استيعاب بروتوكول IPsec IKEv1

المحتويات

المقدمة

يصف هذا المستند عملية بروتوكول تبادل مفاتيح الإنترنت (IKEv1) لإنشاء شبكة خاصة ظاهرية (VPN).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بمفاهيم الأمان الأساسية:

- المصادقة
- السرية
- نزاهة
- IPsec

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

تعتبر عملية بروتوكول تبادل مفتاح الإنترنت (IKEv1) لإنشاء شبكة خاصة ظاهرية (VPN) مهمة لفهم تبادل الحزم من أجل أستكشاف أخطاء أي نوع من مشاكل أمان بروتوكول الإنترنت (IPsec) مع IKEv1 وإصلاحها بشكل أبسط.

IPsec

IPsec هي مجموعة من البروتوكولات التي توفر الأمان لاتصالات الإنترنت في طبقة IP. IPsec هو توفير شبكة خاصة ظاهرية (VPN)، إما بين أكثر الاستخدامات الحالية شيوعا لـ IPsec موقعين (من العبارة إلى البوابة) أو بين مستخدم بعيد وشبكة مؤسسة (من المضيف إلى البوابة).

بروتوكول IKE

يستخدم IPsec بروتوكول IKE للتفاوض حول أنفاق شبكة الاتصال الخاصة الظاهرية (VPN) للوصول الآمن من موقع إلى موقع أو من بعد وإنشائها. ويسمى بروتوكول IKE أيضا بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) (في Cisco فقط).

هناك إصداران من IKE:

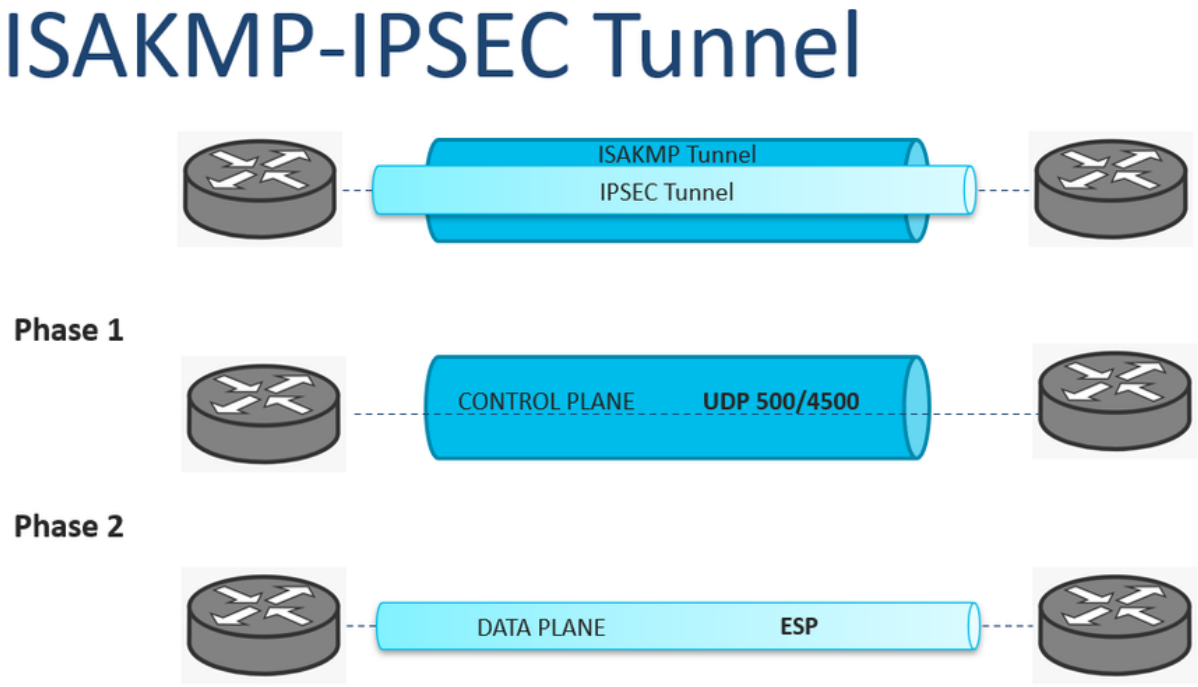
- IKEv1: معرف في RFC 2409، تبادل مفتاح الإنترنت
- IKE الإصدار 2 (IKEv2): معرف في RFC 4306، بروتوكول تبادل مفتاح الإنترنت (IKEv2)

مراحل IKE

يفصل بروتوكول ISAKMP التفاوض إلى مرحلتين:

- المرحلة 1: يعمل نظاراء ISAKMP على إنشاء نفق آمن ومصادق، يحمي رسائل تفاوض ISAKMP. يعرف هذا النفق باسم ISAKMP SA. هناك وضعان محددان من قبل ISAKMP: الوضع الرئيسي (MM) الوضع القوي.
- المرحلة الثانية: يقوم بالتفاوض بشأن المواد الأساسية والخوارزميات الخاصة بتشفير البيانات المراد نقلها عبر نفق IPsec. تسمى هذه المرحلة الوضع السريع.

لتجسيد كافة المفاهيم المجردة، فإن نفق المرحلة الأولى هو النفق الرئيسي والمرحلة 2 هي نفق فرعي. توضح هذه الصورة المرحلتين كأنفاق:



ملاحظة: يحمي نفق المرحلة 1 (ISAKMP) حركة مرور بيانات VPN الخاصة بلوحة التحكم بين العبارتين. يمكن أن تكون حركة مرور مستوى التحكم حزم تفاوض، حزم معلومات، DPD، keepalives، rekey، وما إلى ذلك. يستخدم تفاوض ISAKMP منافذ UDP 500 و 4500 لإنشاء قناة آمنة.

ملاحظة: يحمي نفق المرحلة 2 (IPsec) حركة مرور مستوى البيانات التي تمر عبر الشبكة الخاصة الظاهرية (VPN) بين العبارتين. يتم تكوين الخوارزميات المستخدمة لحماية البيانات في المرحلة الثانية وهي مستقلة عن تلك المحددة في المرحلة الأولى.
البروتوكول المستخدم لتضمين هذه الحزم وتشفيرها هو حمولة أمان التضمين (ESP).

أوضاع IKE (المرحلة 1)

الوضع الرئيسي

تبدأ جلسة عمل IKE عندما يرسل البادئ اقتراحا أو اقتراحا إلى المستجيب. ينشئ التبادل

الألوان بين العقد سياسة الأمان الأساسية؛ ويقترح البادئ خوارزميات التشفير والمصادقة التي سيتم إستخدامها. ويختار المستجيب الاقتراح المناسب (اقتراحات) ويرسله إلى البادئ. يقوم التبادل التالي بتمرير المفاتيح العامة Diffie-Hellman والبيانات الأخرى. يتم تشفير جميع المفاوضات الإضافية داخل IKE SA. يصادق التبادل الثالث جلسة ISAKMP. بمجرد إنشاء IKE SA، تبدأ مفاوضات IPSec (الوضع السريع).

وضع عدواني

يعمل الوضع العدواني على تقييد تفاوض IKE SA في ثلاث حزم، مع تمرير جميع البيانات المطلوبة لـ SA من قبل البادئ. يرسل المستجيب العرض، والمواد الأساسية، والمعرف، ويصادق الجلسة في الحزمة التالية. يرد البادئ على الجلسة ويصدقها. التفاوض أسرع، ويمر معرف البادئ والمستجيب في المسح.

وضع IPsec (المرحلة 2)

الوضع السريع

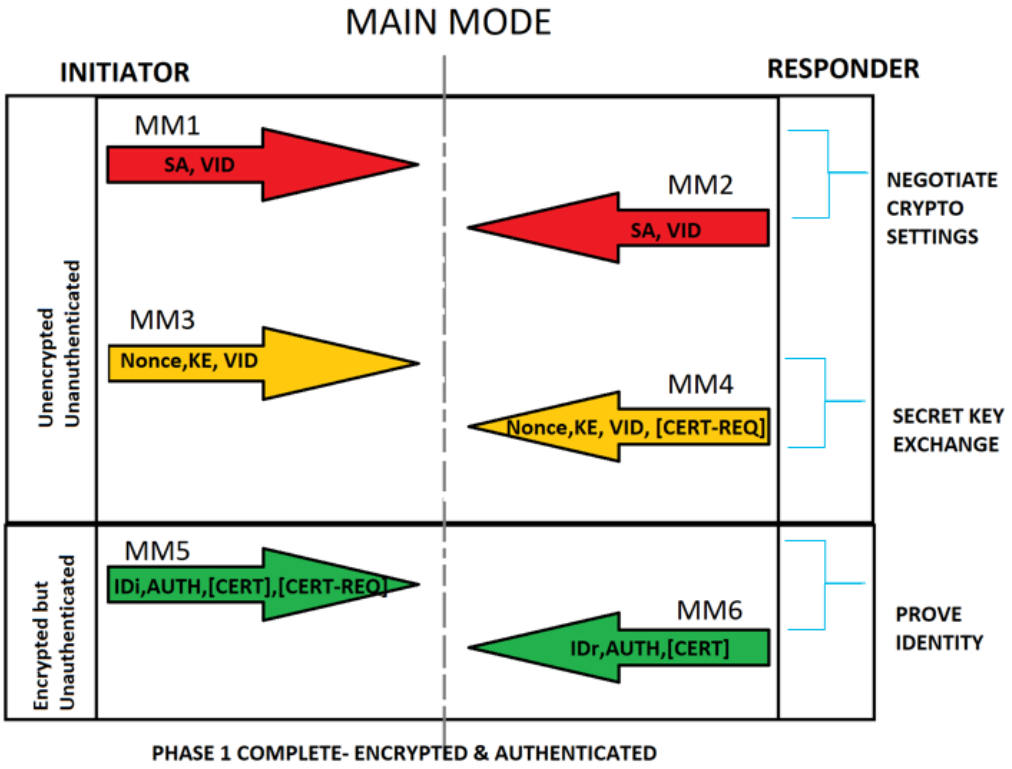
تفاوض IPSec، أو الوضع السريع، مماثل لمفاوضات IKE ذات الوضع العدواني، باستثناء التفاوض، يجب حمايته داخل IKE SA. يقوم الوضع السريع بالتفاوض مع SA لتشفير البيانات وإدارة تبادل المفاتيح لـ IPSec SA هذا.

مسرد إيك

- اقتران الأمان (SA) وهو إنشاء سمات أمان مشتركة بين كيانين على الشبكة لدعم الاتصال الآمن. تتضمن حالة الوصول (SA) سمات مثل خوارزمية التشفير والوضع ومفتاح تشفير حركة مرور البيانات والمعلومات الخاصة ببيانات الشبكة التي سيتم تمريرها عبر الاتصال.
- تتم معالجة معرفات المورد (VID) لتحديد ما إذا كان النظير يدعم ميزة اكتشاف النظير الميت (NAT-Traversal) والتجزئة وما إلى ذلك.
- nonce: رقم تم إنشاؤه عشوائيا يرسله البادئ. يتم تجزئة هذه الرنانة مع العناصر الأخرى مع المفاتيح المتفق عليه المستخدم ويتم إرسالها مرة أخرى. يقوم البادئ بالتحقق من ملف تعريف الارتباط والشخص ويرفض أي رسائل ليس لها الحق مرة واحدة. وهذا يساعد على منع إعادة التشغيل نظرا لأنه لا يمكن لأي طرف ثالث التنبؤ بماهية المشاهدة التي تنشأ عشوائيا.
- معلومات تبادل المفاتيح (KE) لعملية تبادل المفاتيح الآمنة Diffie-Hellman (DH).
- يتم إستخدام معيئ الهوية/المستجيب (IDi/IDr) لإرسال معلومات المصادقة إلى النظير. يتم إرسال هذه المعلومات تحت حماية السر المشترك المشترك المشترك.
- تبادل مفاتيح Diffie-Hellman (DH) وهو طريقة لتبادل خوارزميات التشفير بأمان عبر قناة عامة.
- يمكن اشتقاق مفاتيح IPSec المشترك مع DH المستخدم مرة أخرى لضمان سرية إعادة التوجيه الكاملة (PFS) أو تبادل DH الأصلي الذي تم تحديثه إلى السر المشترك المشتق سابقا.

تبادل حزم الوضع الرئيسي

تحتوي كل حزمة من حزم ISAKMP على معلومات الحمولة لإنشاء النفق. يشرح مسرد IKE إختصارات IKE كجزء من محتوى الحمولة لتبادل الحزم على الوضع الرئيسي كما هو موضح في هذه الصورة.

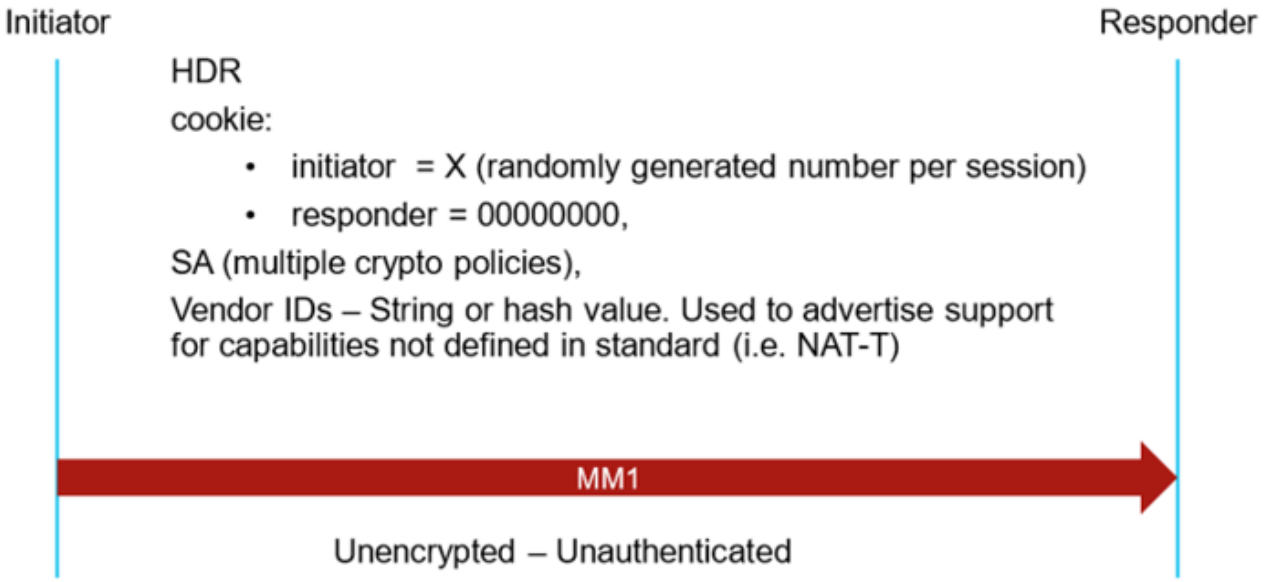


الوضع الرئيسي 1 (MM1)

لتعييني شروط مفاوضات ISAKMP، قم بإنشاء سياسة ISAKMP، والتي تتضمن:

- أسلوب مصادقة، لضمان هوية الأقران.
- أسلوب تشفير لحماية البيانات وضمان الخصوصية.
- أسلوب رموز مصادقة الرسائل المجمعة (HMAC) لضمان هوية المرسل، ولضمان عدم تعديل الرسالة أثناء النقل.
- مجموعة Diffie-Hellman لتحديد قوة خوارزمية تحديد مفتاح التشفير. يستخدم جهاز الأمان هذه الخوارزمية لاستخلاص التشفير ومفاتيح التجزئة.
- حد أقصى للوقت الذي يستخدم فيه جهاز الأمان مفتاح تشفير قبل إستبداله.

يتم إرسال الحزمة الأولى بواسطة البادئ لمفاوضات IKE كما هو موضح في الصورة:



ملاحظة: الوضع الرئيسي 1 وه الحزمة الأولى من تفاوض IKE. لذلك، يتم تعيين SPI للبادئ على قيمة عشوائية بينما يتم تعيين SPI للمسؤول على 0. في الحزمة الثانية (MM2) يجب الرد على SPI الخاص بالمستجيب بقيمة جديدة ويحتفظ التفاوض بالكامل بنفس قيم SPIs.

إذا تم التقاط MM1 وتم إستخدام محلل بروتوكول شبكة Wireshark، فإن قيمة SPI تكون داخل اقتران أمان الإنترنت ومحتوى بروتوكول إدارة المفاتيح كما هو موضح في الصورة:

```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 170.49.116.200, Dst: 209.134.162.150
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
```

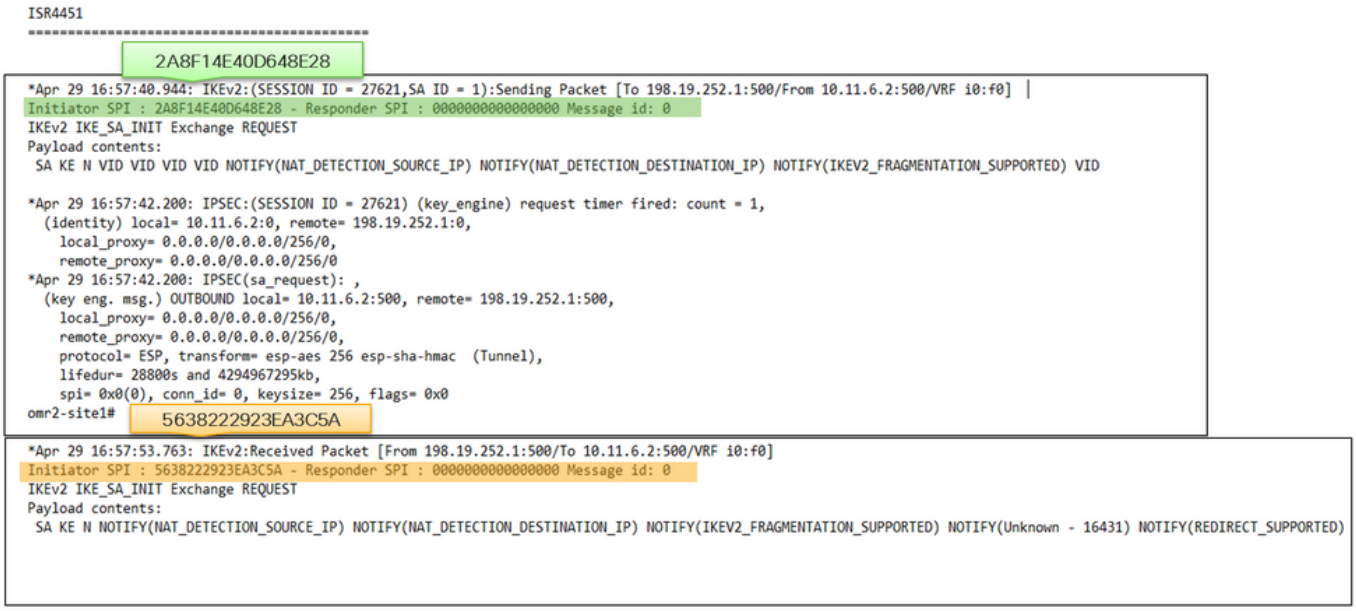
ملاحظة: في الحالة، يتم فقد حزمة MM1 في المسار أو ال يوجد رد على MM2، يحتفظ تفاوض IKE بعمليات إعادة إرسال MM1 حتى يتم الوصول إلى الحد الأقصى لعدد عمليات إعادة الإرسال. عند هذه النقطة، يحتفظ البادئ بنفس SPI حتى يتم تشغيل التفاوض التالي مرة أخرى.

تلميح: يكون تعريف SPIs للبادئ والمستجيب مفيدا جدا لتحديد مفاوضات متعددة ل VPN نفسه وتضييق بعض مشاكل التفاوض.

تحديد مفاوضاتين متزامنتين

على الأنظمة الأساسية Cisco IOS® XE، يمكن تصفية تصحيح الأخطاء لكل نفق باستخدام شرط لعنوان IP البعيد الذي تم تكوينه. ومع ذلك، يتم عرض المفاوضات المتزامنة على السجلات، ولا توجد طريقة لتصفيتها. المطلوب هو القيام بذلك يدويا. وكما ذكر سابقا، يحتفظ التفاوض بأكمله بنفس قيم SPI للبادئ والمستجيب. في حالة

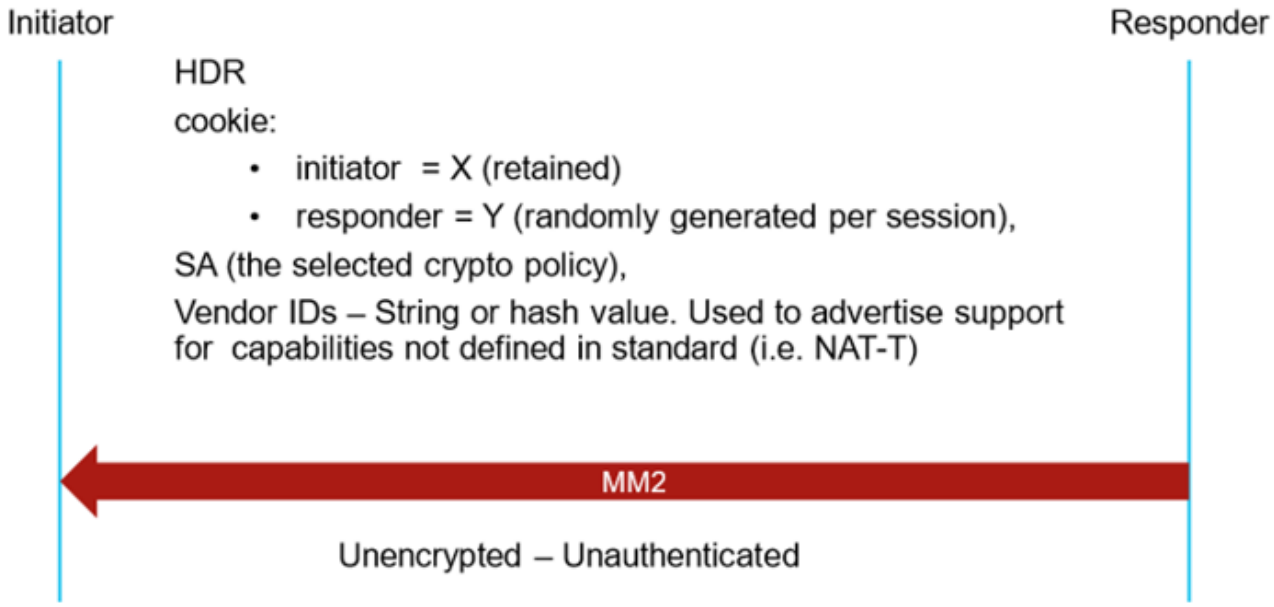
إستلام حزمة من نفس عنوان IP للنظير ولكن لا تتطابق SPI مع القيمة السابقة التي تم تعقبها قبل أن يصل التفاوض إلى الحد الأقصى لعدد إعادة الإرسال، فإنها مفاوضات أخرى لنفس النظير كما هو موضح في الصورة:



ملاحظة: يوضح المثال التفاوض المتزامن للحزمة الأولى في التفاوض (MM1). ومع ذلك، يمكن أن يحدث ذلك عند أي نقطة تفاوض. يجب أن تتضمن جميع الحزم التالية قيمة مختلفة عن 0 على SPI الخاص بالمستجيب.

الوضع الرئيسي 2 (MM2)

في حزمة "الوضع الرئيسي 2"، يرسل المستجيب النهج المحدد للمقترحات المتطابقة، ويتم تعيين SPI الخاص بالمستجيب إلى قيمة عشوائية. يحافظ التفاوض بالكامل على قيم SPIs نفسها. يرد MM2 على MM1 ويتم تعيين المستجيب SPI على قيمة مختلفة من 0 كما هو موضح في الصورة:



إذا تم التقاط MM2 واستخدام محلل بروتوكول شبكة Wireshark، فإن قيم SPI الخاصة بالمنشئ والمستجيب تكون داخل محتوى بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت كما هو موضح في الصورة:

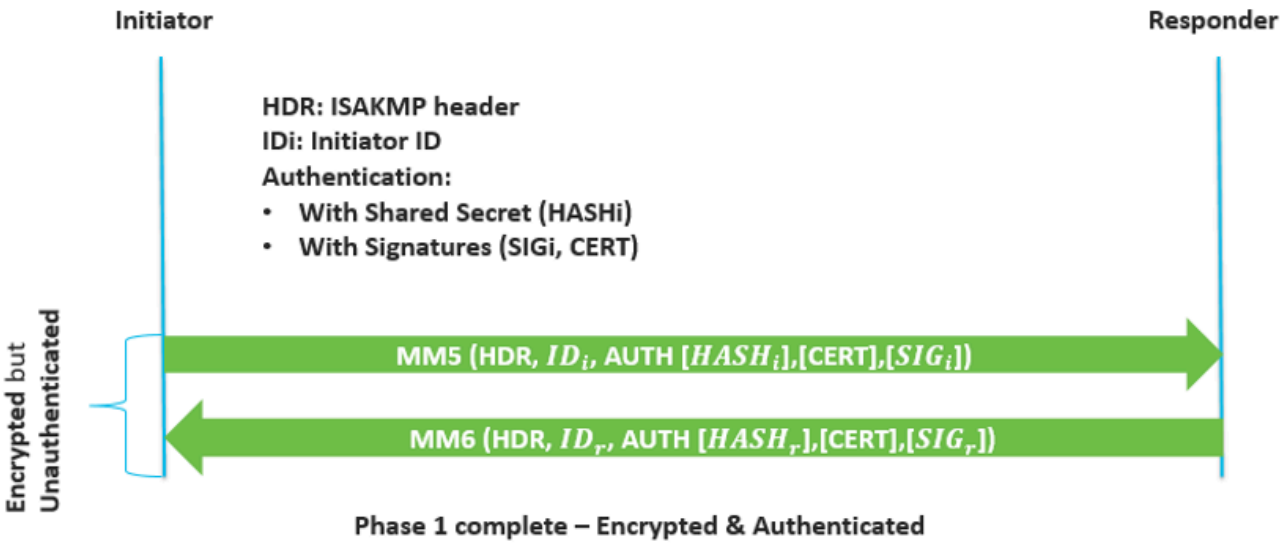
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 2bc06438c94e88dc
    Next payload: Security Association (33)
```

الوضع الرئيسي 3 و 4 (MM3-MM4)

لا تزال حزم MM3 و MM4 غير مشفرة وغير مصدق عليها، ويتم تبادل المفاتيح السرية. يتم عرض MM3 و MM4 في الصورة:

الوضع الرئيسي 5 و 6 (MM5-MM6)

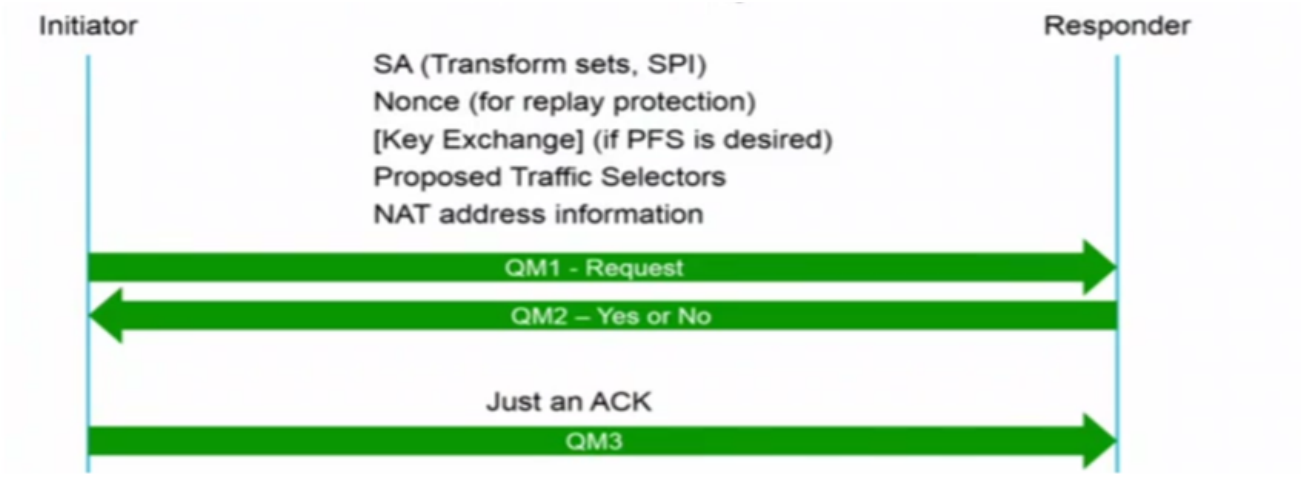
حزم MM5 و MM6 مشفرة بالفعل ولكنها لا تزال غير مصدق عليها. على هذه الحزم، تحدث المصادقة كما هو موضح في الصورة:



الوضع السريع (QM1 و QM2 و QM3)

يحدث الوضع السريع بعد قيام وحدة التحكم في الإنترنت (IKE) بإنشاء النفق الآمن في المرحلة الأولى. يقوم الوضع السريع بالتفاوض على سياسة IPSec المشتركة، لخوارزميات أمان IPSec ويدير تبادل المفاتيح لإنشاء IPSec SA. يتم إستخدام وسائل الاتصال لإنشاء مواد مفتاح سرية مشتركة جديدة ومنع هجمات إعادة التشغيل من شبكات SA المزيفة التي تم إنشاؤها.

يتم تبادل ثلاث حزم في هذه المرحلة كما هو موضح في الصورة:



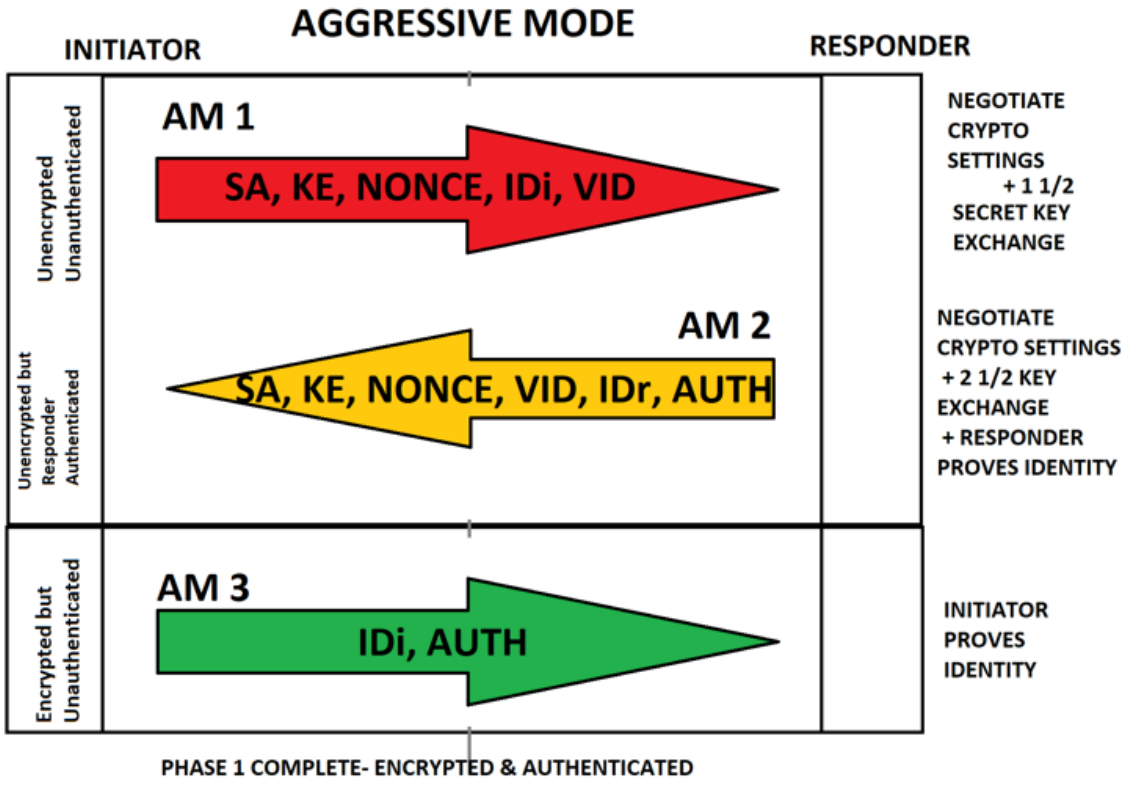
تبادل حزم الوضع الفعال

يعمل الوضع العدواني على تقييد تفاوض IKE SA في ثلاث حزم، مع تمرير جميع البيانات المطلوبة ل SA بواسطة البادئ.

- يرسل المستجيب العرض، والمواد الأساسية، والمعرف، ويصادق الجلسة في الحزمة التالية.
- يرد البادئ على الجلسة ويصدقها.

- التفاوض أسرع، ويمر معرف البادئ والمستجيب في المسح.

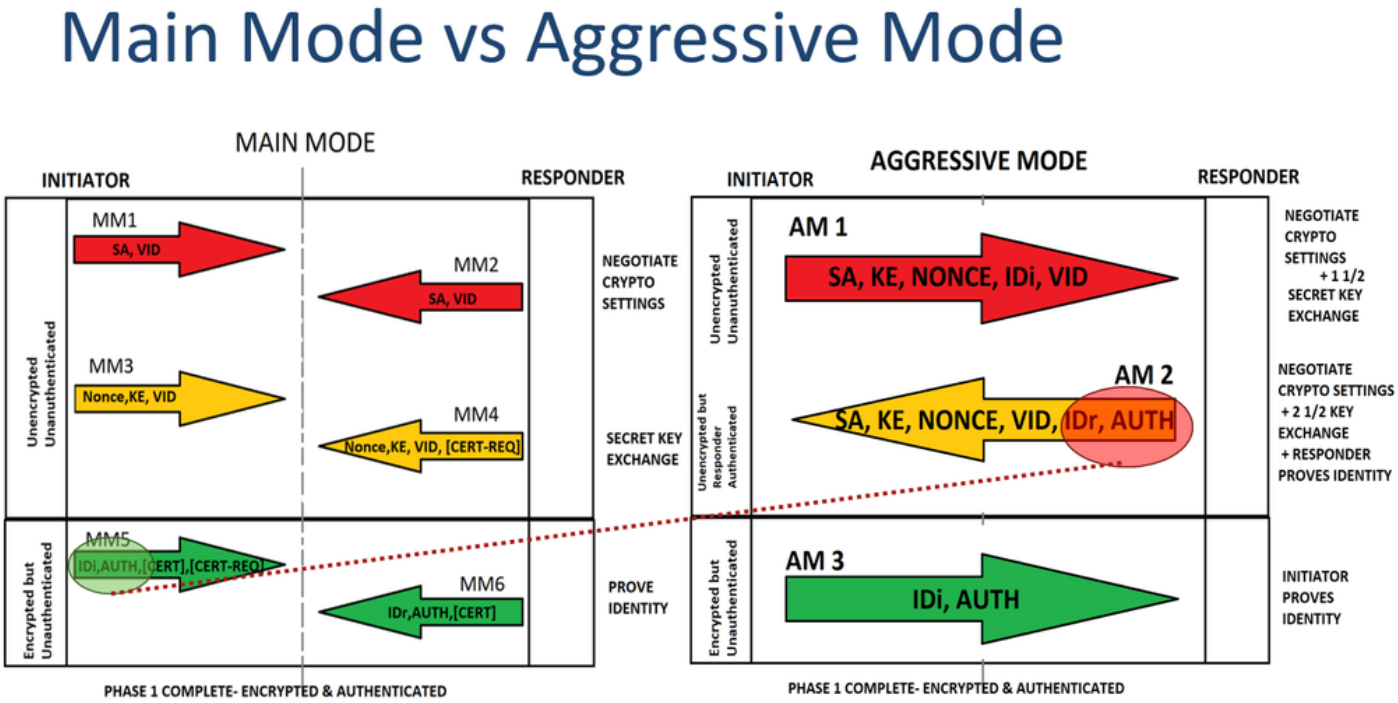
تظهر الصورة محتوى الحمولة للحزم الثلاث التي يتم تبادلها على الوضع القوي:



الوضع الرئيسي مقابل الوضع القوي

مقارنة مع "الوضع الرئيسي"، فإن "الوضع المتميز" يمكن توضيحه في ثلاث حزم:

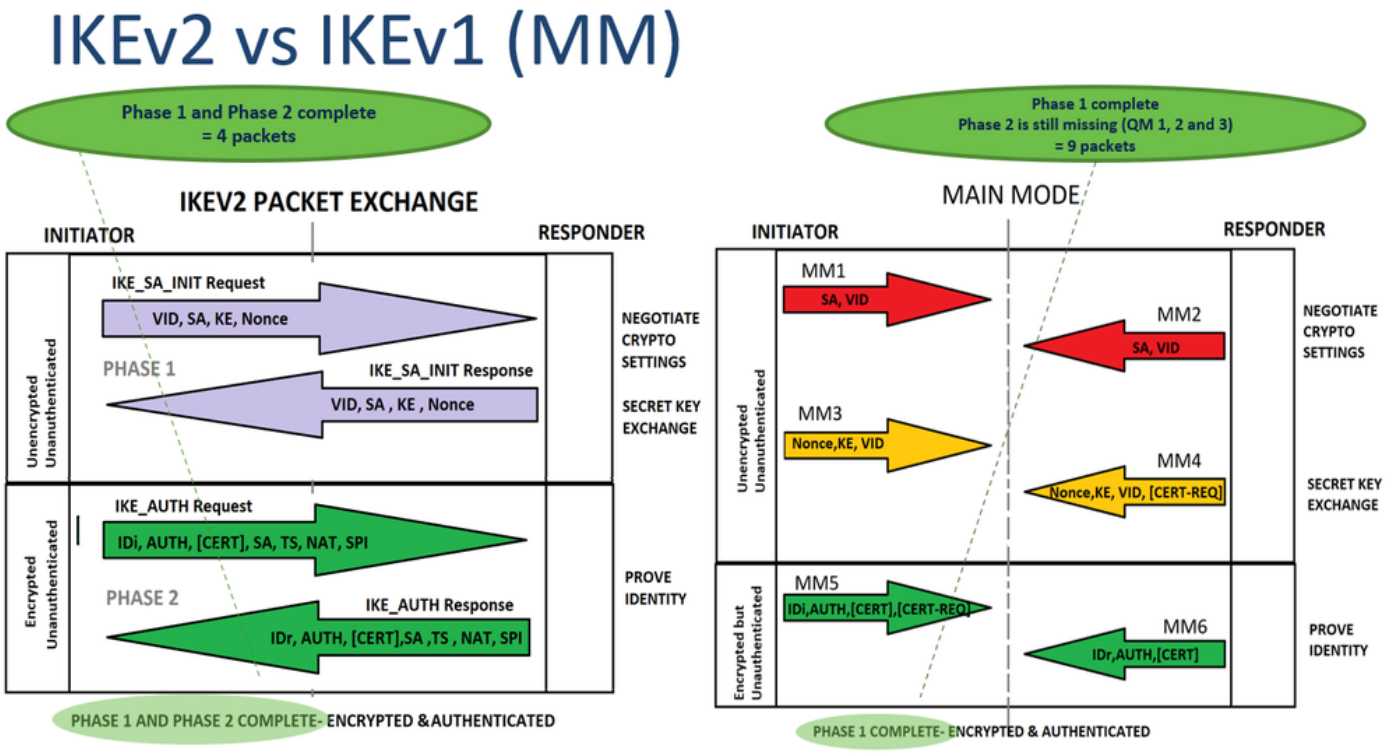
- AM 1 ممتصة MM1 و MM3.
- AM 2 يمتص MM2، MM4، وجزء من MM6. هذا هو المكان الذي يأتي منه التعرض "للوضع العدائي". يقوم AM 2 بتكوين المعرف والمصادقة دون تشفير. بخلاف الوضع الرئيسي، يتم تشفير هذه المعلومات.
- يوفر AM 3 المعرف والمصادقة. هذه القيم مشفرة.



تبادل حزم IKEv2 مقابل IKEv1

في مفاوضات IKEv2، يتم تبادل رسائل أقل لإنشاء نفق. يستخدم IKEv2 أربع رسائل؛ يستخدم IKEv1 إما ست رسائل (في الوضع الرئيسي) أو ثلاث رسائل (في الوضع العدواني).

يتم تعريف أنواع رسائل IKEv2 على أنها أزواج الطلب والاستجابة. تظهر الصورة مقارنة الحزم ومحتوى الحمولة لـ IKEv2 مقابل IKEv1:



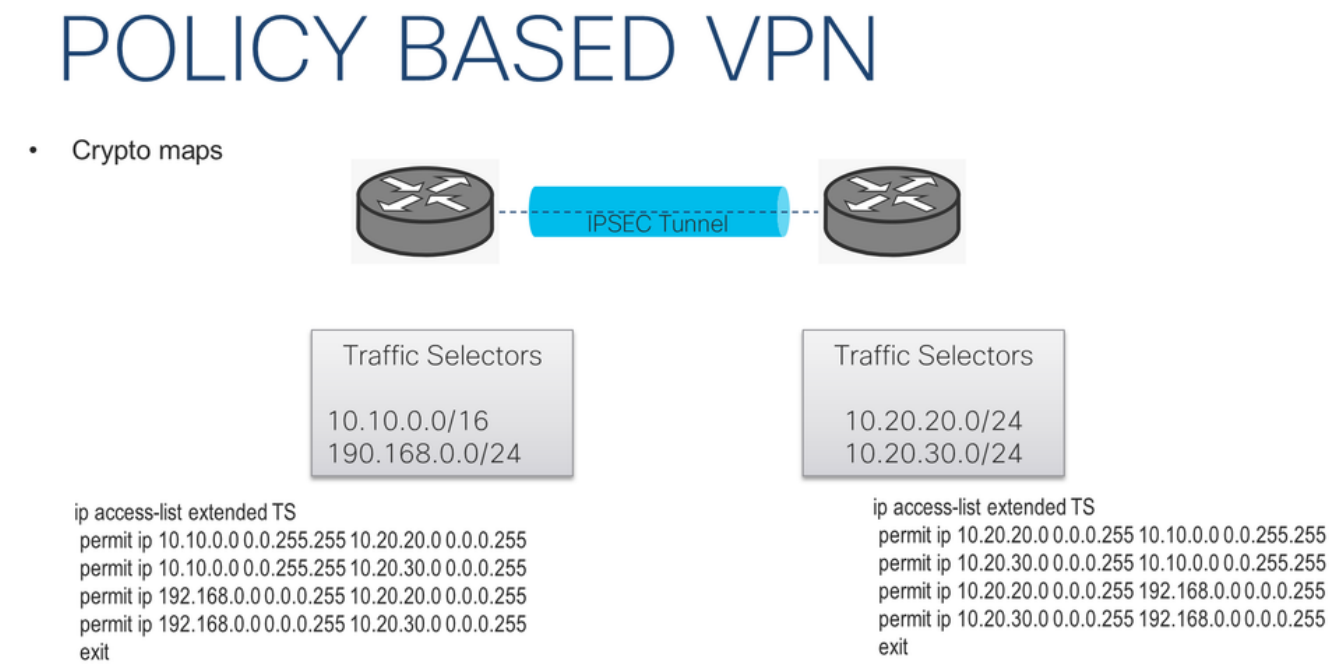
ملاحظة: لا يتعمق هذا المستند في تبادل حزم IKEv2. لمزيد من المراجع، انتقل إلى تبادل حزم IKEv2 وتصحيح أخطاء مستوى البروتوكول.

مستند إلى السياسة مقابل مستند إلى المسار

شبكة VPN المستندة إلى السياسة

كما يشير الإسم، فإن VPN المستند إلى السياسة هو نفق VPN ل IPsec مع إجراء سياسة لحركة مرور النقل التي تلبي معايير مطابقة السياسة. في حالة أجهزة Cisco، يتم تكوين قائمة الوصول (ACL) وإرفاقها بخريطة تشفير لتحديد حركة مرور البيانات التي يجب إعادة توجيهها إلى شبكة VPN والتشفير.

محددات حركة المرور هي الشبكات الفرعية أو الأجهزة المضيفة المحددة في النهج كما هو موضح في الصورة:

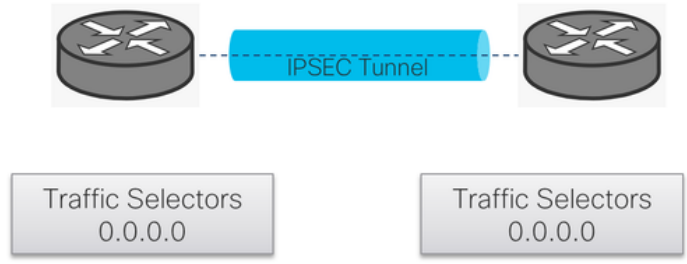


شبكة VPN المستندة إلى المسار

لا توجد حاجة إلى نهج. تتم إعادة توجيه حركة المرور نحو الأنفاق باستخدام المسارات، وهي تدعم التوجيه الديناميكي عبر واجهة النفق. محدد حركة مرور البيانات (يشفر حركة مرور البيانات من خلال VPN) من 0.0.0.0 إلى 0.0.0.0 بشكل افتراضي كما هو موضح في الصورة:

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.




```
interface: Tunnel100001
   Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

  protected vrf:  1
  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)
```

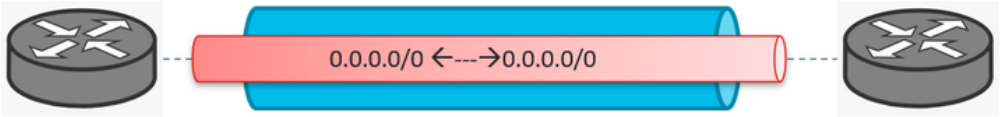
ملاحظة: نظرا لأن محددات حركة المرور هي 0.0.0.0، يتم تضمين أي مضيف أو شبكة فرعية داخل. لذلك، خلقت فقط واحد SA. هناك إستثناء للنفق الديناميكي. لا يصف هذا وثيقة أنفاق ديناميكية.

يمكن تجسيد الشبكة الخاصة الظاهرية (VPN) المستندة إلى السياسة والتوجيه كما هو موضح في الصورة:

ISAKMP-IPSEC Tunnel

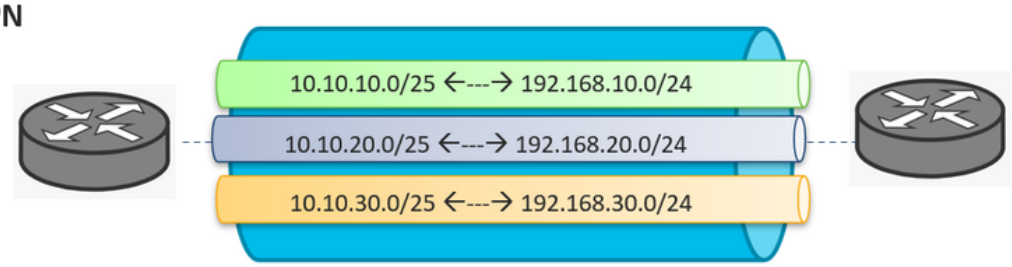
Route based VPN

*** Edges only support this.



Policy based VPN

- IOS - XE
- ASA
- FTD
- 3rd party devices



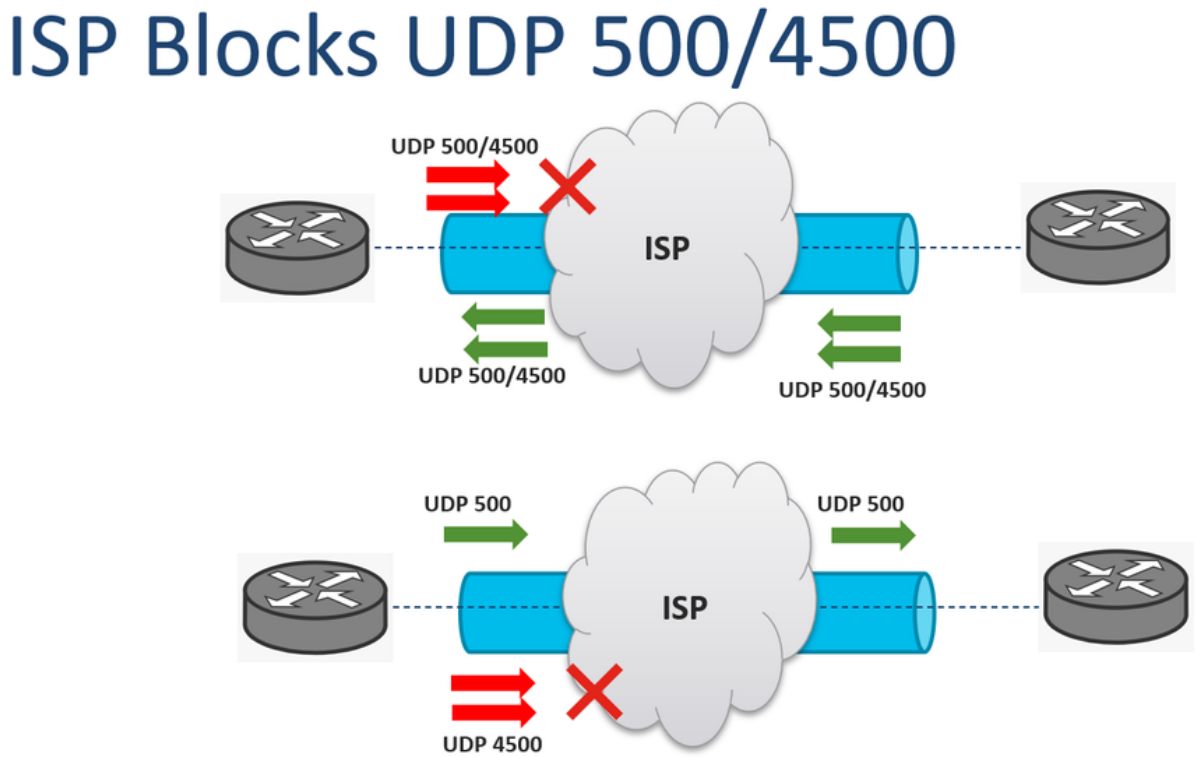
ملاحظة: بخلاف شبكة VPN المستندة إلى المسار التي تم إنشاء SA واحدة فقط، يمكن لشبكة VPN المستندة إلى السياسة إنشاء شبكات SA متعددة. مع تكوين قائمة التحكم في الوصول (ACL)، تقوم كل عبارة على قائمة التحكم في الوصول (إذا كانت مختلفة فيما بينها) بإنشاء نفق فرعي.

المشاكل المشتركة لحركة المرور التي تسللت من خلال VPN

كتل ISP UDP 500/4500

من الشائع جدا أن يقوم موفر خدمات الإنترنت (ISP) بحظر منافذ UDP 500/4500. بالنسبة لإنشاء نفق IPsec، يمكن إشراك اثنين من موفري خدمات الإنترنت (ISPs) المختلفين. يمكن لأحدهما حظر المنافذ، بينما يسمح له الآخر بذلك.

تعرض الصورة السيناريوهين حيث يمكن ل ISP حظر منافذ UDP 500/4500 في إتجاه واحد فقط:

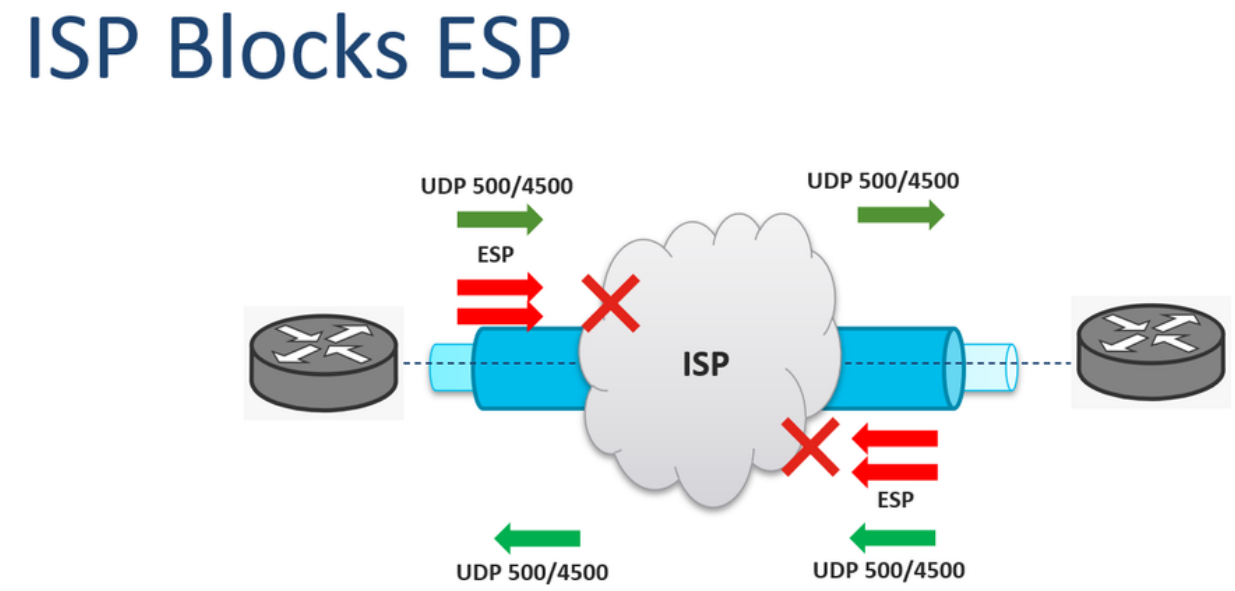


ملاحظة: يتم إستخدام المنفذ UDP 500 من قبل تبادل مفتاح الإنترنت (IKE) لإنشاء أنفاق الشبكة الخاصة الظاهرية (VPN) الآمنة. يتم إستخدام UDP 4500 عندما يكون NAT موجودا في نقطة نهاية VPN واحدة.

ملاحظة: عندما يقوم ISP بحظر UDP 500/4500، يتأثر إنشاء نفق IPsec والى يقوم.

يقوم ISP بحظر ESP

هناك مشكلة أخرى شائعة للغاية على أنفاق IPsec هي أن ISP يقوم بحظر حركة مرور ESP، ومع ذلك، فإنه يسمح بمنافذ UDP 500/4500. على سبيل المثال، يتم السماح بمنافذ UDP 500/4500 في طرق ثنائية الإتجاه. لذلك، يتم إنشاء النفق بنجاح، ولكن يتم حظر حزم ESP بواسطة ISP أو ISPs في كل الاتجاهين. هذا يسبب لا يشفر حركة مرور من خلال لا VPN أن يفشل كما هو موضح في الصورة:



ملاحظة: عندما يقوم ISP بحظر حزم ESP، ينجح إنشاء نفق IPsec، ولكن تتأثر حركة مرور البيانات المشفرة. يمكن التعامل مع الشبكة الخاصة الظاهرية (VPN) الأعلى، ولكن حركة المرور لا تعمل عليه.

تلميح: يمكن أن يكون السيناريو الذي يتم فيه حظر حركة مرور ESP في إتجاه واحد فقط موجودا أيضا. الأعراض هي نفسها، ولكن يمكن العثور عليها بسهولة مع معلومات إحصائيات النفق، التضمين، عدادات إزالة الكبسلة، أو عدادات RX و TX.

معلومات ذات صلة

- تصحيح أخطاء مستوى البروتوكول وتبادل حزم KEv2
- تبادل مفتاح الإنترنت (IKE) - RFC 2409
- بروتوكول تبادل مفتاح الإنترنت (IKEv2)
- 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).