تصحيح أخطاء مستوى البروتوكول وتبادل حزم IKEv2

المحتويات

المقدمة

يوضح هذا المستند ميزات أحدث إصدار من Internet Key Exchange (IKE) والاختلافات بين الإصدار 1 والإصدار 2.

IKE هو البروتوكول المستخدم لإعداد اقتران أمان (SA) في مجموعة بروتوكولات IPsec. IKEv2 هو الإصدار الثاني والأحدث من بروتوكول IKE. وقد بدأ اعتماد هذا البروتوكول في عام 2006. تم وصف الحاجة والنية لإجراء إصلاح لبروتوكول IKE في الملحق أ من *بروتوكول تبادل مفتاح الإنترنت (IKEv2)* في RFC 4306.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

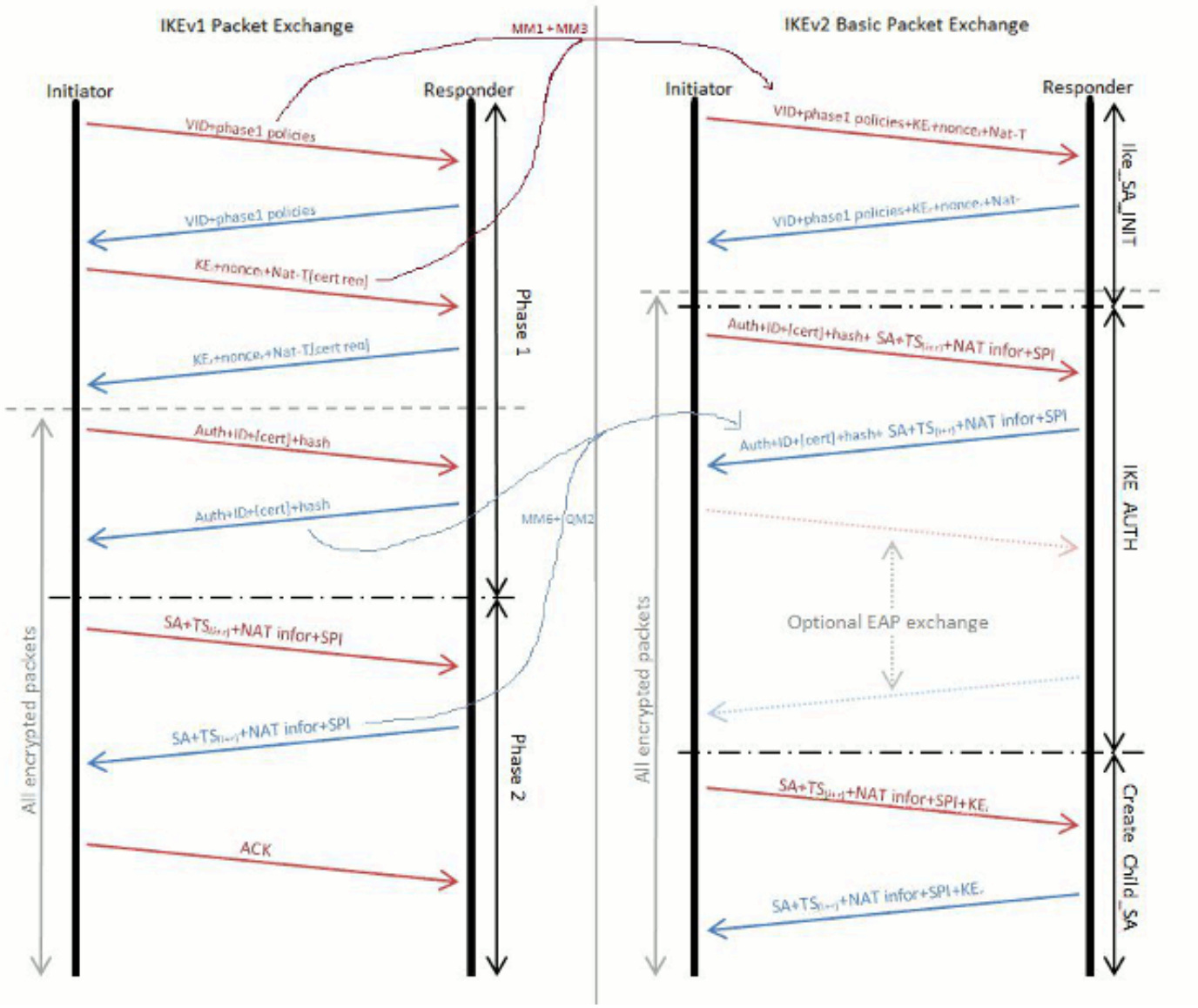
لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

الاختلافات بين IKEv1 و IKEv2

وفي حين يصف *بروتوكول تبادل مفتاح الإنترنت (IKEv2)* في RFC 4306 بشكل تفصيلي كبير ميزات الإصدار الثاني من بروتوكول IKEv2 مقارنة بالإصدار الأول من بروتوكول IKEv1، فمن المهم ملاحظة أنه تم إصلاح تبادل IKE بالكامل. يقدم هذا المخطط مقارنة بين العلامتين:



في IKEv1، كان هناك تبادل في المرحلة الأولى محدد بشكل واضح، ويحتوي على ست حزم متبوعة بتبادل في المرحلة الثانية يتكون من ثلاث حزم، تبادل IKEv2 متغير. في أفضل الأحوال، يمكنه تبادل ما يصل إلى أربع حزم. في أسوأ الحالات، يمكن أن يزيد هذا إلى ما يصل إلى 30 حزمة (إن لم يكن أكثر)، حسب تعقيد المصادقة، عدد سمات بروتوكول المصادقة المتوسع (EAP) المستخدمة، بالإضافة إلى عدد حالات SAs التي تم تكوينها. يقوم IKEv2 بدمج معلومات المرحلة الثانية في IKEv1 في تبادل IKE_AUTH، ويضمن ذلك أنه بعد اكتمال تبادل IKE_AUTH، يكون لدى كلا النظراء بالفعل SA واحد تم إنشاؤه وهو جاهز لتشفير حركة المرور. بنيت هذا SA فقط للوكيل هويات أن يطابق الزناد ربط. أي حركة مرور لاحقة تطابق هويات وكيل أخرى ثم تقوم بتشغيل تبادل CREATE_CHILD_SA، وهو ما يعادل تبادل المرحلة 2 في IKEv1. لا يوجد أي من "الوضع المتميز" أو "الوضع الرئيسي".

المراحل الأولية في تبادل IKEv2

وفي الواقع، لا يتضمن الإصدار الثاني من بروتوكول الغلاف الجوي سوى مرحلتين أوليتين من التفاوض:

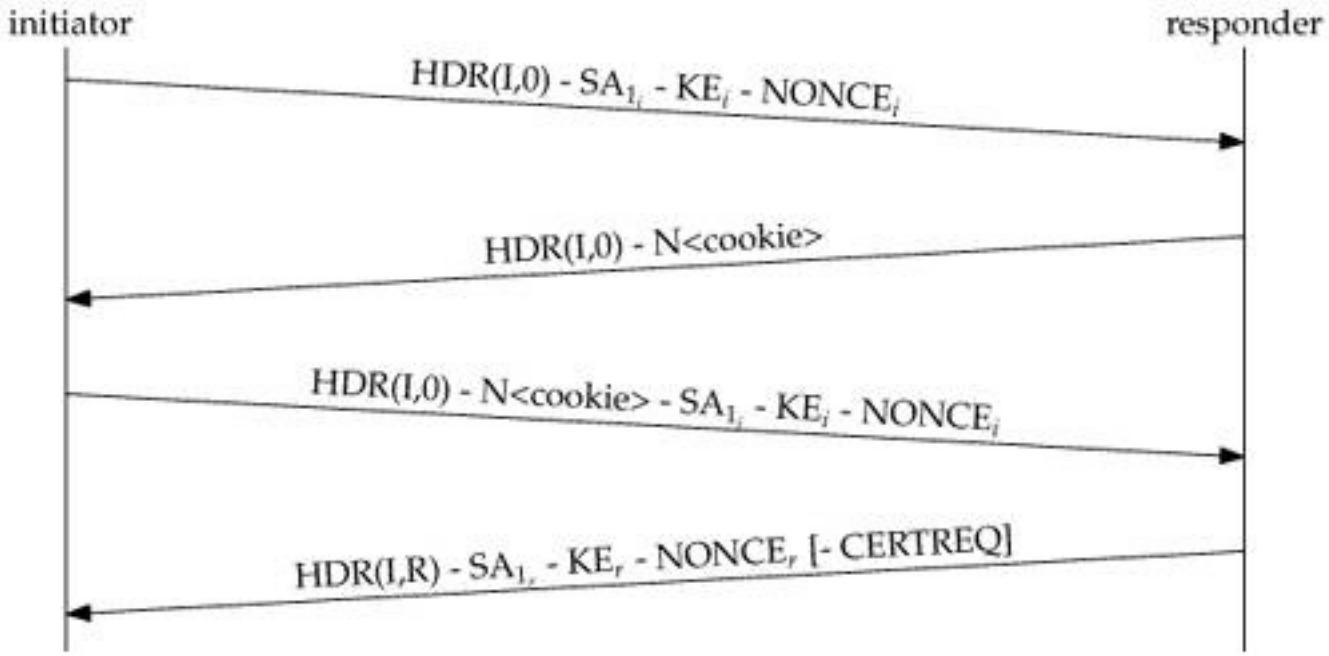
- تبادل IKE_SA_INIT
- تبادل IKE_AUTH

تبادل IKE_SA_INIT

IKE_SA_INIT هو التبادل الأولي الذي يقوم فيه النظراء بإنشاء قناة آمنة. وبعد إتمام عملية التبادل الأولية، يتم تشفير جميع عمليات التبادل الأخرى. وتحتوي عمليات التبادل على حزمتين فقط لأنها تجمع بين جميع المعلومات التي يتم تبادلها عادة في MM1-4 في IKEv1. ونتيجة لذلك، فإن المستجيب مكلف حسابيا لمعالجة حزمة IKE_SA_INIT ويمكن أن يغادر لمعالجة الحزمة الأولى، ويترك البروتوكول مفتوحا لهجوم رفض الخدمة (DoS) من العناوين المنتحلة.

وللحماية من هذا النوع من الهجمات، يحتوي IKEv2 على تبادل إختياري داخل IKE_SA_INIT لمنع الهجمات المنتحلة. إذا تم الوصول إلى حد معين لجلسات العمل غير المكتملة، لا يقوم المستجيب بمعالجة الحزمة بشكل أكبر، بل يرسل بدلا من ذلك إستجابة إلى البادئ مع ملف تعريف إرتباط. لمتابعة جلسة العمل، يجب أن يقوم البادئ بإعادة إرسال حزمة IKE_SA_INIT وتضمين ملف تعريف الارتباط الذي تلقاه.

يقوم البادئ بإعادة إرسال الحزمة الأولية مع حمولة الإعلام من المستجيب التي تثبت عدم انتحال التبادل الأصلي. فيما يلي رسم تخطيطي لعملية تبادل IKE_SA_INIT مع مسابقة ملف تعريف الارتباط:



تبادل IKE_AUTH

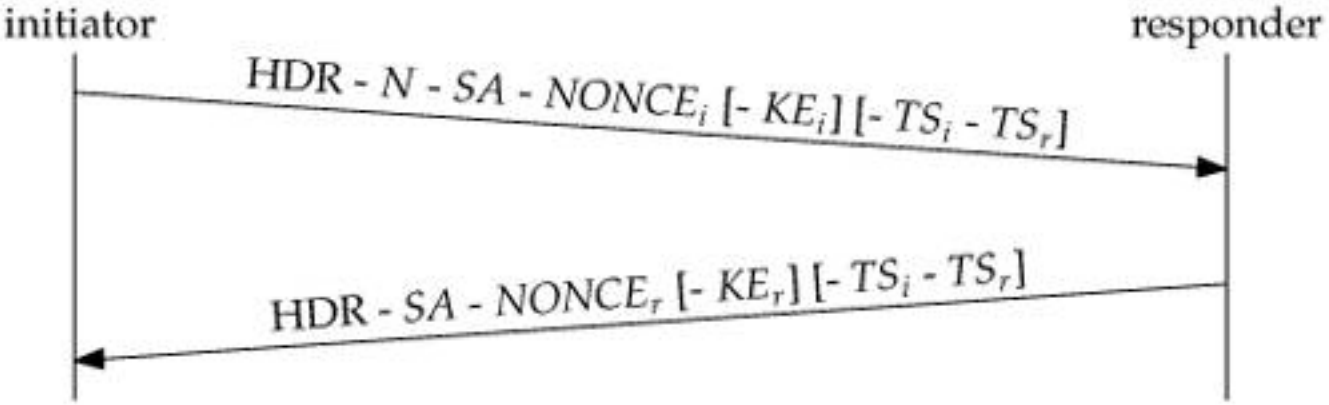
بعد اكتمال تبادل IKE_SA_INIT، يتم تشفير IKEv2 SA، ومع ذلك، لم تتم مصادقة النظير البعيد. يتم إستخدام تبادل IKE_AUTH لمصادقة النظير البعيد وإنشاء IPsec SA الأول.

يحتوي Exchange على معرف بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) مع حمولة مصادقة. تعتمد محتويات حمولة المصادقة على طريقة المصادقة، والتي يمكن أن تكون مفتاح مشترك مسبقا (PSK)، أو شهادات RSA (RSA-SIG)، أو شهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA-SIG)، أو EAP. بالإضافة إلى حمولات المصادقة، يتضمن التبادل حمولات SA و Traffic Selector التي تصف IPsec SA الذي سيتم إنشاؤه.

عمليات تبادل IKEv2 اللاحقة

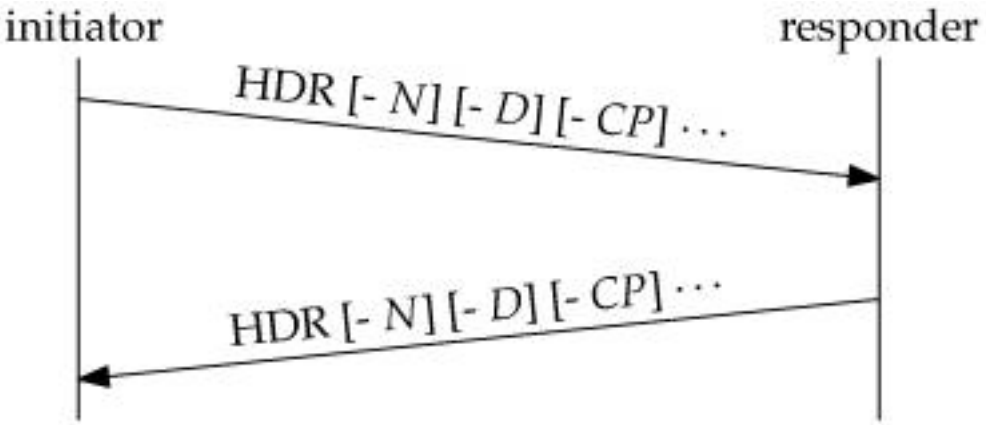
تبادل CREATE_CHILD_SA

إذا كانت هناك حاجة إلى شبكات SA فرعية إضافية، أو إذا كان يلزم إعادة تكوين IKE SA أو أحد شبكات SA التابعة، فإنها تخدم نفس الوظيفة التي يؤديها تبادل الوضع السريع في IKEv1. كما هو موضح في هذا المخطط، هناك حزمتان فقط في هذا التبادل؛ ومع ذلك، يكرر Exchange لكل rekey أو sa جديد:



تبادل المعلومات

وكما هو الحال في جميع عمليات تبادل IKEv2، يتوقع كل طلب من طلبات تبادل المعلومات إستجابة. يمكن تضمين ثلاثة أنواع من الحمولات في عملية تبادل المعلومات. يمكن تضمين أي عدد من أي مجموعة من الحمولات، كما هو موضح في هذا المخطط:



- تم بالفعل عرض حمولة الإعلام (N) بالاقتران مع ملفات تعريف الارتباط. وهناك العديد من الأنواع الأخرى أيضا. فهي تحمل معلومات عن الخطأ والحالة، كما تفعل في IKEv1.
- يقوم "حذف الحمولة (D)" بإعلام النظير بأن المرسل قد قام بحذف واحد أو أكثر من وحدات SA الواردة الخاصة به. من المتوقع أن يقوم المستجيب بحذف أسماء الأمان هذه وعادة ما يتضمن حذف حمولات خاصة بوحدات الخدمة الخاصة التي تتوافق في الإتجاه الآخر في رسالة الرد الخاصة به.
- يتم إستخدام حمولة التكوين (CP) للتفاوض على بيانات التكوين بين الأقران. أحد الاستخدامات الهامة للبروتوكول cp هو طلب (طلب) وتعيين (إستجابة) عنوان على شبكة محمية ببوابة أمان. في الحالة النموذجية، يؤسس مضيف جوال شبكة خاصة ظاهرية (VPN) مع عبارة أمان على شبكته المنزلية ويطلب أن يتم منحها عنوان IP على الشبكة المنزلية.**ملاحظة:** يؤدي هذا إلى إزالة إحدى المشاكل التي من المفترض أن يحلها الاستخدام المجمع لبروتوكول الاتصال النفقي للطبقة 2 (L2TP) و IPsec.

معلومات ذات صلة

- تصحيح أخطاء ASA IKEv2 لشبكة VPN من موقع إلى موقع مع PSKs TechNote
- تصحيح أخطاء ASA IPsec و IKE (الوضع الرئيسي IKEv1) أستكشاف أخطاء TechNote وإصلاحها
- تصحيح أخطاء الوضع الرئيسي ل IPSec و IKE - IKEv1 Main Mode Troubleshooting TechNote
- تصحيح أخطاء ASA IPSec و IKE - IKEv1 Aggressive Mode TechNote
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- تنزيلات برامج أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- مفاوضة IPSec/بروتوكولات IKE

- جدار حماية Cisco IOS
- برنامج IOS من Cisco
- القشرة الآمنة (SSH)
- مفاوضة IPSec/بروتوكولات IKE
- 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).