الأدوات المفيدة

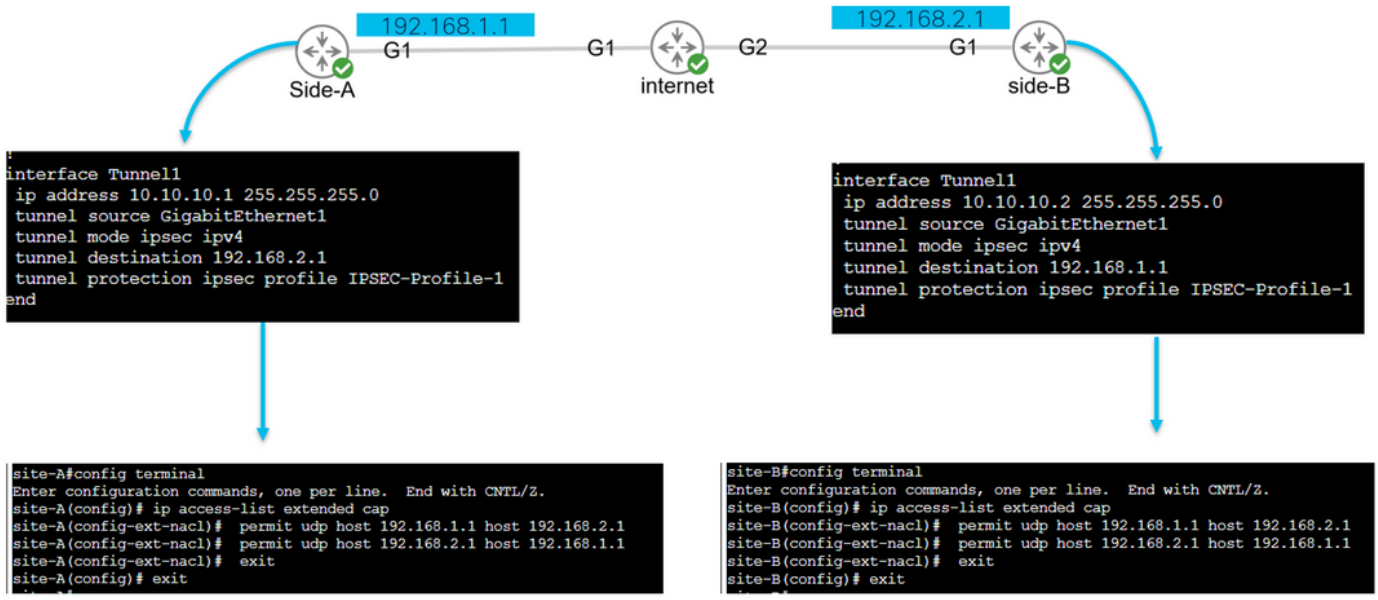
هناك أدوات مفيدة تساعدك على تكوين الالتقاط، واستخراج المخرجات، وتحليلها أكثر. بعضها:

- Wireshark: هذا محلل حزم مفتوح المصدر معروف جيدا ومستخدم.
- على قبض الشاشة: تساعدك ميزة Cisco IOS XE على الموجهات على جمع الالتقاط وتوفير مخرج ضوئي لما يبدو عليه تدفق حركة المرور، والبروتوكول الذي يتم تجميعه، والطوابع الزمنية الخاصة به.

كيفية تكوين الالتقاط على موجه IOS XE

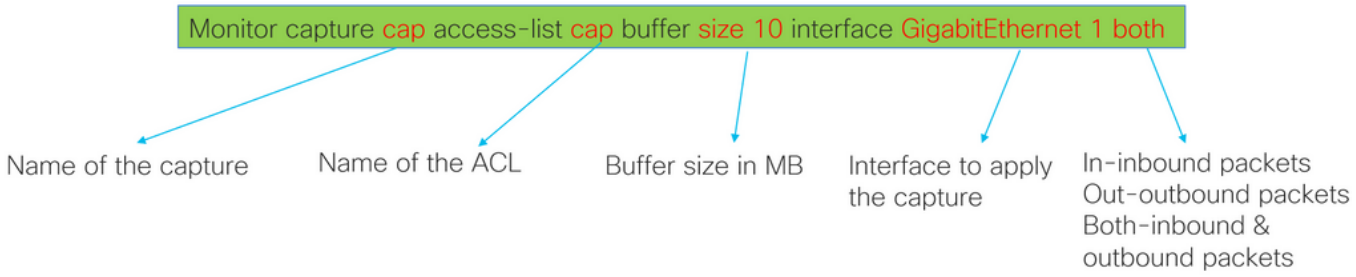
يستخدم الالتقاط قائمة الوصول الموسعة (ACL) التي تحدد نوع حركة المرور التي سيتم تجميعها، وعناوين المصدر والوجهة الخاصة بنظراء VPN أو مقاطع حركة المرور المفيدة. يستعمل نفق ال UDP ميناء 500 وميناء 4500 إن NAT-T يكون مكنت على المسار. بمجرد اكتمال التفاوض وإنشاء النفق، تستخدم حركة المرور المفيدة بروتوكول IP 50 (ESP) أو UDP 4500 إذا تم تمكين NAT-T.

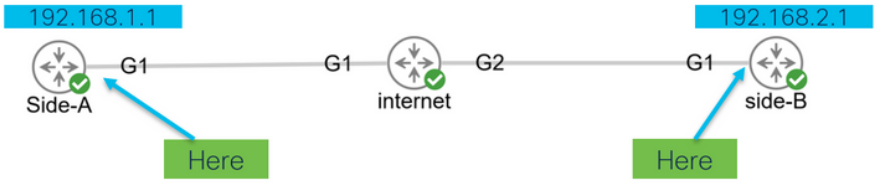
من أجل أستكشاف أخطاء المشاكل المتعلقة بلوحة التحكم وإصلاحها، يجب إستخدام عناوين IP الخاصة بنظراء VPN لالتقاط كيفية التفاوض حول النفق.




```
config terminal
ip access-list extended <ACL name>
permit udp host <local address> host <peer address>
permit udp host <peer address> host <source address>
exit
exit
```

يتم إستخدام قائمة التحكم في الوصول (ACL) التي تم تكوينها لتضييق حركة المرور التي تم الاستيلاء عليها، ويتم وضعها على الواجهة المستخدمة للتفاوض على النفق.






```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-A#
```

```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-B#
```

```
monitor capture <capture name> access-list <ACL name> buffer size <custom buffer size in MB> interface
```

بمجرد تكوين الالتقاط، يمكن التلاعب به لإيقافه، أو مسحه، أو إستخلاص حركة المرور التي تم تجميعها باستخدام الأوامر التالية:

- تحقق من معلومات الالتقاط العامة:show monitor capture
- بدء/إيقاف الالتقاط: بدء/إيقاف التقاط الشاشة
- تحقق من أن الالتقاط يجمع الحزم: show monitor capture cap buffer
- راجع إخراج موجز لحركة المرور: show monitor capture cap buffer موجز
- مسح الالتقاط: مسح حرف التقاط الشاشة
- إستخراج إخراج الالتقاط:
  - عملية تفريغ غطاء الشاشة
  - مدرب التقاط طرف تصدير bootflash:capture.pcap

تحليل إنشاء النفق باستخدام التقاط الحزم

وكما تمت الإشارة مسبقا، للتفاوض على نفق IPSec، يتم إرسال الحزم عبر UDP مع المنفذ 500 والمنفذ 4500 إذا تم تمكين NAT-T. مع عمليات الالتقاط، يمكن رؤية مزيد من المعلومات من تلك الحزم مثل المرحلة التي يتم التفاوض عليها (المرحلة 1 أو المرحلة 2)، أو دور كل جهاز (البادئ أو المستجيب)، أو قيم SPI التي تم إنشاؤها للتو.

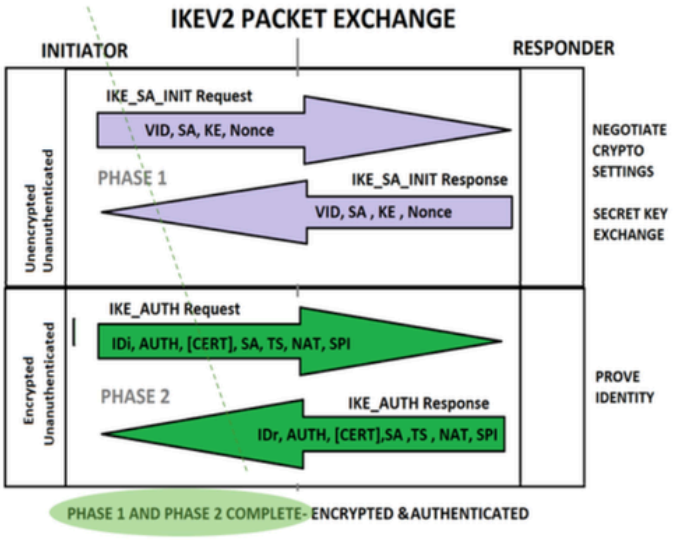
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

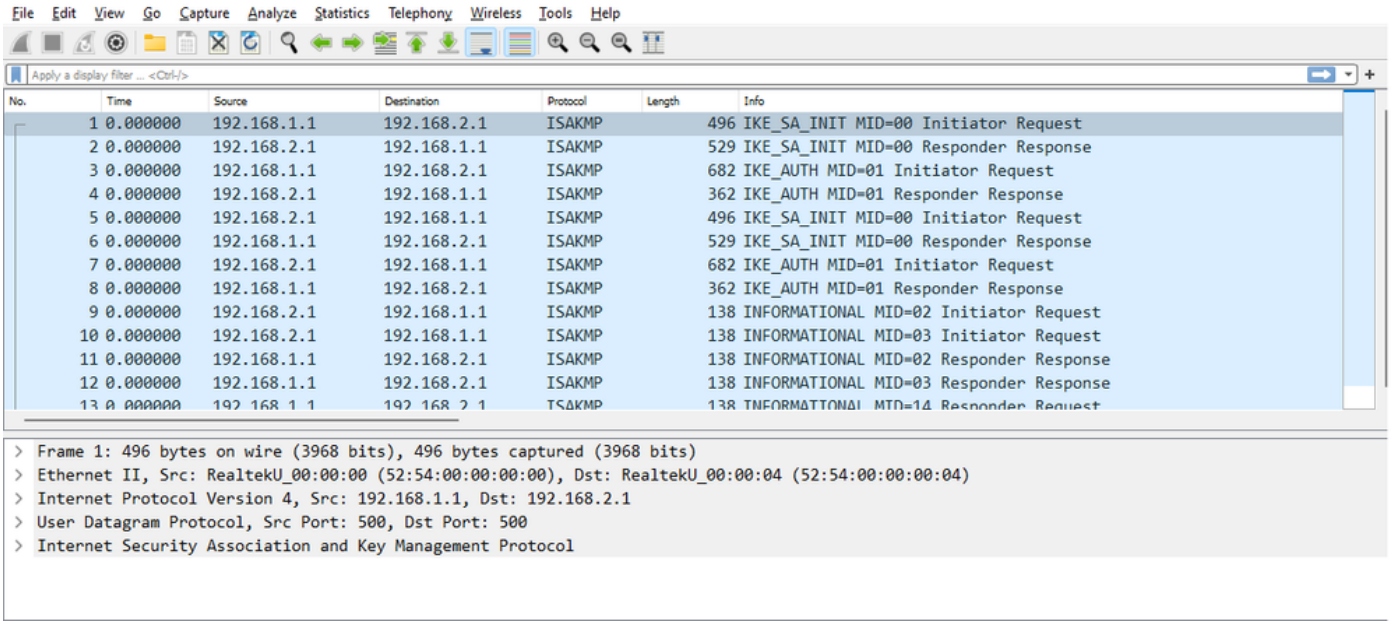
Phase 2 encrypted



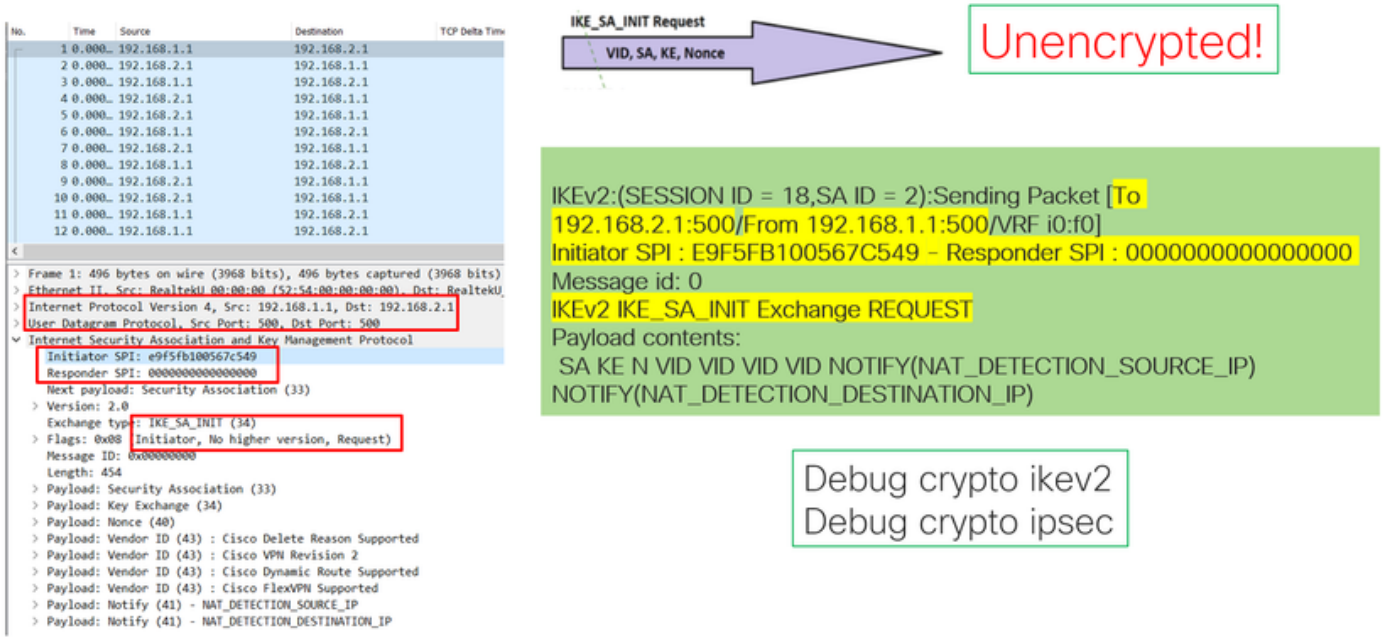
إظهار الإخراج الموجز من الالتقاط من الموجه، يظهر التفاعل بين الأقران، مع إرسال حزم UDP.

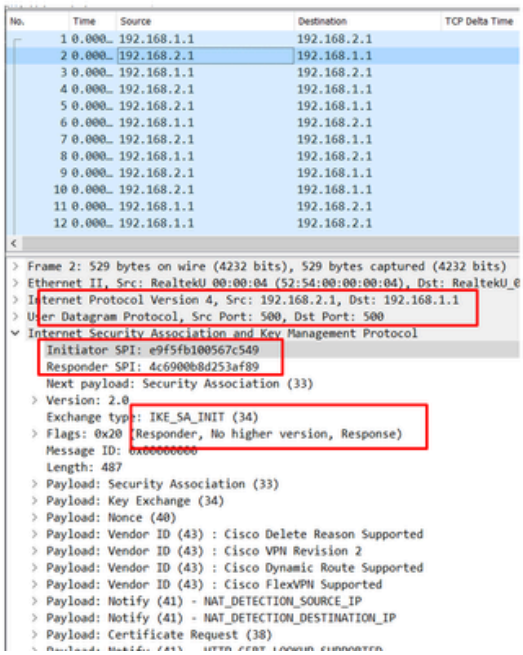
```
site-A#show monitor cap cap buffer brief
 ------------------------------------------------------------------------------
 #   size   timestamp     source               destination      dscp    protocol
 ------------------------------------------------------------------------------
   0  496     0.000000   192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   1  529     0.011992   192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   2  682     0.026991   192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   3  362     0.035993   192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   4  496     0.579016   192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   5  529     0.593023   192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   6  682     0.610020   192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   7  362     0.616017   192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   8  138     0.638019   192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   9  138     0.638019   192.168.2.1       ->  192.168.1.1      48 CS6  UDP
  10  138     0.641009   192.168.1.1       ->  192.168.2.1      48 CS6  UDP
  11  138     0.655016   192.168.1.1       ->  192.168.2.1      48 CS6  UDP
```

بعد إستخراج التفريغ وتصدير ملف PCAP من الموجه، فإن المزيد من المعلومات من الحزم تكون مرئية باستخدام wireshark.



على قسم بروتوكول الإنترنت من حزمة تبادل IKE_SA_INIT الأولى التي يتم إرسالها، يتم تحديد موقع عناوين المصدر والوجهة لحزمة UDP. في قسم بروتوكول مخطط بيانات المستخدم، تظهر المنافذ المستخدمة وقسم اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح إصدار البروتوكول، ونوع الرسالة التي يتم تبادلها، ودور الجهاز، بالإضافة إلى SPI الذي تم إنشاؤه. عند تجميع تصحيح أخطاء IKEv2، يتم عرض المعلومات نفسها داخل سجلات تصحيح الأخطاء.

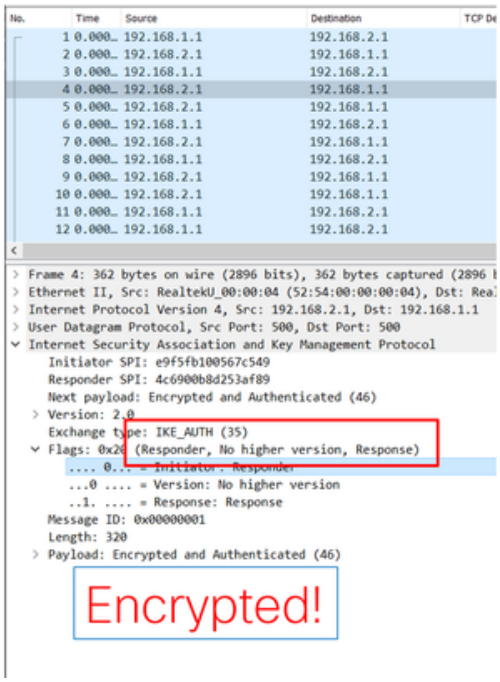




IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

Unencrypted!

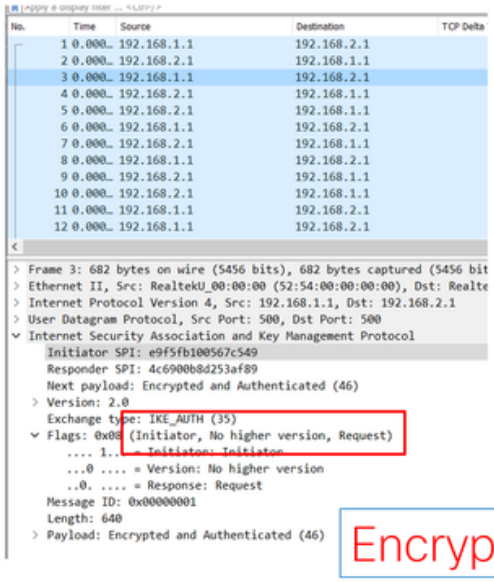
عند إجراء مفاوضات تبادل IKE_AUTH، يتم تشفير الحمولة ولكن، تكون بعض المعلومات حول التفاوض مرئية، مثل SPI الذي تم إنشاؤه مسبقا، ونوع الحركة التي يتم إجراؤها.



IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE

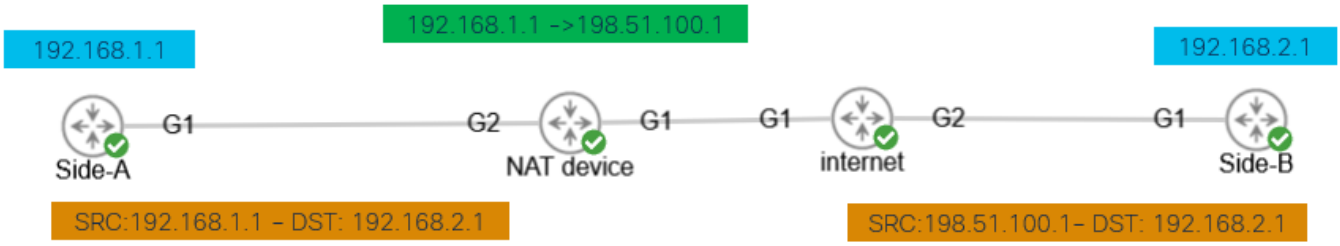
Encrypted!

بمجرد تلقي آخر حزمة تبادل IKE_AUTH، يتم إكمال تفاوض النفق.



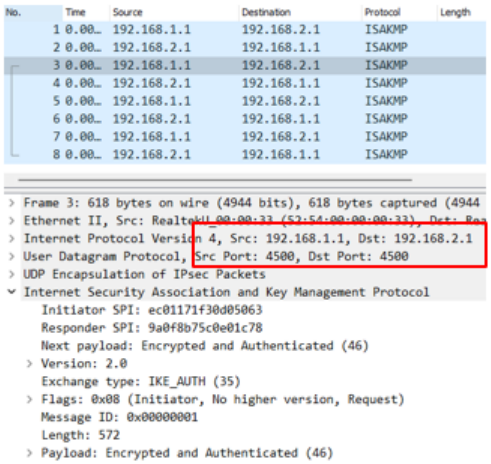
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

الحركة عندما يكون NAT بين



nat-transversal هو ميزة أخرى يمكن رؤيتها عندما يتم تفاوض النفق. إذا كان جهاز متوسط يحمل عنوانا أو كل عنوانين يستخدمان النفق، فإن الأجهزة تغير منفذ UDP من 500 إلى 4500 عند التفاوض على المرحلة 2 (IKE_AUTH Exchange).

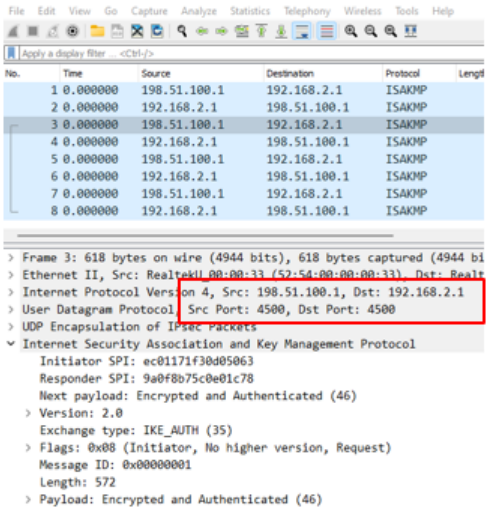
أسر مأخوذ على الجانب أ:



IKEv2:(SESSION ID = 10,SA ID = 1):Received Packet [From 192.168.1.1:4500/To 192.168.2.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST

IKEv2:(SESSION ID = 10,SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SESSION ID = 10,SA ID = 1):Checking NAT discovery
IKEv2:(SESSION ID = 10,SA ID = 1):NAT INSIDE found
IKEv2:(SESSION ID = 10,SA ID = 1):NAT detected float to init port 4500, resp port 4500

أسر مأخوذ على الجانب ب:



IKEv2:(SESSION ID = 11,SA ID = 1):Sending Packet [To 192.168.2.1:4500/From 198.51.100.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:

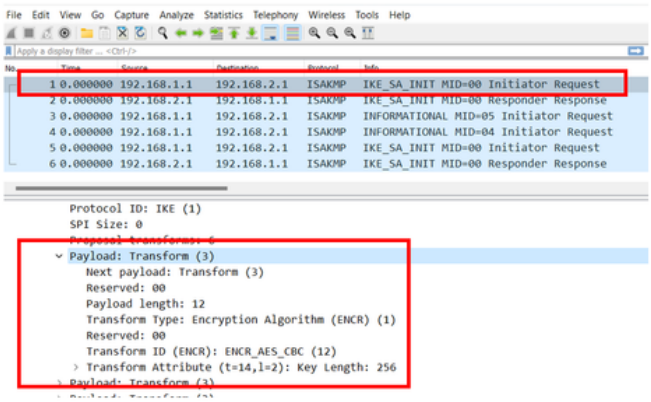
مشاكل مستوى التحكم الشائعة

قد تكون هناك عوامل محلية أو خارجية تؤثر على تفاوض النفق ويمكن تحديدها مع التقاط أيضا. السيناريوهات التالية هي الأكثر شيوعا.

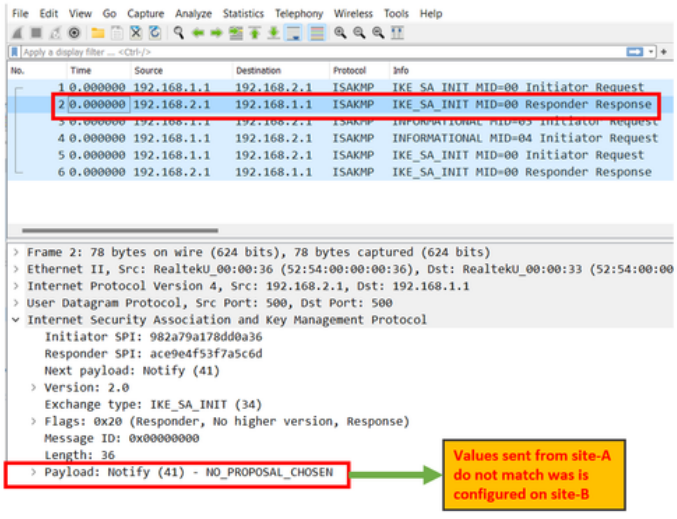
التكوين غير متطابق

يمكن حل هذا السيناريو من خلال النظر في تكوين كل جهاز في المرحلة 1 والمرحلة 2. ومع ذلك، قد تكون هناك سيناريوهات لا تتوفر فيها إمكانية الوصول إلى الطرف البعيد. على سبيل المساعدة عن طريق تحديد الجهاز الذي يرسل NO_PROPOSAL_CHOSEN داخل الحزم إما في المرحلة 1 أو 2. تشير هذه الاستجابة إلى شيء ما يمكن أن يكون خاطئا في التكوين وأي مرحلة يلزم تعديلها.

Side-A



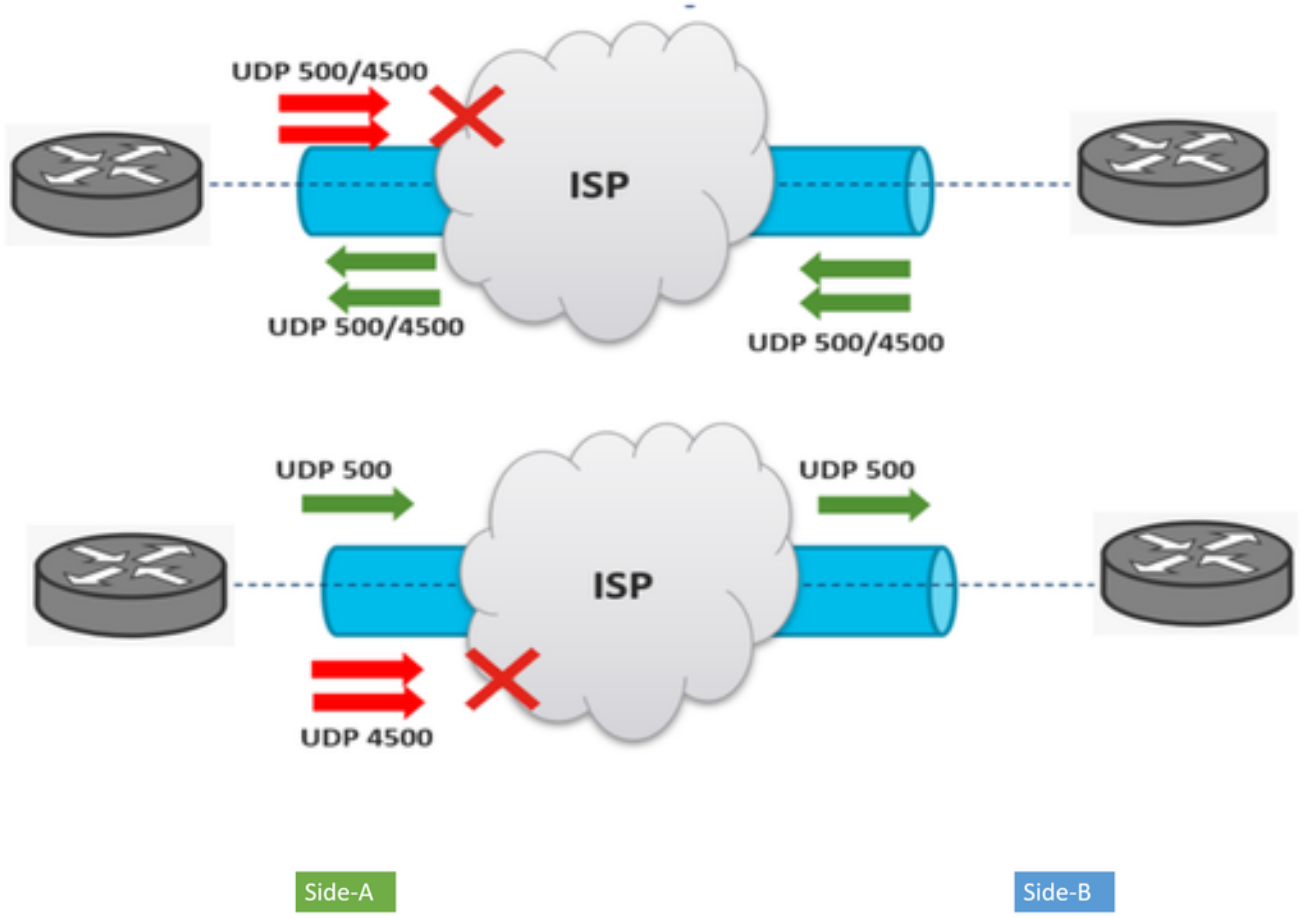
Side-B

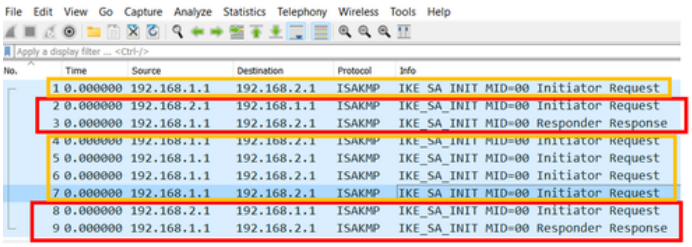


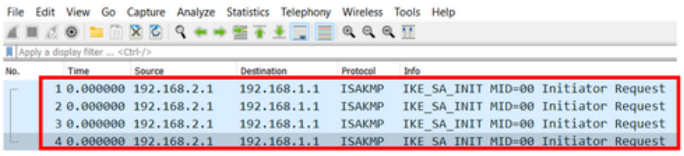
عمليات إعادة الإرسال

يمكن أن يفشل تفاوض نفق IPSec بسبب حزم التفاوض التي يتم إسقاطها على المسار بين الأجهزة الطرفية. يمكن أن تكون الحزم التي تم إسقاطها المرحلة 1 أو المرحلة 2. عندما يكون هذا هو الحالة، يرسل الجهاز الذي يتوقع حزمة إستجابة الحزمة الأخيرة، وإذا لم يكن هناك إستجابة بعد 5 محاولات، يتم أختتام النفق وإعادة تشغيله من البداية.

يلتقط على كل جانب من النفق المساعدة بتحديد ما يمكن ان يعيق حركة المرور وفي أي إتجاه تتأثر.







A device or service in between is blocking UDP packets that come from side-A

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).