تكوين تشفير طبقة الشبكة من Cisco واستكشاف أخطاءه وإصلاحها: الخلفية - الجزء 1

المحتويات

المقدمة

يناقش هذا المستند تكوين تشفير طبقة الشبكة واستكشاف أخطاء هذا التشفير من Cisco باستخدام IPSec وارتباط أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) ويغطي معلومات الخلفية لتشفير طبقة الشبكة والتكوين الأساسي مع IPSec و ISAKMP.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية:

- برنامج IOS® الإصدار 11.2 من Cisco والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

تكوين ومعلومات خلفية تشفير طبقة الشبكة

تم إدخال ميزة تشفير طبقة الشبكة في البرنامج Cisco IOS® Software، الإصدار 11.2. وهو يوفر آلية لنقل البيانات بشكل آمن ويتألف من عنصرين:

- **مصادقة الموجه:** قبل تمرير حركة المرور المشفرة، يقوم موجهان بإجراء مصادقة ثنائية الإتجاه مرة واحدة باستخدام المفاتيح العامة لمعيار التوقيع الرقمي (DSS) لتوقيع تحديات عشوائية.
- **تشفير طبقة الشبكة:** لتشفير حمولة IP، تستخدم الموجهات تبادل مفتاح Diffie-Hellman لإنشاء DES (مفتاح جلسة 40-أو 56-بت) بشكل آمن، أو DES الثلاثي - -168) 3DESبت)، أو معيار التشفير المتقدم الأحدث - -128)AESبت (افتراضي)، أو 192-بت، أو مفتاح 256-بت)، المقدم في 12.2(13)T. يتم إنشاء مفاتيح جلسات عمل جديدة على أساس قابل للتكوين. يتم تعيين سياسة التشفير بواسطة خرائط التشفير التي تستخدم قوائم الوصول إلى IP الموسعة لتحديد أزواج الشبكات أو الشبكات الفرعية أو المضيف أو البروتوكول التي يجب تشفيرها بين الموجهات.

خلفية التشفير

يعنى مجال التشفير بإبقاء الاتصالات خاصة. وكانت حماية الاتصالات الحساسة هي التركيز على التشفير طوال معظم تاريخها. التشفير هو تحويل البيانات إلى شكل غير قابل للقراءة. والغرض منه هو ضمان الخصوصية من خلال إخفاء المعلومات عن أي شخص لا يقصد بها ذلك، حتى إذا كان بإمكانهم رؤية البيانات المشفرة. فك التشفير هو عكس التشفير، إنه تحويل البيانات المشفرة مرة أخرى إلى شكل مفهوم.

ويتطلب التشفير وفك التشفير إستخدام بعض المعلومات السرية، التي يشار إليها عادة باسم "المفتاح". واعتمادا على آلية التشفير المستخدمة، يمكن إستخدام المفتاح نفسه لكل من التشفير وفك التشفير، بينما بالنسبة للآليات الأخرى، قد تكون المفاتيح المستخدمة للتشفير وفك التشفير مختلفة.

التوقيع الرقمي يربط الوثيقة بحامل مفتاح معين، بينما يربط الطابع الزمني الرقمي الوثيقة بإنشائها في وقت معين. يمكن إستخدام آليات التشفير هذه للتحكم في الوصول إلى محرك أقراص مشترك أو تثبيت عالي الأمان أو إلى قناة تلفزيونية تعمل بنظام الدفع لكل عرض.

في حين ان التشفير العصري يزداد تنوعا، فإن التشفير يعتمد بشكل أساسي على مشاكل يصعب حلها. قد تكون المشكلة صعبة لأن حلها يتطلب معرفة المفتاح، مثل فك تشفير رسالة مشفرة أو توقيع وثيقة رقمية. وقد تكون المشكلة صعبة أيضا لأنه من الصعب إكمالها جوهريا، مثل إيجاد رسالة تنتج قيمة تجزئة معينة.

مع تقدم مجال التشفير، فإن الخطوط الفاصلة لما هو وما هو غير تشفير أصبحت غير واضحة. التشفير اليوم يمكن

تلخيصه كدراسة للتقنيات والتطبيقات التي تعتمد على وجود مشاكل رياضية يصعب حلها. يحاول التشفير أختراق الآليات المشفرة، والتشفير هو علم التشفير والتحليل المتراص.

التعاريف

يحدد هذا القسم المصطلحات ذات الصلة المستخدمة في هذا المستند بالكامل.

- **المصادقة:** خاصية معرفة أن البيانات المتلقاة يتم إرسالها بالفعل بواسطة المرسل المزعوم.
- **السرية:** خاصية الاتصال بحيث يعرف المستلمون المعتدون ما يتم إرساله ولكن الأطراف غير المقصودة لا يمكنها تحديد ما يتم إرساله.
- **معيار تشفير البيانات (DES):** يستخدم DES طريقة مفتاح متماثل، تعرف أيضا بطريقة مفتاح سري. وهذا يعني أنه إذا تم تشفير كتلة من البيانات باستخدام المفتاح، فيجب فك تشفير الكتلة المشفرة باستخدام المفتاح نفسه، لذلك يجب أن يستخدم كل من التشفير وفك التشفير المفتاح نفسه. وعلى الرغم من أن أسلوب التشفير معروف ومنشر بشكل جيد، إلا أن أسلوب الهجوم الأكثر شيوعا بين عامة الناس يتم من خلال القوة الغاشمة. يجب إختبار المفاتيح مقابل الكتل المشفرة لمعرفة ما إذا كانت قادرة على حلها بشكل صحيح. مع زيادة المعالجات قوة، تقترب الحياة الطبيعية ل DES من نهايتها. على سبيل المثال، جهد منسق يستخدم طاقة المعالجة الاحتياطية من آلاف أجهزة الكمبيوتر عبر الإنترنت يمكن العثور على المفتاح 56 بت لرسالة DES مشفرة في 21 يوما.يتم التحقق من صلاحية خدمة التشفير الديناميكي (DES) كل خمس سنوات من قبل وكالة الأمن القومي الأمريكية لتلبية أغراض الحكومة الأمريكية. وتنتهي فترة الموافقة الحالية في عام 1998، وأشارت وكالة الأمن القومي إلى أنها لن تعيد التصديق على نظام إدارة المعلومات. وبالانتقال إلى ما بعد DES، هناك خوارزميات تشفير أخرى ليس لديها أيضا أي نقاط ضعف معروفة غير الهجمات العنيفة. لمزيد من المعلومات، راجع DES FIPS 46-2 من قبل المعهد الوطني للمعايير والتكنولوجيا .
- **فك التشفير:** التطبيق العكسي لخوارزمية التشفير على البيانات المشفرة، وبالتالي إستعادة تلك البيانات إلى حالتها الأصلية غير المشفرة.
- **خوارزمية التوقيعات الرقمية (DSA):** تم نشر وكيل خدمة Dell (المعروف باسم NIST) في معيار التوقيع الرقمي (DSS)، الذي يعد جزءا من مشروع Capstone الخاص بحكومة الولايات المتحدة. تم إختيار DSS من قبل NIST، بالتعاون مع NSA، ليكون معيار المصادقة الرقمية للحكومة الأمريكية. وقد صدر هذا المعيار في 19 أيار/مايو 1994.
- **التشفير:** تطبيق خوارزمية معينة على البيانات من أجل تغيير مظهر البيانات مما يجعل من غير المفهوم بالنسبة لأولئك غير المصرح لهم برؤية المعلومات.
- **التكامل:** خاصية التأكد من نقل البيانات من المصدر إلى الوجهة بدون تغيير غير مكشوف.
- **عدم التنكر:** يمكن لخاصية المتلقي أن يثبت أن مرسل بعض البيانات أرسل البيانات في الواقع على الرغم من أن المرسل قد يرغب فيما بعد في رفض إرسال تلك البيانات أبدا.
- **تشفير المفتاح العام:** تستند التشفير التقليدي إلى مرسل الرسالة ومستلمها الذي يعرف نفس المفتاح السري ويستخدمه. يستخدم المرسل المفتاح السري لتشفير الرسالة، ويستخدم المستقبل نفس المفتاح السري لفك تشفير الرسالة. وتعرف هذه الطريقة باسم "المفتاح السري" أو "التشفير التماثلي". تتمثل المشكلة الرئيسية في جعل المرسل والمتلقي يتفقان على المفتاح السري دون أن يكتشف أي شخص آخر ذلك. إذا كانوا في مواقع فعلية منفصلة، يجب أن يثقوا في ساعي البريد، أو في نظام الهاتف، أو في أي وسيلة إرسال أخرى لمنع الإفصاح عن المفتاح السري الذي يتم إبلاغه. يمكن لأي شخص يقوم بمراجعة المفتاح أثناء النقل أو اعتراضه قراءة جميع الرسائل المشفرة أو المصادق عليها أو تعديلها وتزييفها في وقت لاحق باستخدام هذا المفتاح. يسمى إنشاء المفاتيح ونقلها وتخزينها بإدارة المفاتيح؛ ويجب أن تعالج جميع أنظمة التشفير مسائل الإدارة الأساسية. نظرا لأن جميع المفاتيح في نظام تشفير المفاتيح السرية يجب أن تظل سرية، فإن تشفير المفاتيح السرية غالبا ما يواجه صعوبة في توفير إدارة آمنة للمفتاح، وخاصة في الأنظمة المفتوحة التي يوجد بها عدد كبير من المستخدمين.في عام 1976، طرح ويتفلد ديفي ومارتن هيلمان مفهوم تشفير المفاتيح العامة من أجل حل مشكلة الإدارة الأساسية. في مفهومهم، كل شخص يحصل على زوج من المفاتيح، واحد يسمى المفتاح العام والآخر يسمى المفتاح الخاص. يتم نشر المفتاح العام لكل شخص بينما يتم الاحتفاظ بالمفتاح الخاص سرا. تم التخلص من الحاجة إلى مشاركة المرسل والمستلم للمعلومات السرية، وتتضمن جميع الاتصالات المفاتيح العامة فقط، ولا يتم إرسال أي مفتاح خاص أو مشاركته على الإطلاق. لم يعد من الضروري أن تثق في بعض قنوات الإتصالات حتى

تكون آمنة ضد التنصت أو الخيانة. المتطلب الوحيد هو أن تكون المفاتيح العامة مرتبطة بالمستخدمين بطريقة موثوق بها (مصدق عليها) (على سبيل المثال، في دليل موثوق به). يمكن لأي شخص إرسال رسالة سرية ببساطة باستخدام معلومات عامة، ولكن يمكن فك تشفير الرسالة باستخدام مفتاح خاص فقط، وهو في حوزة المستلم المقصود. وعلاوة على ذلك، يمكن إستخدام تشفير المفتاح العام ليس فقط للخصوصية (التشفير)، بل للمصادقة (التوقيعات الرقمية) أيضا.

- **التوقيعات الرقمية للمفتاح العام:** لتوقيع رسالة، يقوم شخص ما بحساب يشمل مفتاحه الخاص والرسالة نفسها. يسمى المخرج التوقيع الرقمي ويرتبط بالرسالة، التي يتم إرسالها بعد ذلك. والشخص الثاني يتحقق من التوقيع بإجراء حساب يشمل الرسالة، التوقيع المزعوم، والمفتاح العام للشخص الاول. إذا كانت النتيجة تحمل بشكل صحيح في علاقة رياضية بسيطة، يتم التحقق من صحة التوقيع. وإلا، فقد يكون التوقيع مخادعا أو قد تكون الرسالة قد تغيرت.
- **تشفير المفتاح العام:** عندما يرغب شخص ما في إرسال رسالة سرية إلى شخص آخر، يقوم الشخص الأول بالبحث عن المفتاح العام للشخص الثاني في دليل، ويستخدمه لتشفير الرسالة وإرسالها. ثم يستخدم الشخص الثاني مفتاحه الخاص لفك تشفير الرسالة وقراءتها. لا أحد يستمع للرسالة يستطيع فك تشفير الرسالة. يمكن لأي شخص إرسال رسالة مشفرة إلى الشخص الثاني ولكن الشخص الثاني فقط يمكنه قراءتها. ومن الواضح أن أحد المتطلبات هو ألا يتمكن أحد من اكتشاف المفتاح الخاص من المفتاح العام المقابل.
- **تحليل حركة المرور:** تحليل تدفق حركة مرور الشبكة بغرض خصم المعلومات المفيدة للخصم. من أمثلة هذه المعلومات تكرار الإرسال، هويات الأطراف المحولة، أحجام الحزم، معرفات التدفق المستخدمة، وهكذا.

معلومات أولية

يناقش هذا القسم بعض مفاهيم تشفير طبقة الشبكة الأساسية. إنه يحتوي على جوانب التشفير التي يجب أن تبحث عنها. في البداية قد لا تكون هذه القضايا منطقية بالنسبة لك، ولكنها فكرة جيدة أن تقرأها الآن وأن تكون على دراية بها لأنها ستكون منطقية أكثر بعد أن تعمل على التشفير لعدة أشهر.

- من المهم ملاحظة أن التشفير يحدث فقط على إخراج واجهة ما وأن فك التشفير يحدث فقط عند الإدخال إلى الواجهة. وهذا التمييز مهم عند وضع سياستكم. نهج التشفير وفك التشفير متماثل. هذا يعني أن تعريف واحد يعطي لك الآخر تلقائيا. باستخدام خرائط التشفير وقوائم الوصول الموسعة المقترنة بها، يتم تعريف نهج التشفير فقط بشكل صريح.يستخدم نهج فك التشفير المعلومات المتطابقة، ولكن عند مطابقة الحزم، فإنه يعكس عناوين ومنافذ المصدر والوجهة. بهذه الطريقة، تتم حماية البيانات في كلا الاتجاهين لاتصال الإرسال ثنائي الإتجاه. يتم إستخدام عبارة *match address x* في الأمر **crypto map** لوصف الحزم التي تترك واجهة. بمعنى آخر، فإنه يصف تشفير الحزم. ومع ذلك، يجب أيضا مطابقة الحزم لفك التشفير عند إدخالها على الواجهة. ويتم القيام بذلك تلقائيا من خلال إجتياز قائمة الوصول باستخدام عناوين المصدر والوجهة والمنافذ المعكوسة. يوفر ذلك تناظرا للاتصال. يجب أن تصف قائمة الوصول التي تشير إليها **خريطة التشفير** حركة المرور في إتجاه واحد (صادر) فقط. سيتم نقل حزم IP التي لا تطابق قائمة الوصول التي تحددها ولكن لن يتم تشفيرها. يشير "رفض" في قائمة الوصول إلى أنه يجب عدم تطابق هذه الأجهزة المضيفة، مما يعني أنها لن يتم تشفيرها. لا يعني "deny"، في هذا السياق، إسقاط الحزمة.
- توخى الحذر عند إستخدام كلمة "any" في قوائم الوصول الموسعة. يتسبب إستخدام "أي" في إسقاط حركة المرور الخاصة بك ما لم يتم توجهها إلى واجهة "عدم تشفير" المطابقة. وبالإضافة إلى ذلك، لا يتم السماح "any" باستخدام IPSec في الإصدار 11.3(3)T من برنامج Cisco IOS Software.
- يتم تثبيط إستخدام الكلمة الأساسية "any" في تحديد عناوين المصدر أو الوجهة. يمكن أن يؤدي تحديد "any" إلى حدوث مشاكل في بروتوكولات التوجيه وبروتوكول وقت الشبكة (NTP) و echo واستجابة صدى صدى الصوت وحركة مرور البث المتعدد، نظرا لأن موجه الاستقبال يتجاهل حركة المرور هذه بصمت. إذا كان "any" ليتم إستخدامه، فيجب أن تكون مسبوقة ببيانات "deny" لحركة المرور التي لا يتم تشفيرها، مثل "ntp".
- لتوفير الوقت، تأكد من إمكانية **إختبار اتصال** الموجه النظير الذي تحاول إستخدام اقتران تشفير به. بالإضافة إلى ذلك، دع الأجهزة الطرفية (التي تعتمد على تشفير حركة مرور البيانات الخاصة بها) تتفاعل مع بعضها البعض قبل أن تستغرق وقتا طويلا في أستكشاف المشكلة الخطأ وإصلاحها. بمعنى آخر، تأكد من عمل التوجيه قبل محاولة تنفيذ **التشفير**. قد لا يحتوي النظير البعيد على مسار لواجهة الخروج، وفي هذه الحالة لا يمكنك الحصول على جلسة عمل تشفير مع هذا النظير (قد تكون قادرا على إستخدام **ip غير المرقمة** على الواجهة التسلسلية).

- يستخدم العديد من إرتباطات WAN من نقطة إلى نقطة عناوين IP غير القابلة للتوجيه، ويعتمد تشفير Cisco IOS الإصدار 11.2 على بروتوكول رسائل التحكم في الإنترنت (ICMP) (بمعنى أنه يستخدم عنوان IP لواجهة الخروج التسلسلية ل ICMP). قد يفرض عليك ذلك إستخدام **IP غير المرقمة** على واجهة WAN. قم دائما بتنفيذ الأمر **ping** و**traceroute** للتأكد من وجود التوجيه في مكانه لموجهات نظير (تشفير/فك تشفير).
- يسمح فقط لموجهين بمشاركة مفتاح جلسة Diffie-Hellman. وهذا يعني، أن مسحاج تخديد واحد يستطيع لا يتبادل ربط مشفر إلى إثنان نظير يستعمل ال نفسه جلسة مفتاح؛ كل زوج من مسحاج تخديد ينبغي يتلقى جلسة مفتاح أن يكون نتيجة تبادل Diffie-Hellman بينهم.
- يكون محرك التشفير إما في Cisco IOS أو Cisco IOS VIP2 أو في الأجهزة مهايئ خدمات التشفير (ESA) على VIP2. بدون VIP2، يتحكم محرك التشفير Cisco IOS في سياسة التشفير على جميع المنافذ. على الأنظمة الأساسية التي تستخدم VIP2، هناك العديد من المحركات المشفرة: واحد في CISCO IOS، وواحد على كل VIP2. يتحكم محرك التشفير على VIP2 في التشفير على المنافذ الموجودة على اللوحة.
- تأكد من تعيين حركة المرور للوصول إلى واجهة معدة لتشفيرها. إذا كان من الممكن لحركة المرور الوصول بشكل ما إلى واجهة أخرى غير تلك التي تم تطبيق **خريطة التشفير** عليها، يتم إسقاطها بصمت.
- وهو يساعد في الحصول على وصول وحدة تحكم (أو بديل) إلى كلا الموجهين عند إجراء تبادل المفاتيح، كما أنه من الممكن الحصول على الجانب السلبي للتعليق أثناء انتظار المفتاح.
- يعد **CFB-64** أكثر فعالية في المعالجة من **CFB-8** من حيث حمل وحدة المعالجة المركزية.
- يحتاج المسحاج تخديد أن يكون يركض الخوارزمية أن أنت تريد أن يستعمل مع ال CFB (cipher-feedback) أسلوب أن أنت تريد أن يستعمل؛ التقصير لكل صورة هو اسم الصورة (مثل "56") مع **CFB-64**.
- فكر في تغيير مهلة المفتاح. إن 30 دقيقة من التخلف عن السداد قصيرة للغاية. حاول زيادتها إلى يوم واحد (1440 دقيقة).
- يتم إسقاط حركة مرور IP أثناء إعادة التفاوض على المفتاح في كل مرة ينتهي فيها المفتاح.
- حدد حركة المرور التي تريد تشفيرها بالفعل فقط (يؤدي ذلك إلى حفظ دورات وحدة المعالجة المركزية).
- باستخدام توجيه الاتصال عند الطلب (DDR)، أجعل ICMP مثيرا للاهتمام أو لن يتصل مطلقا.
- إذا كنت ترغب في تشفير حركة المرور بخلاف IP، فاستخدم نفقا. باستخدام الأنفاق، قم بتطبيق خرائط التشفير على كل من الواجهات المادية وواجهات الأنفاق. راجع العينة 5: تشفير حركة مرور IPX في نفق IP للحصول على مزيد من المعلومات.
- لا يلزم توصيل موجهات نظير التشفير مباشرة.
- قد يمنحك الموجه الطرفي المنخفض رسالة "الخنزير في وحدة المعالجة المركزية". يمكن تجاهل ذلك لأنه يخبرك بأن التشفير يستخدم الكثير من موارد وحدة المعالجة المركزية.
- لا تقم بوضع موجهات تشفير بشكل متكرر حتى تقوم بإلغاء تشفير حركة المرور وإعادة تشفيرها وإتلاف وحدة المعالجة المركزية (CPU). ببساطة قم بالتشفير عند نقطتي النهاية. راجع العينة 3: التشفير إلى الموجه ومن خلاله للحصول على مزيد من المعلومات.
- حاليا، تشفير البث والبث المتعدد غير مدعوم. إذا كانت تحديثات التوجيه "الآمنة" مهمة لتصميم الشبكة، فيجب إستخدام بروتوكول بمصادقة مضمنة، مثل بروتوكول التوجيه المحسن للعبارة الداخلية (EIGRP) أو فتح أقصر مسار أولا (OSPF) أو بروتوكول معلومات التوجيه الإصدار 2 (RIPv2) لضمان تكامل التحديث.

كافيتس

ملاحظة: تم حل جميع التحذيرات المذكورة أدناه.

- لا يمكن للموجه Cisco 7200 الذي يستخدم ESA للتشفير فك تشفير حزمة تحت مفتاح جلسة واحد ثم إعادة تشفيرها تحت مفتاح جلسة مختلف. أحلت cisco بق CSCdj82613 id (يسجل زبون فقط).
- عندما يتم توصيل موجهين بواسطة خط مؤجر مشفر وخط نسخ إحتياطي لشبكة ISDN، إذا تم إسقاط الخط المؤجر، فإن إرتباط ISDN يكون جيدا. ومع ذلك، عند إعادة ظهور الخط المؤجر مرة أخرى، يتعطل الموجه الذي وضع اتصال ISDN. أحلت cisco بق CSCdj00310 id (يسجل زبون فقط).
- بالنسبة لموجهات سلسلة Cisco 7500 التي تحتوي على العديد من الشخصيات المهمة، إذا تم تطبيق **خريطة تشفير** على واجهة واحدة فقط لأي شخصية مهمة، تعطل شخصية مهمة واحدة أو أكثر. أحلت cisco بق id CSCdi88459 (يسجل زبون فقط).

- بالنسبة لموجهات سلسلة Cisco 7500 التي تحتوي على VIP2 و ESA، لا يعرض الأمر **show crypto card** الإخراج ما لم يكن المستخدم في منفذ وحدة التحكم. أحلت cisco بق CSCdj89070 id (يسجل زبون فقط).

تكوين تشفير طبقة الشبكة IOS من Cisco

جاءت عينة العمل من تكوينات Cisco IOS في هذا المستند مباشرة من موجهات المعامل. وكان التغيير الوحيد الذي أدخل عليها هو إزالة تكوينات الواجهة غير المرتبطة. جميع المواد هنا جاءت من المصادر المتاحة مجانا على الإنترنت أو في قسم المعلومات ذات الصلة في نهاية هذه الوثيقة.

تأتي جميع تكوينات النموذج في هذا المستند من برنامج Cisco IOS Software، الإصدار 11.3. هناك عدة تغيير من ال cisco ios برمجية إطلاق 11.2 أمر، مثل الإضافة من التالي كلمة:

- dss في بعض من أمر تكوين المفتاح.
- cisco في بعض من **العرض** أمر و**ال crypto map** أمر أن يميز بين cisco مالك تشفير (كما هو موجود في cisco ios برمجية إطلاق 11.2 وفيما بعد) و IPSec أي في cisco ios برمجية إطلاق 11.3(2)T.

ملاحظة: تم إختيار عناوين IP المستخدمة في أمثلة التكوين هذه بشكل عشوائي في مختبر Cisco ويقصد بها أن تكون عامة بالكامل.

الخطوة 1: إنشاء أزواج مفاتيح DSS يدويا

يجب إنشاء زوج مفاتيح DSS (مفتاح عام ومفتاح خاص) يدويا على كل موجه مشارك في جلسة التشفير. بمعنى آخر، يجب أن يكون لكل موجه مفاتيح DSS خاصة به للمشاركة. يمكن أن يحتوي محرك التشفير على مفتاح DSS واحد فقط يقوم بتعريفه بشكل فريد. تمت إضافة الكلمة الأساسية "dss" في البرنامج Cisco IOS Software، الإصدار 11.3 لتمييز DSS من مفاتيح RSA. يمكنك تحديد أي اسم لمفاتيح DSS الخاصة بالموجه (على الرغم من أنه يوصى باستخدام اسم مضيف الموجه). على وحدة معالجة مركزية (CPU) أقل قوة (مثل سلسلة Cisco 2500)، يستغرق إنشاء زوج المفاتيح حوالي 5 ثوان أو أقل.

يقوم الموجه بإنشاء زوج من المفاتيح:

- مفتاح عام (والذي يتم إرساله لاحقا إلى الموجهات المشاركة في جلسات التشفير).
- مفتاح خاص (لا يرى ولا يتبادل مع أي شخص آخر، بل يخزن في قسم منفصل من ذاكرة NVRAM لا يمكن عرضه).

بمجرد إنشاء زوج مفاتيح DSS الخاص بالموجه، يتم ربطه بشكل فريد بمحرك التشفير في ذلك الموجه. يتم عرض إنشاء زوج المفاتيح في إخراج أمر المثال أدناه.

```
dial-5(config)#crypto key generate dss dial5
.... Generating DSS keys
[OK]

dial-5#show crypto key mypubkey dss
crypto public-key dial5 05679919
160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
quit


dial-5#show crypto engine configuration
slot:                0
engine name:         dial5
engine type:         software
serial number:       05679919
platform:            rp crypto engine
```

```
crypto lib version: 10.0.0

:Encryption Process Info
  input queue top:    43
  input queue bot:    43
   input queue count:  0

dial-5#
```

نظرا لأنه يمكنك إنشاء زوج مفاتيح واحد فقط يعرف الموجه، فيمكنك الكتابة فوق المفتاح الأصلي لديك والحاجة إلى إعادة إرسال مفتاحك العام باستخدام كل موجه في إرتباط التشفير. وهذا موضح في إخراج الأمر المثال أدناه:

```
StHelen(config)#crypto key generate dss barney
Generating new DSS keys will require re-exchanging %
public keys with peers who already have the public key
                                        !named barney
Generate new DSS keys? [yes/no]: yes
.... Generating DSS keys
                                              [OK]


#(StHelen(config
.Mar 16 12:13:12.851: Crypto engine 0: create key pairs
```

الخطوة 2: تبادل مفاتيح DSS العامة يدويا مع الأقران (خارج النطاق)

يعد إنشاء زوج مفاتيح DSS الخاص بالموجه الخطوة الأولى في إنشاء اقتران جلسة عمل تشفير. تتمثل الخطوة التالية في تبادل المفاتيح العامة مع كل موجه آخر. يمكنك إدخال هذه المفاتيح العامة يدويا من خلال إدخال الأمر **show crypto mypubkey** أولا لعرض مفتاح DSS الخاص بالموجه. ثم تقوم بتبادل هذه المفاتيح العامة (عبر البريد الإلكتروني، على سبيل المثال)، و، باستخدام أمر DSS الخاص بسلسلة **مفتاح التشفير** الرئيسي، قم بقص المفتاح العام لموجه النظير ولصقه في الموجه.

يمكنك أيضا إستخدام الأمر **crypto key exchange dss** لجعل الموجهات تتبادل المفاتيح العامة تلقائيا. إذا كنت تستخدم الطريقة المؤتمتة، فتأكد من عدم وجود عبارات **خريطة التشفير** على الواجهات المستخدمة لتبادل المفاتيح. يفيد **مفتاح تشفير تصحيح الأخطاء** هنا.

ملاحظة: إنها لفكرة جيدة أن تقوم **بإختبار اتصال** نظيرك قبل محاولة تبادل المفاتيح.

```
Loser#ping 19.19.19.20

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds
!!!!!

Loser(config)#crypto key exchange dss passive
.Enter escape character to abort if connection does not complete
[Wait for connection from peer[confirm
.... Waiting


StHelen(config)#crypto key exchange dss 19.19.19.19 barney
:Public key for barney
Serial Number 05694352
Fingerprint   309E D1DE B6DA 5145 D034

[Wait for peer to send a key[confirm


:Public key for barney
```

```
                                        Serial Number 05694352
                                Fingerprint   309E D1DE B6DA 5145 D034

                        Add this public key to the configuration? [yes/no]:yes


                        .Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes
                        .Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes
                        .Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes
                       .Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes


                             .Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes
                             .Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes
                             .Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes
                             .Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes
                            .Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes
                            .Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes

                                        [Send peer a key in return[confirm
                                                        ?Which one

                                                             :[fred? [yes
                                                    :Public key for fred
                                                  Serial Number 02802219
                                        Fingerprint   2963 05F9 ED55 576D CF9D


                                                     .... Waiting
                                                :Public key for fred
                                              Serial Number 02802219
                                    Fingerprint   2963 05F9 ED55 576D CF9D

                        :[Add this public key to the configuration? [yes/no

                                                                #(Loser(config
                                   .Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes
                                   .Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes
                                   .Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes
                                   .Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes
                                  .Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes
                                                #(Loser(config

                                   .Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes
                                   .Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes
                                   .Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes
                                   .Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes
                                  .Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes
                                  .Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes
                        Add this public key to the configuration? [yes/no]: yes
                                                StHelen(config)#^Z
                                                        #StHelen
```

الآن بعد تبادل مفاتيح DSS العامة، تأكد من أن كلا الموجهين يحتويان على المفاتيح العامة الخاصة ببعضهما البعض ومن أنهما متطابقين، كما هو موضح في إخراج الأمر أدناه.

```
                                                Loser#show crypto key mypubkey dss
                                                   crypto public-key fred 02802219
                 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
                 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
                                                                                quit

                                                Loser#show crypto key pubkey-chain dss
```

```
                                        crypto public-key barney 05694352
B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
                                                              quit

                                                        --------

                                     StHelen#show crypto key mypubkey dss
                                        crypto public-key barney 05694352
B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
                                                              quit

                                  StHelen#show crypto key pubkey-chain dss
                                        crypto public-key fred 02802219
79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
                                                              quit
```

النموذج 1: تكوين Cisco IOS للارتباط المخصص

بعد إنشاء مفاتيح DSS على كل موجه وتبادل مفاتيح DSS العامة، يمكن تطبيق أمر **خريطة التشفير** على الواجهة. تبدأ جلسة التشفير بإنشاء حركة مرور تطابق قائمة الوصول المستخدمة بواسطة خرائط التشفير.

```
                                     Loser#write terminal
                                  ...Building configuration

                                     :Current configuration
                                                              !
                  Last configuration change at 13:01:18 UTC Mon Mar 16 1998 !
                  NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998 !
                                                              !
                                                   version 11.3
                                 service timestamps debug datetime msec
                                        no service password-encryption
                                                              !
                                                 hostname Loser
                                                              !
                               enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
                                                              !
                                                    ip subnet-zero
                                                 no ip domain-lookup
                                               crypto map oldstyle 10
                                                     set peer barney
                                                  match address 133
                                                              !
                                            crypto key pubkey-chain dss
                                                      named-key barney
                                                 serial-number 05694352
                                                          key-string
B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
                                                              quit
                                                              !
                                                   interface Ethernet0
                                          ip address 40.40.40.41 255.255.255.0
                                                 no ip mroute-cache
                                                              !
                                                    interface Serial0
                                          ip address 18.18.18.18 255.255.255.0
                                                  encapsulation ppp
                                                 no ip mroute-cache
```

```
                                                                shutdown
                                                                    !
                                                        interface Serial1
                                                ip address 19.19.19.19 255.255.255.0
                                                        encapsulation ppp
                                                    no ip mroute-cache
                                                        clockrate 2400
                                                        no cdp enable
                                                    crypto map oldstyle
                                                                    !
                                            ip default-gateway 10.11.19.254
                                                        ip classless
                                            ip route 0.0.0.0 0.0.0.0 19.19.19.20
        access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
                                                                    !
                                                            line con 0
                                                    exec-timeout 0 0
                                                            line aux 0
                                                              no exec
                                                transport input all
                                                            line vty 0 4
                                                            password ww
                                                                  login
                                                                    !
                                                                  end

                                                            #Loser
                                                ---------------------------

                                                    StHelen#write terminal
                                                ...Building configuration

                                                    :Current configuration
                                                                    !
                        Last configuration change at 13:03:05 UTC Mon Mar 16 1998 !
                        NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998 !
                                                                    !
                                                            version 11.3
                                            service timestamps debug datetime msec
                                                    no service password-encryption
                                                                    !
                                                        hostname StHelen
                                                                    !
                                                boot system flash c2500-is56-l
                                                        enable password ww
                                                                    !
                                                    partition flash 2 8 8
                                                                    !
                                                      no ip domain-lookup
                                                    crypto map oldstyle 10
                                                            set peer fred
                                                       match address 144
                                                                    !
                                                crypto key pubkey-chain dss
                                                            named-key fred
                                                   serial-number 02802219
                                                                key-string
        79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
        C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
                                                                    quit
                                                                        !
                                                                        !
                                                            interface Ethernet0
                                                ip address 30.30.30.31 255.255.255.0
```

```
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 encapsulation x25
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 compress stac
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.19
access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

#StHelen
```

النموذج 2: تكوين IOS لترحيل الإطارات متعدد النقاط من Cisco

تم أخذ إخراج الأمر العينة التالية من موجه الموزع.

```
Loser#write terminal
...Building configuration

:Current configuration
!
Last configuration change at 10:45:20 UTC Wed Mar 11 1998 !
NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998 !
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
!
crypto map oldstuff 10
 set peer barney
```

```
                                                    match address 133
                                                crypto map oldstuff 20
                                                       set peer wilma
                                                    match address 144
                                                                    !
                                               crypto key pubkey-chain dss
                                                         named-key barney
                                                   serial-number 05694352
                                                                key-string
1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D
                                                                     quit
                                                          named-key wilma
                                                   serial-number 01496536
                                                                key-string
C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70 7B29279C
E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939
                                                                     quit
                                                                     !
                                            crypto cisco pregen-dh-pairs 5
                                                                     !
                                             crypto cisco key-timeout 1440
                                                                     !
                                                        interface Ethernet0
                                     ip address 190.190.190.190 255.255.255.0
                                                    no ip mroute-cache
                                                                     !
                                                      interface Serial1
                                         ip address 19.19.19.19 255.255.255.0
                                                  encapsulation frame-relay
                                                    no ip mroute-cache
                                                      clockrate 500000
                                                 crypto map oldstuff
                                                                     !
                                                                     !
                                            ip default-gateway 10.11.19.254
                                                                ip classless
                               ip route 200.200.200.0 255.255.255.0 19.19.19.20
                               ip route 210.210.210.0 255.255.255.0 19.19.19.21
 access-list 133 permit ip 190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255
 access-list 144 permit ip 190.190.190.0 0.0.0.255 210.210.210.0 0.0.0.255
                                                                     !
                                                              line con 0
                                                    exec-timeout 0 0
                                                              line aux 0
                                                                no exec
                                                 transport input all
                                                              line vty 0 4
                                                              password ww
                                                                    login
                                                                     !
                                                                   end

                                                                #Loser
```

تم أخذ إخراج الأمر العينة التالية من الموقع البعيد A.

```
                                                  WAN-2511a#write terminal
                                                ...Building configuration

                                                  :Current configuration
                                                                     !
                                                              version 11.3
```

```
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
set peer fred
match address 133
!
crypto key pubkey-chain dss
named-key fred
serial-number 02802219
key-string
4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D 56841777
D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
quit
!
interface Ethernet0
ip address 210.210.210.210 255.255.255.0
shutdown
!
interface Serial0
ip address 19.19.19.21 255.255.255.0
encapsulation frame-relay
no fair-queue
crypto map mymap
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
exec-timeout 0 0
line 1
no exec
transport input all
line 2 16
no exec
line aux 0
line vty 0 4
password ww
login
!
end

#WAN-2511a
```

تم أخذ إخراج الأمر العينة التالية من الموقع البعيد B.

```
StHelen#write terminal
...Building configuration

:Current configuration
!
Last configuration change at 19:00:34 UTC Tue Mar 10 1998 !
NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998 !
!
version 11.3
service timestamps debug datetime msec
```

```
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
set peer fred
match address 144
!
crypto key pubkey-chain dss
named-key fred
serial-number 02802219
key-string
4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D 56841777
D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
quit
!
interface Ethernet0
ip address 200.200.200.200 255.255.255.0
!
interface Serial1
ip address 19.19.19.20 255.255.255.0
encapsulation frame-relay
no ip mroute-cache
crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
exec-timeout 0 0
line aux 0
transport input all
line vty 0 4
password ww
login
!
end

#StHelen
```

تم أخذ إخراج الأمر العينة التالية من محول ترحيل الإطارات.

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
```

```
frame-relay switching
!
interface Serial0
no ip address
encapsulation frame-relay
clockrate 500000
frame-relay intf-type dce
frame-relay route 200 interface Serial1 100
!
interface Serial1
no ip address
encapsulation frame-relay
frame-relay intf-type dce
frame-relay route 100 interface Serial0 200
frame-relay route 300 interface Serial2 200
!
interface Serial2
no ip address
encapsulation frame-relay
clockrate 500000
frame-relay intf-type dce
frame-relay route 200 interface Serial1 300
!
```

النموذج 3: التشفير إلى موجه ومن خلاله

لا يجب أن تكون موجهات النظير على بعد خطوة واحدة. أنت يستطيع خلقت نظرة جلسة مع مسحاج تخديد بعيد. في المثال التالي، الهدف هو تشفير جميع حركة مرور الشبكة بين 24/180.180.180.0 و 24/40.40.40.0 وبين 24/180.180.180.0 و 24/30.30.30.0. لا يوجد أي اهتمام بتشفير حركة المرور بين 24/40.40.40.0 و 24/30.30.30.0.

يحتوي الموجه WAN-4500b على اقتران جلسة عمل تشفير مع Loser وأيضا مع StHelen. من خلال تشفير حركة المرور من جزء إيثرنت الخاص بشبكة WAN-4500b إلى جزء إيثرنت من شركة StHelen، يمكنك تجنب خطوة فك التشفير غير الضرورية عند Ser. أما الخاسر فيمرر ببساطة حركة المرور المشفرة إلى واجهة StHelen التسلسلية، حيث يتم فك تشفيرها. وهذا يقلل من تأخر حركة المرور لحزم IP ودورات وحدة المعالجة المركزية (CPU) على خادم الموجه. والأهم من ذلك، أنه يزيد من أمن النظام إلى حد كبير، حيث أن مدور التنصت في شركة Ser لا يستطيع قراءة حركة المرور. إذا قام "الخاسر" بفك تشفير حركة المرور، فسيكون من المحتمل تحويل البيانات التي تم فك تشفيرها.

```
[wan-4500b]<Ser0>--   ---<Ser0> [Loser] <Ser1>--   ----<Ser1>[StHelen]
|                          |                          |
|                          |                          |
-------                    -------                    -----
30.30.30/24                40.40.40/24                180.180.180/24
```

```
wan-4500b#write terminal
...Building configuration

:Current configuration
!
version 11.3
no service password-encryption
!
hostname wan-4500b
!
enable password 7 111E0E
!
username cse password 0 ww
no ip domain-lookup
!
crypto map toworld 10
```

```
                                                    set peer loser
                                                  match address 133
                                               crypto map toworld 20
                                                   set peer sthelen
                                                  match address 144
                                                                  !
                                            crypto key pubkey-chain dss
                                                      named-key loser
                                                 serial-number 02802219
                                                          key-string
F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
                                                                  quit
                                                    named-key sthelen
                                                 serial-number 05694352
                                                          key-string
5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
                                                                  quit
                                                                     !
                                                  interface Ethernet0
                                       ip address 180.180.180.180 255.255.255.0
                                                                  !
                                                   interface Serial0
                                          ip address 18.18.18.19 255.255.255.0
                                                  encapsulation ppp
                                                crypto map toworld
                                                                  !
                                                          router rip
                                                   network 18.0.0.0
                                                network 180.180.0.0
                                                                  !
                                                        ip classless
                                           ip route 0.0.0.0 0.0.0.0 30.30.30.31
                                 ip route 171.68.118.0 255.255.255.0 10.11.19.254
    access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255
    access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255
                                                                  !
                                                          line con 0
                                                   exec-timeout 0 0
                                                          line aux 0
                                                 password 7 044C1C
                                                        line vty 0 4
                                                        login local
                                                                  !
                                                                end

                                                          #wan-4500b

                                                --------------------

                                                     Loser#write terminal
                                                ...Building configuration

                                                    :Current configuration
                                                                  !
                        Last configuration change at 11:01:54 UTC Wed Mar 18 1998 !
                        NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998 !
                                                                  !
                                                         version 11.3
                                           service timestamps debug datetime msec
                                                  no service password-encryption
                                                                  !
                                                       hostname Loser
```

```
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
ip host StHelen.cisco.com 19.19.19.20
ip domain-name cisco.com
!
crypto map towan 10
set peer wan
match address 133
!
crypto key pubkey-chain dss
named-key wan
serial-number 07365004
key-string
A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit
!
interface Ethernet0
ip address 40.40.40.40 255.255.255.0
no ip mroute-cache
!
interface Serial0
ip address 18.18.18.18 255.255.255.0
encapsulation ppp
no ip mroute-cache
clockrate 64000
crypto map towan
!
interface Serial1
ip address 19.19.19.19 255.255.255.0
encapsulation ppp
no ip mroute-cache
priority-group 1
clockrate 64000
!
!
router rip
network 19.0.0.0
network 18.0.0.0
network 40.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
exec-timeout 0 0
line aux 0
no exec
transport input all
line vty 0 4
password ww
login
!
end

#Loser

-------------------------

StHelen#write terminal
```

```
...Building configuration

:Current configuration
!
Last configuration change at 11:13:18 UTC Wed Mar 18 1998 !
NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998 !
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map towan 10
set peer wan
match address 144
!
crypto key pubkey-chain dss
named-key wan
serial-number 07365004
key-string
A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit
!
interface Ethernet0
no ip address
!
interface Ethernet1
ip address 30.30.30.30 255.255.255.0
!
interface Serial1
ip address 19.19.19.20 255.255.255.0
encapsulation ppp
no ip mroute-cache
load-interval 30
crypto map towan
!
router rip
network 30.0.0.0
network 19.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
exec-timeout 0 0
line aux 0
transport input all
line vty 0 4
password ww
login
!
end

#StHelen
```

```
                                                  -------------------------

                                                wan-4500b#show crypto cisco algorithms
                                                                     des cfb-64
                                                                  40-bit-des cfb-64

                                                wan-4500b#show crypto cisco key-timeout
                                             Session keys will be re-negotiated every 30 minutes

                                                wan-4500b#show crypto cisco pregen-dh-pairs
                                                      Number of pregenerated DH pairs: 0

                                                wan-4500b#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
   Serial0         18.18.18.19 set    DES_56_CFB64    1683     1682    1
   Serial0         18.18.18.19 set    DES_56_CFB64    1693     1693    5

                                             wan-4500b#show crypto engine connections dropped-packet
                                                       Interface            IP-Address    Drop Count

                                                            Serial0             18.18.18.19   52
                                                wan-4500b#show crypto engine configuration
                                                                        slot:              0
                                                                   engine name:        wan
                                                               engine type:        software
                                                               serial number:      07365004
                                                          platform:           rp crypto engine
                                                                    crypto lib version: 10.0.0

                                                                     :Encryption Process Info
                                                                      input queue top:    303
                                                                      input queue bot:    303
                                                                        input queue count:  0

                                                wan-4500b#show crypto key mypubkey dss
                                                                      crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
                                                                                                quit

                                                wan-4500b#show crypto key pubkey-chain dss
                                                                   crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
                                                                                                quit
                                                                 crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
                                                                                                quit

                                                wan-4500b#show crypto map interface serial 1
                                                                     .No crypto maps found

                                                                        wan-4500b#show crypto map
                                                                    Crypto Map "toworld" 10 cisco
                                          (Connection Id = 1        (1 established,    0 failed
                                                                              Peer = loser
                                                                         PE = 180.180.180.0
                                                                           UPE = 40.40.40.0
                                                                    Extended IP access list 133
                                                                   access-list 133 permit ip
                                                 source: addr = 180.180.180.0/0.0.0.255
                                                    dest:   addr = 40.40.40.0/0.0.0.255
```

```
                                        Crypto Map "toworld" 20 cisco
        (Connection Id = 5       (1 established,    0 failed
                                             Peer = sthelen
                                          PE = 180.180.180.0
                                            UPE = 30.30.30.0
                                       Extended IP access list 144
                                     access-list 144 permit ip
                  source: addr = 180.180.180.0/0.0.0.255
                     dest:   addr = 30.30.30.0/0.0.0.255

                                                                #wan-4500b

                                                ------------------------

                                          Loser#show crypto cisco algorithms
                                                              des cfb-64
                                                               des cfb-8
                                                         40-bit-des cfb-64
                                                          40-bit-des cfb-8

                                          Loser#show crypto cisco key-timeout
                                    Session keys will be re-negotiated every 30 minutes

                                       Loser#show crypto cisco pregen-dh-pairs
                                          Number of pregenerated DH pairs: 10

                                    Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
   Serial0         18.18.18.18 set    DES_56_CFB64    1683     1682   61

                                    Loser#show crypto engine connections dropped-packet
                                          Interface            IP-Address    Drop Count

                                             Serial0              18.18.18.18   1
                                            Serial1              19.19.19.19   90
                                           Loser#show crypto engine configuration
                                                        slot:               0
                                                   engine name:        loser
                                                engine type:        software
                                                serial number:      02802219
                                             platform:           rp crypto engine
                                                      crypto lib version: 10.0.0

                                                       :Encryption Process Info
                                                        input queue top:    235
                                                        input queue bot:    235
                                                          input queue count:  0

                                          Loser#show crypto key mypubkey dss
                                            crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
                                                                        quit

                                          Loser#show crypto key pubkey-chain dss
                                                  crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
                                                                        quit

                                       Loser#show crypto map interface serial 1
                                                        .No crypto maps found
```

```
                                                    Loser#show crypto map
                                                  Crypto Map "towan" 10 cisco
              (Connection Id = 61       (0 established,    0 failed
                                                      Peer = wan
                                                   PE = 40.40.40.0
                                                  UPE = 180.180.180.0
                                               Extended IP access list 133
                                             access-list 133 permit ip
                                  source: addr = 40.40.40.0/0.0.0.255
                                dest:   addr = 180.180.180.0/0.0.0.255

                                                                    #Loser

                                ----------------------------------------

                                     StHelen#show crypto cisco algorithms
                                                          des cfb-64

                                    StHelen#show crypto cisco key-timeout
                                  Session keys will be re-negotiated every 30 minutes

                                          StHelen#show crypto cisco pregen-dh-pairs
                                            Number of pregenerated DH pairs: 10

                                   StHelen#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
   Serial1         19.19.19.20 set    DES_56_CFB64    1694     1693   58

                         StHelen#show crypto engine connections dropped-packet
                                 Interface           IP-Address    Drop Count

                                     Ethernet0           0.0.0.0       1
                                    Serial1             19.19.19.20   80
                                 StHelen#show crypto engine configuration
                                               slot:               0
                                         engine name:        sthelen
                                        engine type:        software
                                        serial number:      05694352
                                    platform:           rp crypto engine
                                             crypto lib version: 10.0.0

                                               :Encryption Process Info
                                                input queue top:    220
                                                input queue bot:    220
                                                  input queue count:  0

                                     StHelen#show crypto key mypubkey dss
                                       crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
                                                                    quit

                                    StHelen#show crypto key pubkey-chain dss
                                                 crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
                                                                    quit

                                  StHelen#show crypto map interface serial 1
                                                  Crypto Map "towan" 10 cisco
              (Connection Id = 58       (1 established,    0 failed
                                                      Peer = wan
                                                   PE = 30.30.30.0
```

```
                                                    UPE = 180.180.180.0
                                                Extended IP access list 144
                                            access-list 144 permit ip
                                    source: addr = 30.30.30.0/0.0.0.255
                                dest:   addr = 180.180.180.0/0.0.0.255

                                                        StHelen#show crypto map
                                                    Crypto Map "towan" 10 cisco
                            (Connection Id = 58       (1 established,    0 failed
                                                             Peer = wan
                                                        PE = 30.30.30.0
                                                    UPE = 180.180.180.0
                                                Extended IP access list 144
                                            access-list 144 permit ip
                                    source: addr = 30.30.30.0/0.0.0.255
                                dest:   addr = 180.180.180.0/0.0.0.255

#StHelen
```

النموذج 4: تشفير باستخدام DDR

نظرا لأن Cisco IOS تعتمد على ICMP لإنشاء جلسات تشفير، يجب تصنيف حركة مرور ICMP على أنها "مثيرة للاهتمام" في قائمة المتصل عند إجراء تشفير عبر إرتباط DDR.

ملاحظة: يعمل الضغط في الإصدار 11.3 من برنامج Cisco IOS Software، ولكنه ليس مستخدم جدا للبيانات المشفرة. لأن البيانات المشفرة تبدو عشوائية إلى حد ما، الضغط فقط يبطئ الأمور. ولكن يمكنك ترك الميزة قيد التشغيل لحركة المرور غير المشفرة.

في بعض الحالات، ستحتاج إلى النسخ الاحتياطي للطلب على الموجه نفسه. على سبيل المثال، فإنه يستخدم الوقود عندما يريد المستخدمون الحماية من فشل رابط معين في شبكات WAN الخاصة بهم. إذا ذهبت واجهتان إلى النظير نفسه، يمكن إستخدام خريطة التشفير نفسها على كلا الواجهات. يجب إستخدام واجهة النسخ الاحتياطي حتى تعمل هذه الميزة بشكل صحيح. إذا كان لتصميم النسخ الاحتياطي طلب موجه في مربع مختلف، فيجب إنشاء خرائط تشفير مختلفة وتعيين الأقران وفقا لذلك. مرة أخرى، يجب إستخدام أمر **واجهة النسخ الاحتياطي**.

```
                                                        dial-5#write terminal
                                                    ...Building configuration

                                                       :Current configuration
                                                                              !
                                                                   version 11.3
                                                no service password-encryption
                                                     service udp-small-servers
                                                     service tcp-small-servers
                                                                              !
                                                              hostname dial-5
                                                                              !
                                            boot system c1600-sy56-l 171.68.118.83
                                        enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10
                                                                              !
                                                 username dial-6 password 0 cisco
                                                       isdn switch-type basic-ni1
                                                                              !
                                                         crypto map dial6 10
                                                             set peer dial6
                                                          match address 133
                                                                              !
                                                crypto key pubkey-chain dss
                                                           named-key dial6
                                                  serial-number 05679987
                                                               key-string
```

```
753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82
2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C
                                                                quit
                                                                   !
                                                    interface Ethernet0
                                          ip address 20.20.20.20 255.255.255.0
                                                                   !
                                                         interface BRI0
                                          ip address 10.10.10.11 255.255.255.0
                                                       encapsulation ppp
                                                     no ip mroute-cache
                                                       load-interval 30
                                                 dialer idle-timeout 9000
                                      dialer map ip 10.10.10.10 name dial-6 4724118
                                                    dialer hold-queue 40
                                                         dialer-group 1
                                               isdn spid1 919472417100 4724171
                                               isdn spid2 919472417201 4724172
                                                       compress stac
                                             ppp authentication chap
                                                       ppp multilink
                                                  crypto map dial6
                                                                   !
                                                        ip classless
                                       ip route 40.40.40.0 255.255.255.0 10.10.10.10
             access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255
                                               dialer-list 1 protocol ip permit
                                                                   !
                                                          line con 0
                                                     exec-timeout 0 0
                                                          line vty 0 4
                                                          password ww
                                                                login
                                                                   !
                                                              end

                                                           dial-5#

                                                    ----------------------

                                                       dial-6#write terminal
                                                  ...Building configuration

                                                    :Current configuration
                                                                   !
                                                             version 11.3
                                           no service password-encryption
                                                service udp-small-servers
                                                service tcp-small-servers
                                                                   !
                                                       hostname dial-6
                                                                   !
                                              boot system c1600-sy56-l 171.68.118.83
                                      .enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc
                                                                   !
                                               username dial-5 password 0 cisco
                                                        no ip domain-lookup
                                                isdn switch-type basic-ni1
                                                                   !
                                                      crypto map dial5 10
                                                           set peer dial5
                                                        match address 144
                                                                   !
                                                   crypto key pubkey-chain dss
```

```
                                                named-key dial5
                                            serial-number 05679919
                                                    key-string
160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
                                                        quit
                                                            !
                                                            !
                                                interface Ethernet0
                                        ip address 40.40.40.40 255.255.255.0
                                                            !
                                                    interface BRI0
                                        ip address 10.10.10.10 255.255.255.0
                                                encapsulation ppp
                                               no ip mroute-cache
                                            dialer idle-timeout 9000
                                    dialer map ip 10.10.10.11 name dial-5 4724171
                                                dialer hold-queue 40
                                        dialer load-threshold 5 outbound
                                                    dialer-group 1
                                        isdn spid1 919472411800 4724118
                                        isdn spid2 919472411901 4724119
                                                compress stac
                                        ppp authentication chap
                                                ppp multilink
                                            crypto map dial5
                                                            !
                                                ip classless
                                    ip route 20.20.20.0 255.255.255.0 10.10.10.11
                    access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255
                                        dialer-list 1 protocol ip permit
                                                            !
                                                  line con 0
                                           exec-timeout 0 0
                                                line vty 0 4
                                               password ww
                                                      login
                                                            !
                                                        end

                                                dial-6#
```

النموذج 5: تشفير حركة مرور IPX في نفق IP

في هذا المثال، يتم تشفير حركة مرور IPX في نفق IP.

ملاحظة: يتم تشفير حركة مرور البيانات فقط في هذا النفق (IPX). يتم ترك جميع حركة مرور IP الأخرى وحدها.

```
                                                WAN-2511a#write terminal
                                               ...Building configuration

                                                  :Current configuration
                                                            !
                                                    version 11.2
                                        no service password-encryption
                                          no service udp-small-servers
                                          no service tcp-small-servers
                                                            !
                                                hostname WAN-2511a
                                                            !
                                                enable password ww
                                                            !
```

```
                                                    no ip domain-lookup
                                                ipx routing 0000.0c34.aa6a
                                                                      !
                                            crypto public-key wan2516 01698232
        B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
        B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
                                                                         quit
                                                                      !
                                                        crypto map wan2516 10
                                                            set peer wan2516
                                                          match address 133
                                                                      !
                                                                      !
                                                      interface Loopback1
                                                ip address 50.50.50.50 255.255.255.0
                                                                      !
                                                        interface Tunnel1
                                                           no ip address
                                                         ipx network 100
                                                tunnel source 50.50.50.50
                                             tunnel destination 60.60.60.60
                                                      crypto map wan2516
                                                                      !
                                                      interface Ethernet0
                                                ip address 40.40.40.40 255.255.255.0
                                                         ipx network 600
                                                                      !
                                                       interface Serial0
                                                ip address 20.20.20.21 255.255.255.0
                                                       encapsulation ppp
                                                      no ip mroute-cache
                                                      crypto map wan2516
                                                                      !
                                                       interface Serial1
                                                           no ip address
                                                                shutdown
                                                                      !
                                             ip default-gateway 10.11.19.254
                                                                ip classless
                                           ip route 0.0.0.0 0.0.0.0 20.20.20.20
                                access-list 133 permit ip host 50.50.50.50 host 60.60.60.60
                                                                      !
                                                                line con 0
                                                          exec-timeout 0 0
                                                               password ww
                                                                     login
                                                                line 1 16
                                                              line aux 0
                                                               password ww
                                                                     login
                                                              line vty 0 4
                                                               password ww
                                                                     login
                                                                      !
                                                                    end

                                                                 #WAN-2511a

                                                        ------------------------

                                                       WAN-2516a#write terminal
                                                      ...Building configuration

                                                        :Current configuration
```

```
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname WAN-2516a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c3b.cc1e
!
crypto public-key wan2511 01496536
C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
quit
!
crypto map wan2511 10
set peer wan2511
match address 144
!
!
hub ether 0 1
link-test
auto-polarity
!
<other hub interfaces snipped> !
!
hub ether 0 14
link-test
auto-polarity
!
interface Loopback1
ip address 60.60.60.60 255.255.255.0
!
interface Tunnel1
no ip address
ipx network 100
tunnel source 60.60.60.60
tunnel destination 50.50.50.50
crypto map wan2511
!
interface Ethernet0
ip address 30.30.30.30 255.255.255.0
ipx network 400
!
interface Serial0
ip address 20.20.20.20 255.255.255.0
encapsulation ppp
clockrate 2000000
crypto map wan2511
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
shutdown
!
ip default-gateway 20.20.20.21
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit ip host 60.60.60.60 host 50.50.50.50
access-list 188 permit gre any any
!
line con 0
exec-timeout 0 0
password ww
login
line aux 0
password ww
login
modem InOut
transport input all
flowcontrol hardware
line vty 0 4
password ww
login
!
end

#WAN-2516a
-----------------------

WAN-2511a#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
S - Static, F - Floating static, L - Local (internal), W - IPXWAN
R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
s - seconds, u - uses

.Total IPX routes. Up to 1 parallel paths and 16 hops allowed 3

.No default route known

C        100 (TUNNEL),        Tu1
C        600 (NOVELL-ETHER),  Et0
R        400 [151/01] via      100.0000.0c3b.cc1e,   24s, Tu1


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
Serial0         20.20.20.21 set    DES_56_CFB64    207      207    1


WAN-2511a#ping 400.0000.0c3b.cc1e
"Translating "400.0000.0c3b.cc1e

.Type escape sequence to abort
:Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
Serial0         20.20.20.21 set    DES_56_CFB64    212      212    1


WAN-2511a#ping 30.30.30.30

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

```
WAN-2511a#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
    Serial0         20.20.20.21 set    DES_56_CFB64    212      212    1

#WAN-2511a
```

نموذج 6: تشفير أنفاق L2F

في هذا المثال، تتم محاولة تشفير حركة مرور L2F فقط للمستخدمين الذين يقومون بالاتصال. هنا، يتصل "user@cisco.com" بخادم الوصول إلى الشبكة المحلي (NAS) المسمى "Demo2" في مدينتهم ويتم إنشاء قنوات له على القرص المضغوط الخاص بالبوابة الرئيسية. يتم تشفير جميع حركة مرور الإصدار التجريبي 2 (بالإضافة إلى حركة مرور متصلين آخرين من المستوى الثاني). نظرا لأن L2F يستخدم منفذ UDP 1701، فهذه هي الطريقة التي يتم بها إنشاء قائمة الوصول، لتحديد حركة المرور التي يتم تشفيرها.

ملاحظة: إذا لم يتم إعداد اقتران التشفير بالفعل، مما يعني أن المتصل هو أول شخص يتم الاتصال به وإنشاء نفق L2F، فقد يتم إسقاط المتصل بسبب التأخير في إعداد اقتران التشفير. قد لا يحدث ذلك على الموجهات التي تحتوي على طاقة كافية لوحدة المعالجة المركزية (CPU). كما قد ترغب في زيادة **مهلة المفتاح** بحيث يحدث إعداد التشفير وإبطاله فقط أثناء ساعات الذروة.

تم أخذ إخراج الأمر العينة التالية من وحدة التخزين المتصلة بالشبكة (NAS) البعيدة.

```
DEMO2#write terminal
...Building configuration

:Current configuration
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname DEMO2
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
no ip domain-lookup
vpdn enable
vpdn outgoing cisco.com NAS1 ip 20.20.20.20
!
crypto public-key wan2516 01698232
B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit
!
crypto map vpdn 10
 set peer wan2516
match address 133
!
crypto key-timeout 1440
!
interface Ethernet0
ip address 40.40.40.40 255.255.255.0
!
 interface Serial0
ip address 20.20.20.21 255.255.255.0
encapsulation ppp
```

```
 no ip mroute-cache
    crypto map vpdn
                  !
  interface Serial1
     no ip address
          shutdown
                  !
interface Group-Async1
          no ip address
    encapsulation ppp
 async mode dedicated
no peer default ip address
          no cdp enable
ppp authentication chap pap
      group-range 1 16
                  !
ip default-gateway 10.11.19.254
               ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit udp host 20.20.20.21 eq 1701
      host 20.20.20.20 eq 1701
                  !
                  !
        line con 0
   exec-timeout 0 0
        password ww
               login
          line 1 16
        modem InOut
 transport input all
         speed 115200
 flowcontrol hardware
          line aux 0
        login local
        modem InOut
 transport input all
 flowcontrol hardware
        line vty 0 4
        password ww
               login
                  !
                end

DEMO2#
```

تم أخذ إخراج الأمر العينة التالية من البوابة الرئيسية.

```
CD#write terminal
...Building configuration

:Current configuration
                  !
           version 11.2
        no service pad
no service password-encryption
     service udp-small-servers
     service tcp-small-servers
                  !
         hostname CD
                  !
    enable password ww
                  !
username NAS1 password 0 SECRET
```

```
username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco
no ip domain-lookup
vpdn enable
vpdn incoming NAS1 HomeGateway virtual-template 1
!
crypto public-key wan2511 01496536
C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
quit
!
crypto key-timeout 1440
!
crypto map vpdn 10
set peer wan2511
match address 144
!
!
hub ether 0 1
link-test
auto-polarity
!
interface Loopback0
ip address 70.70.70.1 255.255.255.0
!
interface Ethernet0
ip address 30.30.30.30 255.255.255.0
!
interface Virtual-Template1
ip unnumbered Loopback0
no ip mroute-cache
peer default ip address pool default
ppp authentication chap
!
interface Serial0
ip address 20.20.20.20 255.255.255.0
encapsulation ppp
clockrate 2000000
crypto map vpdn
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
shutdown
!
ip local pool default 70.70.70.2 70.70.70.77
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit udp host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701
!
line con 0
exec-timeout 0 0
password ww
login
line aux 0
password ww
login
modem InOut
transport input all
flowcontrol hardware
```

```
line vty 0 4
password ww
 login
!
end
```

استكشاف الأخطاء وإصلاحها

بشكل عام، من الأفضل أن تبدأ كل جلسة أستكشاف الأخطاء وإصلاحها عن طريق تجميع المعلومات باستخدام أوامر **show** التالية. تشير العلامة النجمية (*) إلى أمر مفيد بشكل خاص. يرجى أيضا الاطلاع على أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها للحصول على معلومات إضافية.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

الأوامر	
إظهار خوارزميات Cisco التشفير	show crypto cisco key-timeout
show crypto cisco pregen-dh-pairs	* إظهار إتصالات محركات التشفير النشطة
show crypto engine connections drop-packet	show crypto engine configuration
show crypto key mypubkey dss	* إظهار DSS سلسلة مفاتيح العانة للتشفير
show crypto map interface serial 1	* إظهار خريطة التشفير
محرك تصحيح الأخطاء المشفرة	* تصحيح أخطاء التشفير
مفتاح تصحيح الأخطاء	مسح اتصال التشفير
أصفار التشفير	لا يوجد مفتاح عام تشفير

- **إظهار خوارزميات Cisco التشفير**- يجب تمكين جميع خوارزميات معيار تشفير البيانات (DES) التي يتم إستخدامها للاتصال مع أي موجه تشفير نظير آخر. إذا لم تقم بتمكين خوارزمية DES، فلن تتمكن من إستخدام هذه الخوارزمية، حتى إذا حاولت تعيين الخوارزمية إلى **خريطة تشفير** في وقت لاحق.إذا حاول الموجه الخاص بك إعداد جلسة اتصال مشفرة باستخدام موجه نظير، ولم يتضمن الموجهان نفس خوارزمية DES الممكنة في كلا النهايتين، فإن الجلسة المشفرة تفشل. في حالة تمكين خوارزمية DES مشتركة واحدة على الأقل في كلا النهايتين، يمكن متابعة الجلسة المشفرة.**ملاحظة:** تظهر الكلمة الإضافية من Cisco IOS في الإصدار 11.3 من برنامج Cisco IOS والمطلوبة للتمييز بين تشفير IPSec وتشفير Cisco الخاص الموجود في برنامج Cisco IOS الإصدار 11.2.

```
Loser#show crypto cisco algorithms
        des cfb-64
        des cfb-8
    40-bit-des cfb-64
    40-bit-des cfb-8
```

- **show crypto cisco key-timeout** - بعد إنشاء جلسة اتصال مشفرة، تكون صالحة لفترة زمنية محددة. وبعد هذا الطول من الوقت، تنتهي مدة الجلسة. يجب التفاوض على جلسة جديدة، ويجب إنشاء مفتاح DES (جلسة) جديد لمتابعة الاتصال المشفر. أستخدم هذا الأمر لتغيير الوقت الذي تستمر فيه جلسة الاتصال المشفرة قبل انتهاء صلاحيتها (عدد المرات خارج).

```
Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes
```

أستخدم هذه الأوامر لتحديد طول الوقت قبل إعادة التفاوض على مفاتيح DES.

```
StHelen#show crypto conn
```

```
                                                    Connection Table
                    PE              UPE         Conn_id New_id Algorithm    Time
DES_56_CFB64 Mar 01 1993 03:16:09      0    4        0.0.0.1         0.0.0.1
                                             flags:TIME_KEYS


                                                StHelen#show crypto key
                                    Session keys will be re-negotiated every 30 minutes

                                                StHelen#show clock
                                                *UTC Mon Mar 1 1993 03:21:23.031
```

- **show crypto cisco pregen-dh-pairs** - تستخدم كل جلسة مشفرة زوج فريد من أرقام DH. في كل مرة يتم إنشاء جلسة عمل جديدة، يجب إنشاء أزواج أرقام DH جديدة. عند اكتمال الجلسة، يتم تجاهل هذه الأرقام. يعد إنشاء أزواج أرقام DH الجديدة نشاطا كثيف لوحدة المعالجة المركزية (CPU)، والذي يمكن أن يجعل إعداد الجلسة بطيئا، وخاصة للموجهات الطرفية المنخفضة.لتسريع إعداد جلسة العمل، يمكنك إختيار أن يكون لديك مقدار محدد من أزواج أرقام DH تم إنشاؤها مسبقا والاحتفاظ بها في الحجز. ثم، عندما يتم إعداد جلسة اتصال مشفرة، يتم توفير زوج أرقام DH من هذا الاحتياطي. بعد إستخدام زوج أرقام DH، يتم تزويد المحمية تلقائيا بزوج أرقام DH جديد، بحيث يكون هناك دائما زوج أرقام DH جاهز للاستخدام.لا يلزم عادة أن يكون هناك أكثر من واحد أو إثنين من أزواج أرقام DH تم إنشاؤها مسبقا، ما لم يكن الموجه الخاص بك يقوم بإعداد جلسات عمل مشفرة متعددة بشكل متكرر بحيث يتم إستنزاف إحتياطي تم إنشاؤه مسبقا مكون من واحد أو إثنين من أزواج أرقام DH بسرعة كبيرة.

```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

- **show crypto cisco connections active**وفيما يلي عينة من مخرجات الأمر.

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
    Serial1         19.19.19.19 set    DES_56_CFB64    376      884   16
```

- **show crypto cisco engine connections drop-packet**وفيما يلي عينة من مخرجات الأمر.

```
Loser#show crypto engine connections dropped-packet
      Interface            IP-Address    Drop Count

      Serial1              19.19.19.19   39
```

- **show crypto engine configuration** (كان **show crypto engine brief** في برنامج Cisco IOS Software، الإصدار 11.2.)وفيما يلي عينة من مخرجات الأمر.

```
Loser#show crypto engine configuration
                    slot:              0
                 engine name:        fred
              engine type:        software
              serial number:      02802219
          platform:           rp crypto engine
                crypto lib version: 10.0.0

                :Encryption Process Info
                 input queue top:    465
                 input queue bot:    465
                   input queue count:  0
```

- **show crypto key mypubkey dss**وفيما يلي عينة من مخرجات الأمر.

```
Loser#show crypto key mypubkey dss
                  crypto public-key fred 02802219
79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
                                                                  quit
```

- **show crypto key pubkey series dss**وفيما يلي عينة من مخرجات الأمر.

```
Loser#show crypto key pubkey-chain dss
                      crypto public-key barney 05694352
B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
                                                                  quit
```

- show crypto map interface serial 1وفيما يلي عينة من مخرجات الأمر.

```
Loser#show crypto map interface serial 1
                        Crypto Map "oldstyle" 10 cisco
(Connection Id = 16       (8 established,    0 failed
                                    Peer = barney
                                  PE = 40.40.40.0
                                 UPE = 30.30.30.0
                              Extended IP access list 133
                            access-list 133 permit ip
                  source: addr = 40.40.40.0/0.0.0.255
                  dest:   addr = 30.30.30.0/0.0.0.255
```

لاحظ التفاوت الزمني عند إستخدام الأمر ping.

```
wan-5200b#ping 30.30.30.30

                                    .Type escape sequence to abort
   :Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds
                                                            !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
                                                      #wan-5200b
                                                     -----------
                                  wan-5200b#ping 30.30.30.31

                                    .Type escape sequence to abort
   :Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds
                                                            !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms
                                          -----------------

                                  wan-5200b#ping 19.19.19.20

                                    .Type escape sequence to abort
   :Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds
                                                            !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
                                         ------------
```

- show crypto map interface serial 1وفيما يلي عينة من مخرجات الأمر.

```
                                    Loser#show crypto map
                                  Crypto Map "oldstyle" 10 cisco
(Connection Id = 16       (8 established,    0 failed
                                    Peer = barney
                                  PE = 40.40.40.0
                                 UPE = 30.30.30.0
                              Extended IP access list 133
                            access-list 133 permit ip
                  source: addr = 40.40.40.0/0.0.0.255
                  dest:   addr = 30.30.30.0/0.0.0.255
```

- محرك تصحيح الأخطاء المشفرةوفيما يلي عينة من مخرجات الأمر.

```
                                    Loser#debug crypto engine
                Mar 17 11:49:07.902: Crypto engine 0: generate alg param

                Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
          Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
                Mar 17 11:49:11.758: Crypto engine 0: generate alg param

          Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
       Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
                  Mar 17 11:49:13.346: Crypto engine 0: verify signature
          Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
     Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
   Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25
```

```
Mar 17 11:49:24.946: Crypto engine 0: generate alg param
```

- **debug crypto sesmgmt**وفيما يلي عينة من مخرجات الأمر.

```
StHelen#debug crypto sessmgmt

,Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328
                                .Found an ICMP connection message

                          Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
      Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
                          Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
 Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
 Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
   Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
                            Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK
Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19
        Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent
 Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK
                          Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM
   Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
                          Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK
  (Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0
       .Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0
        Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0
     Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK
     ~~ <---------- This is good ----------> ~~
```

إذا تم تعيين النظير الخطأ على خريطة التشفير، فأنت تتلقى رسالة الخطأ هذه.

```
:Mar  2 12:19:12.639: CRYPTO-SDU:Far end authentication error
                        Connection message verify failed
```

إذا لم تتطابق خوارزميات التشفير، تتلقى رسالة الخطأ هذه.

```
Mar  2 12:26:51.091: CRYPTO-SDU: Connection
                        failed due to incompatible policy
```

إذا كان مفتاح DSS مفقودا أو غير صالح، تتلقى رسالة الخطأ هذه.

```
:Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error
                        Connection message verify failed
```

- **مفتاح تصحيح الأخطاء للتشفير**وفيما يلي عينة من مخرجات الأمر.

```
StHelen#debug crypto key
.Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes
.Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes
.Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes
.Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes
.Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes

.Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes
.Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes
.Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes
.Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes
.Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes
.Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes
```

- **مسح اتصال التشفير**وفيما يلي عينة من مخرجات الأمر.

```
wan-2511#show crypto engine connections act
  ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
       Serial0         20.20.20.21 set    DES_56_CFB64    29       28    9

wan-2511#clear crypto connection 9
wan-2511#
 (Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0*
              Mar  5 04:58:20.694: Crypto engine 0: delete connection 9*
   Mar  5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK*
wan-2511#
wan-2511#show crypto engine connections act
  ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
```

```
wan-2511#
```

- **أصفار التشفير**وفيما يلي عينة من مخرجات الأمر.

```
wan-2511#show crypto mypubkey
crypto public-key wan2511 01496536
11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

wan-2511#configure terminal
.Enter configuration commands, one per line.  End with CNTL/Z
wan-2511(config)#crypto zeroize
.Warning! Zeroize will remove your DSS signature keys
Do you want to continue? [yes/no]: yes
.Keys to be removed are named wan2511 %
Do you really want to remove these keys? [yes/no]: yes
.Zeroize done %

wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto mypubkey
wan-2511#
```

- **لا يوجد مفتاح عام تشفير**وفيما يلي عينة من مخرجات الأمر.

```
wan-2511#show crypto pubkey
crypto public-key wan2516 01698232
B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit

wan-2511#configure terminal
.Enter configuration commands, one per line.  End with CNTL/Z
? wan-2511(config)#crypto public-key
  WORD  Peer name

#(wan-2511(config
wan-2511(config)#no crypto public-key wan2516 01698232
wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto pubkey
wan-2511#
```

أستكشاف أخطاء Cisco 7200 وإصلاحها مع ESA

كما توفر Cisco خيار مساعدة الأجهزة لإجراء التشفير على موجهات سلسلة Cisco 7200، والتي يطلق عليها اسم ESA. ESA في شكل مهايئ منفذ لبطاقة VIP2-40 أو مهايئ منفذ مستقل ل Cisco 7200. يتيح هذا الترتيب إستخدام إما مهايئ جهاز أو محرك برنامج VIP2 لتشفير البيانات التي تدخل إلى الواجهات أو تخرج منها على البطاقة VIP2 7500 من Cisco وفك تشفيرها. يسمح Cisco 7200 للأجهزة بمساعدة تشفير حركة مرور البيانات لأي واجهات على هيكل Cisco 7200. يساعد إستخدام تشفير على حفظ دورات وحدة المعالجة المركزية (CPU) القيمة التي يمكن إستخدامها لأغراض أخرى، مثل التوجيه أو أي من وظائف Cisco IOS الأخرى.

على Cisco 7200، يتم تكوين مهايئ المنفذ المستقل تماما مثل محرك تشفير برنامج Cisco IOS Software، ولكنه يحتوي على بعض الأوامر الإضافية التي يتم إستخدامها فقط للأجهزة ولتحديد المحرك (البرامج أو الأجهزة) الذي سيقوم بالتشفير.

أولا، قم بتحضير الموجه لتشفير الأجهزة:

```
#(wan-7206a(config
OIR-6-REMCARD: Card removed from slot 3, interfaces disabled%
Mar  2 08:17:16.739: ...switching to SW crypto engine*
```

```
wan-7206a#show crypto card 3

Crypto card in slot: 3

   Tampered:        No
  Xtracted:        Yes
  Password set:    Yes
  DSS Key set:     Yes
FW version       0x5049702
#wan-7206a

#(wan-7206a(config

wan-7206a(config)#crypto zeroize 3
.Warning! Zeroize will remove your DSS signature keys
Do you want to continue? [yes/no]: yes
.Keys to be removed are named hard %
Do you really want to remove these keys? [yes/no]: yes
[OK]
```

تمكين تشفير الأجهزة أو تعطيله كما هو موضح أدناه:

```
wan-7206a(config)#crypto esa shutdown 3
switching to SW crypto engine...


wan-7206a(config)#crypto esa enable 3
.There are no keys on the ESA in slot 3- ESA not enabled
```

بعد ذلك، قم بإنشاء مفاتيح ل ESA قبل تمكينها.

```
wan-7206a(config)#crypto gen-signature-keys hard
Initialize the crypto card password. You will need %
 this password in order to generate new signature
 .keys or clear the crypto card extraction latch

:Password
:Re-enter password
.... Generating DSS keys
[OK]

#(wan-7206a(config
wan-7206a#show crypto mypubkey
crypto public-key hard 00000052
EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905
DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804
quit

#wan-7206a
wan-7206a(config)#crypto esa enable 3
switching to HW crypto engine...

wan-7206a#show crypto engine brie
crypto engine name:   hard
 crypto engine type:   ESA
serial number:        00000052
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 3

#wan-7206a
```

أستكشاف أخطاء VIP2 وإصلاحها مع ESA

يستخدم مهايئ منفذ الأجهزة ESA الموجود على بطاقة VIP2 لتشفير البيانات التي تصل إلى الواجهات أو تخرج منها على بطاقة VIP2 وفك تشفيرها. كما هو الحال مع Cisco 7200، يساعد إستخدام تشفير في توفير دورات وحدة المعالجة المركزية (CPU) القيمة. في هذه الحالة، لا يوجد الأمر **crypto esa enable** لأن مهايئ منفذ ESA يقوم بتشفير المنافذ على بطاقة VIP2 إذا كان ESA موصلا. يلزم تطبيق مفتاح **التشفير** clear-latch على تلك الفتحة في حالة تثبيت مهايئ منفذ ESA لأول مرة فقط، أو إزالته ثم إعادة تثبيته.

```
Router#show crypto card 11

   Crypto card in slot: 11

       Tampered:        No
      Xtracted:        Yes
      Password set:    Yes
      DSS Key set:     Yes
FW version       0x5049702
                  #Router
```

نظرا لاستخراج وحدة تشفير ESA، ستحصل على رسالة الخطأ التالية حتى تقوم بإصدار أمر **crypto clear-latch** على تلك الفتحة، كما هو موضح أدناه.

```
                                                                    ----
.Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed*
                                                                   -----
                                ? Router(config)#crypto clear-latch
                                     Chassis slot number  <0-15>

                               Router(config)#crypto clear-latch 11
                                  .Enter the crypto card password %
                                                          :Password
                                               Router(config)#^Z
```

إذا نسيت كلمة مرور تم تعيينها مسبقا، فاستخدم الأمر **crypto zeroize** بدلا من الأمر **crypto clear-latch** لإعادة ضبط ESA. بعد إصدار الأمر **crypto zeroize**، يجب إعادة إنشاء مفاتيح DSS وإعادتها. عندما تقوم بإعادة إنشاء مفاتيح DSS، سيطلب منك إنشاء كلمة مرور جديدة. ويرد أدناه مثال على ذلك.

```
                                                          #Router
                                SYS-5-CONFIG_I: Configured from console by console%
                                               Router#show crypto card 11

                                   Crypto card in slot: 11

                                       Tampered:        No
                                       Xtracted:        No
                                      Password set:    Yes
                                      DSS Key set:     Yes
                                FW version       0x5049702
                                                  #Router

-------------------------------------------------------------------------------


                                Router#show crypto engine brief
                                    crypto engine name:   TERT
                                crypto engine type:   software
```

```
                                        serial number:        0459FC8C
                                crypto engine state:  dss key generated
                                    crypto lib version:   5.0.0
                                       crypto engine in slot: 6

                                    crypto engine name:   WAAA
                                     crypto engine type:   ESA
                                        serial number:        00000078
                                crypto engine state:  dss key generated
                                  crypto firmware version:  5049702
                                       crypto engine in slot: 11

                                                                #Router
                                                           -----------
                                     Router(config)#crypto zeroize
                    .Warning! Zeroize will remove your DSS signature keys
                                    Do you want to continue? [yes/no]: yes
                                      .Keys to be removed are named TERT %
                    Do you really want to remove these keys? [yes/no]: yes
                                                            .Zeroize done %

                                     Router(config)#crypto zeroize  11
                    .Warning! Zeroize will remove your DSS signature keys
                                    Do you want to continue? [yes/no]: yes
                                      .Keys to be removed are named WAAA %
                    Do you really want to remove these keys? [yes/no]: yes
                                                                    [OK]

                                                  Router(config)#^Z
                                        Router#show crypto engine brief
                                      crypto engine name:   unknown
                                     crypto engine type:   software
                                     serial number:        0459FC8C
                                    crypto engine state:  installed
                                        crypto lib version:   5.0.0
                                           crypto engine in slot: 6

                                      crypto engine name:   unknown
                                         crypto engine type:   ESA
                                     serial number:        00000078
                                    crypto engine state:  installed
                                  crypto firmware version:  5049702
                                           crypto engine in slot: 11

                                                                #Router
                                                          --------------
                                  Router(config)#crypto gen-signature-keys VIPESA 11
                                Initialize the crypto card password. You will need %
                                 this password in order to generate new signature
                                  .keys or clear the crypto card extraction latch

                                                               :Password
                                                         :Re-enter password
                                                  .... Generating DSS keys
                                                                    [OK]

                                                               #(Router(config
                    .Jan 24 01:39:52.923: Crypto engine 11: create key pairs*
                                                                    Z^
                                                                #Router
                                                                 ------
                                        Router#show crypto engine brief
                                      crypto engine name:   unknown
                                     crypto engine type:   software
```

```
                                        serial number:        0459FC8C
                                      crypto engine state:  installed
                                          crypto lib version:   5.0.0
                                             crypto engine in slot: 6

                                        crypto engine name:   VIPESA
                                           crypto engine type:   ESA
                                      serial number:        00000078
                                  crypto engine state:  dss key generated
                                       crypto firmware version:  5049702
                                             crypto engine in slot: 11

                                                                #Router
                                                              ----------
                                  Router#show crypto engine connections active 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
   Serial11/0/0    20.20.20.21 set    DES_56_CFB64    9996     9996    2

                                                                #Router
                                     Router#clear crypto connection 2 11
                                                                #Router
(Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11*
                  Jan 24 01:41:04.611: Crypto engine 11: delete connection 2*
  Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK*
                                  Router#show crypto engine connections active 11
                                                          .No connections

                                                                #Router
          Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries*
                                                        received from VIP 0
                                                               ------------

                                                      Router#show crypto mypub
                                                            :Key for slot 11 %
                                                 crypto public-key VIPESA 00000078
 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD A87BF7FE
 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508
                                                                quit

                                                      Router#show crypto pub
                                                 crypto public-key wan2516 01698232
 C5DE8C46 8A69932C 70C92A2C 729449B3 FD10AC4D 1773A997 7F6BA37D 61997AC3
 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22 CFAAC1A8 9CE82985
                                                                quit

                                                                #Router
                                                              ----------
                                                    interface Serial11/0/0
                                          ip address 20.20.20.21 255.255.255.0
                                                     encapsulation ppp
                                               ip route-cache distributed
                                                        no fair-queue
                                                        no cdp enable
                                                    crypto map test
                                                                !
                                                              ----------
                                                 Router#show crypto eng conn act 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    761      760    3

                                                                #Router
                                  Jan 24 01:50:43.555: CRYPTO ENGINE:Number of connection*
                                                        entries received from VIP 1
```

```
#Router
```

معلومات ذات صلة

- تكوين تشفير طبقة الشبكة من Cisco واستكشاف أخطائه وإصلاحها: IPSec و ISAKMP - الجزء 2
- DES FIPS 46-2 في المعهد الوطني للمعايير والتكنولوجيا
- برنامج DSS FIPS 186 في المعهد الوطني للمعايير والتكنولوجيا (NIST)
- أسئلة كثيرا ما تطرحها مختبرات RSA حول التشفير الحالي
- معايير أمان IETF
- تكوين بروتوكول أمان Internet Key Exchange
- تكوين أمان شبكة IPSec
- صفحة دعم IPSec
- الدعم الفني - 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).