شبكات VPN Dynamic Multipoint IPsec (إستخدام Multipoint GRE/NHRP لقياس شبكات VPN IPsec)

المحتويات

المقدمة

يناقش هذا المستند شبكات VPN IPsec متعددة النقاط الديناميكية (DMVPN) ولماذا قد ترغب إحدى الشركات في تصميم شبكتهم أو ترحيلها لاستخدام حل IPsec VPN الجديد هذا في برنامج Cisco IOS®.

معلومات أساسية

قد تحتاج الشركات إلى ربط العديد من المواقع بموقع رئيسي، وربما أيضا ببعضها البعض، عبر الإنترنت مع تشفير حركة المرور لحمايتها. على سبيل المثال، قد تحتاج مجموعة من متاجر البيع بالتجزئة التي تحتاج إلى الاتصال بمقر الشركة للمخزون والطلب إلى الاتصال بالمتاجر الأخرى داخل الشركة للتحقق من توفر المنتج. في الماضي، كانت الطريقة الوحيدة لإجراء الاتصال هي إستخدام شبكة الطبقة 2 مثل ISDN أو ترحيل الإطارات للربط بين كل شيء. وقد يستغرق إعداد هذه الارتباطات السلكية السلكية الثابتة ودفع ثمنها لحركة مرور IP الداخلية وقتا طويلا كما أنها مكلفة. إذا كانت كافة المواقع (بما في ذلك الموقع الرئيسي) تتوفر بالفعل على وصول رخيص نسبيا إلى الإنترنت، يمكن إستخدام هذا الوصول إلى الإنترنت أيضا للاتصال الداخلي عبر بروتوكول الإنترنت (IP) بين المتاجر والمقر الرئيسي باستخدام أنفاق بروتوكول IPsec لضمان الخصوصية وسلامة البيانات.

لكي تتمكن الشركات من إنشاء شبكات IPsec كبيرة متصلة بمواقعها عبر الإنترنت، يجب أن تكون قادرا على تطوير شبكة IPsec. يقوم IPsec بتشفير حركة مرور البيانات بين نقطتي النهاية (الأقران)، ويتم التشفير باستخدام نقطتي النهاية المشتركتين باستخدام "سر" مشترك. نظرا لمشاركة هذا السر فقط بين نقطتي النهاية هاتين، فإن الشبكات المشفرة هي بطبيعتها مجموعة من الارتباطات من نقطة إلى نقطة. ولهذا السبب، يعد IPsec شبكة نفق من نقطة إلى نقطة في حد ذاته. الطريقة الأكثر جدوى لتطوير شبكة كبيرة من نقطة إلى نقطة هي تنظيمها في شبكة شبكة شبكية محورية أو كاملة (جزئية). في معظم الشبكات، تكون معظم حركة مرور IP بين الفروع والمحور، والقليل جدا بين الفروع، لذلك فإن تصميم المحور والمحور غالبا ما يكون أفضل خيار. يتوافق هذا التصميم أيضا مع شبكات ترحيل الإطارات القديمة نظرا لأن تكلفة الدفع للروابط بين جميع المواقع في هذه الشبكات كانت باهظة.

عند إستخدام الإنترنت كربط بين المحور والأخاديد، يكون في متناول الفروع أيضا بشكل مباشر مع بعضها البعض بدون أي تكلفة إضافية، ولكن كان من الصعب جدا، إن لم يكن من المستحيل، لإقامة و / أو إدارة شبكة كاملة (جزئية) متداخلة. غالبا ما تكون شبكات الشبكة المعشقة الكاملة أو الجزئية مرغوب فيها لأنه يمكن أن يكون هناك توفير في التكلفة إذا كان من الممكن لحركة المرور عبر المحادثة المباشرة بدلا من ذلك من خلال الصرة. حركة مرور البيانات التي يتم التحدث بها عبر الصرة تستخدم موارد الصرة ويمكن أن تتسبب في تأخيرات إضافية، خاصة عند إستخدام تشفير IPsec، حيث أن الصرة ستحتاج إلى فك تشفير الحزم الواردة من الفروع المرسلة ثم إعادة تشفير حركة مرور البيانات لإرسالها إلى محادثة الاستلام. مثال آخر حيث المحادثات المباشرة تكون حركة المرور مفيدة وهو حالة الناموسين في نفس المدينة والمحور في جميع أنحاء البلاد.

مع نشر شبكات موزع وتكرار IPsec وحجمها المتزايد، أصبح من الأفضل أن تقوم بتوجيه حزم IP بشكل ديناميكي قدر الإمكان. في الشبكات القديمة لترحيل الإطارات، تم تحقيق ذلك من خلال تشغيل بروتوكول توجيه ديناميكي مثل OSPF أو EIGRP عبر إرتباطات ترحيل الإطارات. كان هذا مفيدا للإعلان ديناميكيا عن إمكانية الوصول إلى الشبكات التي تم التحدث وأيضا لدعم التكرار في شبكة توجيه IP. إذا فقدت الشبكة موجه لوحة وصل، فيمكن لموجه لوحة وصل نسخ إحتياطي أن يتولى الأمر تلقائيا للاحتفاظ باتصال الشبكة بالشبكات التي يتم التحدث بها.

هناك مشكلة أساسية مع أنفاق IPsec وبروتوكولات التوجيه الديناميكية. تعتمد بروتوكولات التوجيه الديناميكية على إستخدام حزم بث IP المتعدد أو البث المتعدد، ولكن IPsec لا يدعم تشفير حزم البث المتعدد أو البث. الطريقة الحالية لحل هذه المشكلة هي إستخدام أنفاق تضمين التوجيه العام (GRE) بالاشتراك مع تشفير IPsec.

تدعم أنفاق GRE نقل حزم بث IP المتعدد والبث إلى الطرف الآخر من نفق GRE. حزمة نفق GRE هي حزمة IP للبث الأحادي، لذلك يمكن تشفير حزمة GRE باستخدام IPsec. في هذا السيناريو، تقوم GRE بعمل الاتصال النفقي ويقوم IPsec بجزء التشفير لدعم شبكة VPN. عند تكوين أنفاق GRE، يجب أن تكون عناوين IP لنقاط النهاية للنفق **(مصدر النفق...، وجهة النفق ...)** معروفة بنقطة النهاية الأخرى ويجب أن تكون قابلة للتوجيه عبر الإنترنت. هذا يعني أن الصرة وكل من تحدثت مسحاج تخديد في هذا شبكة ينبغي يتلقى ساكن إستاتيكي غير خاص عنوان.

لاتصالات الموقع الصغير بالإنترنت، من الطبيعي أن يتغير عنوان IP الخارجي الخاص بمتكلم كل مرة يتصل فيها بالإنترنت لأن مزود خدمة الإنترنت الخاص به (ISP) يوفر بشكل ديناميكي عنوان الواجهة الخارجية (عبر بروتوكول التكوين الديناميكي للمضيف (DHCP) كل مرة يأتي فيها الحديث على الخط (خط المشترك الرقمي غير المتماثل (ADSL) وخدمات الكبلات). يتيح هذا التخصيص الديناميكي ل "العنوان الخارجي" للموجه ل ISP الاشتراك الزائد في إستخدام مساحة عنوان الإنترنت الخاصة بهم، نظرا لعدم وجود جميع المستخدمين على الإنترنت في نفس الوقت. قد يكون دفع الموفر لتخصيص عنوان ثابت للموجه المتصل أكثر تكلفة إلى حد كبير. يتطلب تشغيل بروتوكول توجيه ديناميكي عبر شبكة VPN IPsec إستخدام أنفاق GRE، ولكن تفقد خيار الحصول على حزم باستخدام عناوين IP التي تم تخصيصها ديناميكيا على الواجهات المادية الخارجية الخاصة بها.

ويرد موجز للقيود المذكورة أعلاه ولبعض القيود الأخرى في النقاط الأربع التالية:

- يستخدم IPsec قائمة تحكم في الوصول (ACL) لتحديد البيانات المراد تشفيرها. لذلك، في كل مرة تتم إضافة شبكة (فرعية) جديدة خلف موجهات محورية أو محورية، يجب على العميل تغيير قائمة التحكم في الوصول (ACL) على كل من موجهات المحوري والمحوري. إذا كان مزود الخدمة (SP) يدير الموجه، فيجب على العميل إعلام مزود الخدمة (SP) من أجل تغيير قائمة التحكم في الوصول (ACL) إلى IPsec حتى يتم تشفير حركة المرور الجديدة.
- مع الشبكات الكبيرة والمحورية، يمكن أن يصبح حجم التكوين على موجه الموزع كبير جدا، لدرجة أنه غير قابل للاستخدام. على سبيل المثال، سيحتاج موجه صرة إلى ما يصل إلى 3900 سطر من التكوين لدعم الموجهات التي يبلغ عددها 300. هذا كبير بدرجة كافية بحيث يصعب إظهار التكوين والبحث عن قسم التكوين المرتبط بمشكلة حالية قيد تصحيح الأخطاء. أيضا، قد يكون تكوين هذا الحجم أكبر من أن يمكن إحتوائه في ذاكرة NVRAM وسيحتاج إلى تخزينه على ذاكرة Flash (الذاكرة المؤقتة).
- يجب أن تعرف GRE + IPsec عنوان نظير نقطة النهاية. تتصل عناوين IP الخاصة بالخوادم مباشرة بالإنترنت عبر مزود خدمة الإنترنت (ISP) الخاص بها، وغالبا ما يتم إعدادها حتى لا يتم إصلاح عناوين الواجهة الخارجية الخاصة بها. يمكن تغيير عناوين IP كل مرة يصبح فيها الموقع متصلا (عبر DHCP).
- إذا كانت المحددات بحاجة إلى التحدث مباشرة مع بعضها البعض عبر شبكة VPN IPsec، فيجب أن تصبح الشبكة المحورية شبكة كاملة. وبما انه ليس معروفا الآن أي من القبيلتين يلزم ان يتكلما مباشرة واحدهما مع الآخر، يلزم ان تكون هنالك شبكة كاملة، على الرغم من ان كلا منهما قد لا يحتاج إلى التكلم مباشرة مع كل متكلم آخر. كما أنه من غير الممكن تكوين IPsec على موجه صغير يتم التحدث به حتى يكون له اتصال مباشر مع جميع الموجهات الأخرى في الشبكة، وبالتالي قد تكون الموجهات التي يتم التحدث بها بحاجة إلى أن تكون موجهات أكثر قوة.

حل DMVPN

يستخدم حل DMVPN بروتوكول GRE متعدد النقاط (Multipoint GRE) وبروتوكول تحليل الخطوة التالية (Hop) (NHRP)، مع IPsec وبعض التحسينات الجديدة، لحل المشاكل السابقة بطريقة قابلة للتطوير.

بدء تشفير IPsec التلقائي

عند عدم إستخدام حل DMVPN، لا يتم بدء تشغيل نفق تشفير IPsec حتى يكون هناك حركة مرور بيانات تتطلب إستخدام نفق IPsec هذا. قد يستغرق إكمال بدء نفق IPsec من 1 إلى 10 ثوان، وقد يتم إسقاط حركة مرور البيانات أثناء هذا الوقت. عند إستخدام GRE مع IPsec، يتضمن تكوين نفق GRE بالفعل عنوان نظير نفق GRE (**وجهة النفق ...**)، وهو أيضا عنوان نظير IPsec. تم تكوين كلا هذين العنوانين مسبقا.

إذا كنت تستخدم اكتشاف نقطة نهاية النفق (TED) وخرائط التشفير الديناميكية على موجه المحور، بعد ذلك يمكنك تجنب الاضطرار إلى تكوين عناوين نظير IPsec مسبقا على الموزع، ولكن يلزم إرسال واستقبال تحقيق TED والاستجابة قبل بدء تفاوض ISAKMP. ولا ينبغي أن يكون هذا ضروريا لأن عناوين مصدر ووجهة النظير معروفة بالفعل عند إستخدام GRE. وهي إما في التكوين أو تم حلها باستخدام NHRP (لأنفاق GRE متعددة النقاط).

باستخدام حل DMVPN، يتم تشغيل IPsec فورا لكل من أنفاق GRE من نقطة إلى نقطة و Multipoint. أيضا، ليس من الضروري تكوين أي قوائم التحكم في الوصول إلى التشفير، نظرا لأنه سيتم اشتقاقها تلقائيا من مصدر نفق GRE وعناوين الوجهة. يتم إستخدام الأوامر التالية لتعريف معلمات تشفير IPsec. لاحظ عدم وجود **مجموعة نظير ...** أو **أوامر مطابقة ...** مطلوبة لأن هذه المعلومات مشتقة مباشرة من نفق GRE المقترن أو تعيينات NHRP.

crypto ipsec profile

set transform-set

يربط الأمر التالي واجهة نفق بملف تعريف IPsec.

```
interface tunnel

...
tunnel protection ipsec profile
```

إنشاء النفق الديناميكي للروابط "التي يتم التحدث إليها"

لم يتم تكوين أي معلومات GRE أو IPsec حول إحدى الشبكات على موجه الموزع في شبكة DMVPN . تم تكوين نفق GRE الخاص بالموجه الذي تم التحدث به (عبر أوامر NHRP) باستخدام معلومات حول موجه الموزع. عند بدء تشغيل الموجه الذي يتم التحدث به، فإنه يقوم تلقائيا ببدء نفق IPsec باستخدام موجه الموزع كما هو موضح أعلاه. ثم يستخدم NHRP لإعلام موجه الموزع بعنوان IP للواجهة المادية الحالية الخاصة به. وهذا مفيد لثلاثة أسباب:

- إذا كان الموجه الموجه الذي يتحدث تم تعيين عنوان IP للواجهة المادية الخاصة به بشكل ديناميكي (مثل مع ADSL أو CableModem)، فلا يمكن تكوين موجه الموزع باستخدام هذه المعلومات نظرا لأنه في كل مرة يتم فيها إعادة تحميل الموجه الذي يتحدث به يحصل على عنوان IP للواجهة المادية الجديدة.
- يتم إختصار وتبسيط تكوين موجه الموزع نظرا لأنه لا يحتاج إلى وجود أي معلومات GRE أو IPsec حول موجهات النظير. وكل هذه المعلومات يتم التعرف عليها بشكل ديناميكي من خلال NHRP.
- عندما تقوم بإضافة موجه جديد إلى شبكة DMVPN، لا تحتاج إلى تغيير التكوين على الموزع أو على أي من الموجهات التي يتم التحدث بها حاليا. يتم تكوين الموجه الموجه الذي يتم التحدث به باستخدام معلومات الصرة، وعندما يبدأ في التشغيل، فإنه يقوم بالتسجيل بشكل ديناميكي باستخدام موجه الصرة. يقوم بروتوكول التوجيه الديناميكي بنشر معلومات التوجيه الخاصة بهذا الأمر الذي تم التحدث إليه في الصرة. يقوم الصرة بنشر معلومات التوجيه الجديدة هذه إلى الفروع الأخرى. كما أنها تنشر معلومات التوجيه من الفروع الأخرى إلى هذه المحادثة.

إنشاء نفق ديناميكي لحركة المرور "المنقولة عبر الهاتف"

وكما تمت الإشارة مسبقا، حاليا في شبكة شبكة متداخلة، يجب تكوين جميع أنفاق IPsec من نقطة إلى نقطة (أو IPsec+GRE) على جميع الموجهات، حتى إذا لم تكن بعض/معظم هذه الأنفاق قيد التشغيل أو مطلوبة في جميع الأوقات. باستخدام حل DMVPN، يكون أحد الموجهات هو الموزع، ويتم تكوين جميع الموجهات الأخرى (الفروع) باستخدام أنفاق إلى الصرة. الأنفاق المحورية يتم تعبئتها باستمرار، والأخاديد لا تحتاج إلى تهيئة للأنفاق المباشرة إلى أي من الأخاديد الأخرى. بدلا من ذلك، عندما يريد أحد المتحدثين إرسال حزمة إلى آخر تم التحدث به (مثل الشبكة الفرعية خلف آخر تم التحدث به)، فإنه يستخدم NHRP لتحديد عنوان الوجهة المطلوب للهدف الذي تم التحدث به بشكل ديناميكي. يعمل موجه الصرة كخادم NHRP ويعالج هذا الطلب للمصدر الذي يتحدث. وبعد ذلك، يقوم الخادمان بإنشاء نفق IPsec بينهما بشكل ديناميكي (عبر واجهة mGRE الأحادية) ويمكن نقل البيانات مباشرة. سيتم تدمير هذا النفق الديناميكي الذي يتم التحدث إليه تلقائيا بعد فترة (قابلة للتكوين) من عدم النشاط.

دعم بروتوكولات التوجيه الديناميكية

يعتمد حل DMVPN على أنفاق GRE التي تدعم حزم IP للبث/البث المتعدد النفقي، لذلك يدعم حل DMVPN أيضا بروتوكولات التوجيه الديناميكية التي تعمل عبر أنفاق IPsec+mGRE. سابقا، تطلبت NHRP أنت أن يشكل بشكل صريح البث/multicast يخطط ل النفق غاية عنوان أن يدعم GRE tunneling من multicast وبث ip ربط. على سبيل المثال، في الصرة ستحتاج إلى سطر تكوين **ip nhrp map multicast <spoke-n-addr>** لكل **كلمة**. باستخدام حل DMVPN، لا يتم التعرف على العناوين التي يتم التحدث بها مسبقا، لذلك لا يمكن إجراء هذا التكوين. وبدلا من ذلك، يمكن تكوين NHRP لإضافة كل رسالة تلقائيا إلى قائمة وجهة البث المتعدد على الموزع باستخدام الأمر **ip nhrp map multicast dynamic**. باستخدام هذا الأمر، عندما تقوم الموجهات التي يتم التحدث بها بتسجيل تعيين NHRP للبث الأحادي باستخدام خادم NHRP (المحور)، سيقوم NHRP أيضا بإنشاء تعيين بث/بث متعدد لهذا النوع من الكلام. وهذا يزيل الحاجة إلى معرفة العناوين التي يجري التكلم بها مسبقا.

التحويل السريع لإعادة التوجيه السريع Cisco Express Forwarding ل mGRE

حاليا، يتم تحويل حركة مرور البيانات في واجهة mGRE، مما يؤدي إلى أداء ضعيف. يضيف حل DMVPN تحويل إعادة التوجيه السريع من Cisco لحركة مرور البيانات mGRE، مما ينتج عنه أداء أفضل بكثير. لا توجد أوامر تكوين ضرورية لتشغيل هذه الميزة. إذا تم السماح بتحويل إعادة التوجيه السريع من Cisco على واجهة نفق GRE والواجهات المادية الصادرة/الواردة، فسيتم تحويل حزم نفق GRE متعدد النقاط بواسطة إعادة التوجيه السريع من Cisco.

إستخدام التوجيه الديناميكي عبر شبكات VPN المحمية عبر IPsec

يصف هذا القسم حالة الشؤون الحالية (حل ما قبل DMVPN). يتم تنفيذ IPsec على موجهات Cisco عبر مجموعة من الأوامر التي تعرف التشفير ثم يتم تطبيق الأمر **crypto map <map-name>** على الواجهة الخارجية للموجه. بسبب هذا التصميم وعدم وجود معيار حاليا لاستخدام IPsec لتشفير حزم البث/البث المتعدد ل IP، لا يمكن "إعادة توجيه" حزم بروتوكول توجيه IP من خلال نفق IPsec ولا يمكن نشر أي تغييرات توجيه ديناميكيا إلى الجانب الآخر من نفق IPsec.

ملاحظة: تستخدم جميع بروتوكولات التوجيه الديناميكية باستثناء BGP البث أو حزم IP للبث المتعدد. يتم إستخدام أنفاق GRE بالاشتراك مع IPsec لحل هذه المشكلة.

يتم تنفيذ أنفاق GRE على موجهات Cisco باستخدام واجهة نفق ظاهري (**نفق الواجهة<#>**). تم تصميم بروتوكول اتصال GRE النفقي لمعالجة حزم بث/بث IP المتعدد حتى يمكن "تشغيل" بروتوكول التوجيه الديناميكي عبر نفق GRE. حزم نفق GRE هي حزم IP للبث الأحادي التي تغلف حزمة IP المتعددة/البث الأحادي الأصلية. يمكنك بعد ذلك إستخدام IPsec لتشفير حزمة نفق GRE. يمكنك أيضا تشغيل IPsec في وضع النقل وحفظ 20 بايت نظرا لأن GRE قد قام بالفعل بتضمين حزمة البيانات الأصلية لذلك لا تحتاج إلى IPsec لتضمين حزمة GRE IP في رأس IP آخر.

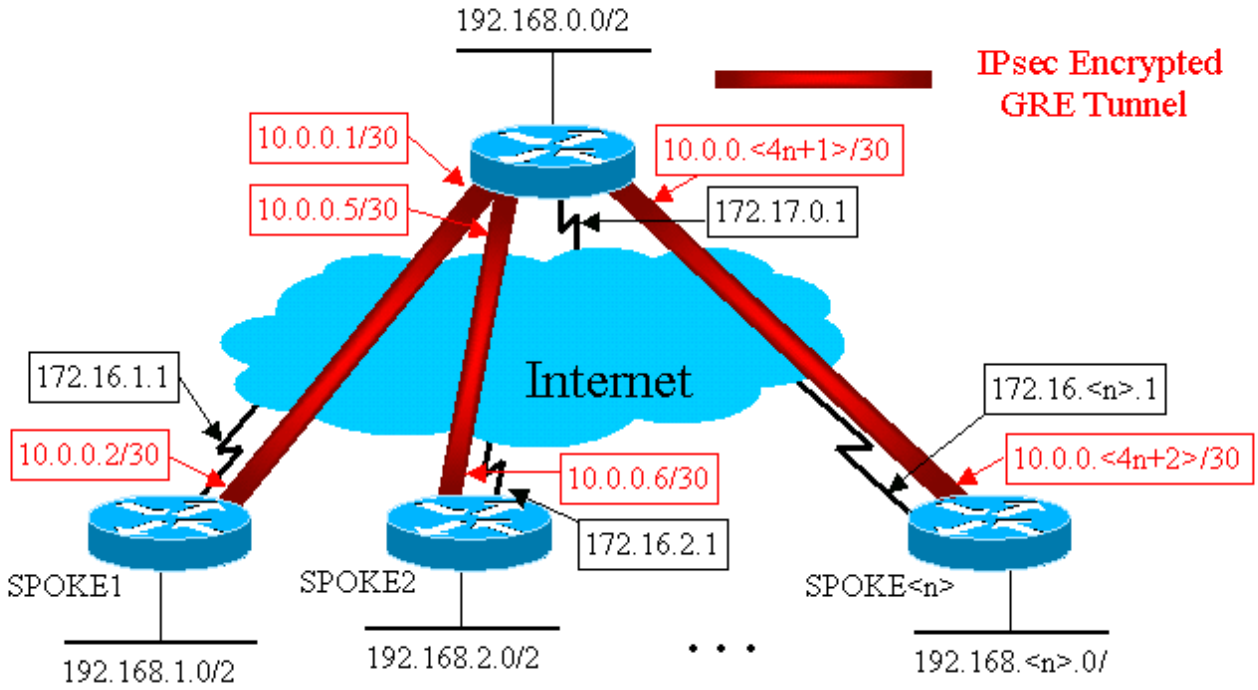
عند تشغيل IPsec في وضع النقل، هناك تقييد مفاده أن عناوين مصدر IP والوجهة للحزمة المراد تشفيرها يجب أن تطابق عناوين نظير IPsec (الموجه نفسه). في هذه الحالة، يعني ذلك فقط أن نقطة نهاية نفق GRE وعناوين نظراء IPsec يجب أن تكون متماثلة. لا تمثل هذه مشكلة نظرا لأن الموجهات نفسها هي نقاط النهاية لنفق IPsec و GRE على حد سواء. من خلال دمج أنفاق GRE مع تشفير IPsec، يمكنك إستخدام بروتوكول توجيه IP ديناميكي لتحديث جداول التوجيه على كلا طرفي النفق المشفر. سيكون لإدخالات جدول توجيه IP للشبكات التي تم التعرف عليها من خلال النفق المشفر الطرف الآخر من النفق (عنوان IP الخاص بواجهة نفق GRE) كعنوان IP التالي. وبالتالي، إذا تغيرت الشبكات على أي من جانبي النفق، فإن الجانب الآخر سيتعلم بشكل ديناميكي عن التغيير وسيستمر الاتصال دون أي تغييرات في التكوين على الموجهات.

التكوين الأساسي

فيما يلي تكوين IPsec+GRE قياسي من نقطة إلى نقطة. وبعد ذلك، هناك سلسلة من أمثلة التكوين التي تتم فيها

إضافة ميزات محددة لحل DMVPN في الخطوات اللازمة لإظهار القدرات المختلفة لشبكة DMVPN. يعتمد كل مثال على الأمثلة السابقة لإظهار كيفية إستخدام حل DMVPN في تصميمات الشبكات التي تزداد تعقيدا. يمكن إستخدام هذه السلسلة المتعاقبة من الأمثلة كقالب لترحيل شبكة خاصة ظاهرية (VPN) حالية خاصة ب IPsec+GRE إلى شبكة DMVPN. يمكنك إيقاف "الترحيل" عند أي نقطة إذا كان مثال التكوين هذا يطابق متطلبات تصميم الشبكة لديك.

IPsec + محور GRE والتحدث (n = 1،2،3،...)



موجه الموزع

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
set peer 172.16.1.1
set transform-set trans2
match address 101
crypto map vpnmap1 20 ipsec-isakmp
set peer 172.16.2.1
set transform-set trans2
match address 102
. . .
crypto map vpnmap1 <10*n> ipsec-isakmp
.set peer 172.16
```

```
interface Tunnel1
 bandwidth 1000
ip address 10.0.0.1 255.255.255.252
 ip mtu 1400
 delay 1000
tunnel source Ethernet0
tunnel destination 172.16.1.1
!
interface Tunnel2
 bandwidth 1000
ip address 10.0.0.5 255.255.255.252
 ip mtu 1400
 delay 1000
tunnel source Ethernet0
tunnel destination 172.16.2.1
!
. . .
!
interface Tunnel
```

```
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
...
access-list
```

الموجه TALK1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
```

```
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.1.1 255.255.255.252
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre host 172.16.1.1 host
172.17.0.1
```

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.6 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.2.1 255.255.255.252
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.2.1 255.255.255.0
!
```

```
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.2.1 host
172.17.0.1
```

تم التحديث<Router n>

```
version 12.3
!
<hostname Spoke<n
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<4n-2> 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
!
interface Ethernet0
 ip address 172.16.<n>.1 255.255.255.252
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 .network 192.168
```

في التكوين المذكور أعلاه، يتم إستخدام قوائم التحكم في الوصول (ACL) لتحديد حركة المرور التي سيتم تشفيرها. على كل من الموجهات المحورية والمحكية، تحتاج قائمة التحكم في الوصول هذه فقط إلى مطابقة حزم IP الخاصة بنفق GRE. بغض النظر عن كيفية تغيير الشبكات في أي من النهايتين، لن تتغير حزم نفق GRE IP، لذلك لا يلزم تغيير قائمة التحكم في الوصول هذه.

ملاحظة: عند إستخدام إصدارات برنامج Cisco IOS Software قبل الإصدار 12.2(13)T، يجب عليك تطبيق أمر التكوين **crypto map vpnmap1** على كل من واجهات نفق GRE (Tunnel<x>) والواجهة المادية (Ethernet0). باستخدام الإصدار 12.2(13)T من Cisco IOS والإصدارات الأحدث، يمكنك فقط تطبيق أمر التكوين **crypto map vpnmap1** على الواجهة المادية (Ethernet0).

أمثلة لجداول التوجيه على الموجهات المحكية والموجهة

جدول التوجيه على موجه الموزع

```
                is subnetted, 1 subnets 172.17.0.0/24
   C       172.17.0.0 is directly connected, Ethernet0
            is subnetted, <n> subnets 10.0.0.0/30
        C       10.0.0.0 is directly connected, Tunnel1
        C       10.0.0.4 is directly connected, Tunnel2
                                                    ...
 <C       10.0.0.<4n-4> is directly connected, Tunnel<n
   C    192.168.0.0/24 is directly connected, Ethernet1
         D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
                                        18:28:19, Tunnel1
  D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
                                                Tunnel2
                                                    ...
  D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
                                         <2d05h, Tunnel<n
```

جدول التوجيه على الموجه Talk1

```
                is subnetted, 1 subnets 172.16.0.0/24
   C       172.16.1.0 is directly connected, Ethernet0
            is subnetted, <n> subnets 10.0.0.0/30
        C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
                                                Tunnel0
                                                    ...
        D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
                                        23:00:58, Tunnel0
         D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
                                        23:00:58, Tunnel0
   C    192.168.1.0/24 is directly connected, Loopback0
         D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
                                        23:00:58, Tunnel0
                                                    ...
       D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
                                        23:00:58, Tunnel0
```

جدول التوجيه على الموجه الذي يتم التحدث به<n>

```
                is subnetted, 1 subnets 172.16.0.0/24
   C       172.16.<n>.0 is directly connected, Ethernet0
             is subnetted, <n> subnets 10.0.0.0/30
   D       10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
                                                Tunnel0
   D       10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
                                                Tunnel0
                                                    ...
   C        10.0.0.<4n-4> is directly connected, Tunnel0
         D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
                                        22:01:21, Tunnel0
         D    192.168.1.0/24 [90/3097600] via 10.0.0.1,
                                        22:01:21, Tunnel0
         D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
                                        22:01:21, Tunnel0
                                                    ...
   C    192.168.<n>.0/24 is directly connected, Ethernet0
```

وهذا تكوين أساسي للعمل، ويتم إستخدامه كنقطة بداية للمقارنة مع التكوينات الأكثر تعقيدا الممكنة باستخدام حل DMVPN. سيؤدي التغيير الأول إلى تقليل حجم التكوين على موجه الموزع. لا يكون هذا مهما مع أعداد صغيرة من الموجهات التي يتم التحدث عنها، ولكنه يصبح حاسما عندما يكون هناك أكثر من 50 إلى 100 موجه.

تقليل حجم تكوين موجه الموزع

في المثال التالي، يتم تغيير التكوين على موجه الموزع كحد أدنى من واجهات نفق GRE المتعددة من نقطة إلى نقطة إلى واجهة نفق GRE متعددة النقاط. هذه خطوة أولى في حل DMVPN.

هناك كتلة فريدة من خطوط التكوين على موجه الصرة لتحديد خصائص خريطة التشفير لكل موجه تمت محادثته. تحدد هذه القطعة من التكوين قائمة التحكم في الوصول (ACL) للتشفير وواجهة نفق GRE لذلك الموجه الذي يتحدث. وتكون هذه الخصائص هي نفسها في معظم الأحيان لجميع الفروع، باستثناء عناوين IP (**مجموعة النظير ...**، **وجهة النفق ...**).

بالنظر إلى التكوين المذكور أعلاه على موجه الموزع، تلاحظ أن هناك 13 خطا على الأقل من التكوين لكل موجه تم التحدث عنه، أربعة لخريطة التشفير، وواحد لقائمة التحكم في الوصول إلى التشفير، وثمانية لواجهة نفق GRE. ويبلغ العدد الإجمالي لبنود التكوين، إذا كان هناك 300 موجه، 3900 سطر. كما تحتاج إلى 300 شبكة فرعية (/30) لمعالجة كل إرتباط نفق. من الصعب جدا إدارة تكوين بهذا الحجم، بل إنه أكثر صعوبة عند أستكشاف أخطاء شبكة VPN وإصلاحها. لتقليل هذه القيمة، يمكنك إستخدام خرائط التشفير الديناميكية، والتي من شأنها تقليل القيمة المذكورة أعلاه بمقدار 1200 خط، تاركا 2700 خط في شبكة 300 محادثة.

ملاحظة: عند إستخدام خرائط التشفير الديناميكية، يجب بدء تشغيل نفق تشفير IPsec بواسطة الموجه المتكلم. يمكنك أيضا إستخدام **واجهة <IP<interface غير المرقمة** لتقليل عدد الشبكات الفرعية اللازمة لأنفاق GRE، ولكن قد يؤدي هذا إلى جعل أستكشاف الأخطاء وإصلاحها أكثر صعوبة لاحقا.

باستخدام حل DMVPN، يمكنك تكوين واجهة نفق GRE متعددة النقاط واحدة وملف تعريف IPsec واحد على موجه الموزع لمعالجة جميع الموجهات التي يتم التحدث بها. وهذا يسمح لحجم التكوين على موجه الصرة بأن يبقى ثابتا، بغض النظر عن عدد الموجهات التي يتم الحديث بها التي يتم إضافتها إلى شبكة VPN.

يقدم حل DMVPN الأوامر الجديدة التالية:

```
crypto ipsec profile
```

يتم إستخدام الأمر **crypto ipSec profile <name>**كخريطة تشفير ديناميكية، ويتم تصميمه خصيصا لواجهات النفق. يتم إستخدام هذا الأمر لتحديد معلمات تشفير IPsec على أنفاق شبكة VPN التي يتم التحدث بها وعلى شبكة VPN. المعلمة الوحيدة المطلوبة ضمن ملف التعريف هي مجموعة التحويل. يتم اشتقاق عنوان نظير IPsec **وعنوان المطابقة ...** عبارة وكيل IPsec تلقائيا من تعيينات NHRP لنفق GRE.

يتم تكوين الأمر <name>**حماية النفق لملف تعريف IPsec** تحت واجهة نفق GRE ويتم إستخدامه لإقران واجهة نفق GRE بملف تعريف IPsec. وبالإضافة إلى ذلك، يمكن إستخدام أمر **ملف تعريف <name>**لحماية النفق مع نفق GRE من نقطة إلى نقطة. في هذه الحالة، فإنه سيستمد معلومات نظير IPsec والوكيل من **مصدر النفق**..**ووجهة النفق ...** التكوين. وهذا يعمل على تبسيط التكوين نظرا لأن نظير IPsec وقوائم التحكم في الوصول (ACL) المشفرة لم تعد مطلوبة.

ملاحظة: يحدد الأمر **حماية النفق ...** أنه سيتم تشفير IPsec بعد إضافة عملية كبسلة GRE إلى الحزمة.

هذان الأمران الجديدان الأولان مماثلان لتكوين خريطة تشفير وتعيين خريطة التشفير إلى واجهة باستخدام الأمر **crypto map <name>**. يكمن الاختلاف الكبير في أنه، باستخدام الأوامر الجديدة، لا تحتاج إلى تحديد عنوان نظير IPsec أو قائمة تحكم في الوصول (ACL) لمطابقة الحزم التي سيتم تشفيرها. ويتم تحديد هذه المعلمات تلقائيا من تعيينات NHRP لواجهة نفق mGRE.

ملاحظة: عند إستخدام الأمر **حماية النفق** على واجهة النفق، لا يتم تكوين أمر **crypto map ...** على الواجهة الصادرة الفعلية.

الأمر الجديد الأخير، **ip nhrp map multicast dynamic**، يسمح NHRP بإضافة الموجهات التي يتم التحدث بها تلقائيا إلى تعيينات NHRP للبث المتعدد عندما تقوم هذه الموجهات التي يتم التحدث بها ببدء نفق mGRE+IPsec وتسجيل تعيينات NHRP للبث الأحادي الخاصة بها. يلزم هذا لتمكين بروتوكولات التوجيه الديناميكية للعمل عبر أنفاق mGRE+IPsec بين الموزع والأقسام الفرعية. إذا لم يكن هذا الأمر متوفرا، فسيحتاج موجه الموزع إلى الحصول على سطر تكوين منفصل لتعيين البث المتعدد لكل متحدث.

ملاحظة: باستخدام هذا التكوين، يجب أن تبدأ الموجهات التي يتم التحدث بها اتصال نفق mGRE+IPsec، نظرا لأنه لم يتم تكوين موجه الموزع باستخدام أي معلومات حول الفروع. ولكن، هذه ليست مشكلة لأنه مع DMVPN يتم بدء تشغيل نفق mGRE+IPsec تلقائيا عند بدء تشغيل الموجه الذي يتم التحدث به، ويستمر في العمل.

ملاحظة: يوضح المثال التالي واجهات نفق GRE من نقطة إلى نقطة على الموجهات التي يتم التحدث بها وخطوط تكوين NHRP التي تمت إضافتها على كل من موجهات جهات جهات المحوري والمكالمات لدعم نفق MGRE على موجه المحولات. تكون تغييرات التكوين كما يلي.

موجه الموزع (قديم)

```
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.16.1.1
 set transform-set trans2
 match address 101
crypto map vpnmap1 20 IPsec-isakmp
 set peer 172.16.2.1
 set transform-set trans2
 match address 102
 . . .
crypto map vpnmap1 <10n> IPsec-isakmp
 .set peer 172.16
```

```
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
 crypto map vpnmap1
!
access-list 101 permit gre host 172.17.0.1 host
 172.16.1.1
access-list 102 permit gre host 172.17.0.1 host
 172.16.2.1
 . . .
 access-list
```

موجه الموزع (جديد)

```
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
no ip split-horizon eigrp 1
 delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
 tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
```

تم التحديث<Router n> (قديم)

```
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
ip address 10.0.0.<4n-2> 255.255.255.252
 ip mtu 1400
 delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.<n>.1 255.255.255.252
 crypto map vpnmap1
!
. . .
!
access-list 101 permit gre host 172.16.<n>.1 host
 172.17.0.1
!
```

تم التحديث<Router n> (جديد)

```
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
.ip address 10.0.0
```

```
                                                delay 1000
                                        tunnel source Ethernet0
                                    tunnel destination 172.17.0.1
                                              tunnel key 100000
                                                             !
                                             interface Ethernet0
                                ip address 172.16.<n>.1 255.255.255.252
                                              crypto map vpnmap1
                                                             !
                                                         . . .
                                                             !
                        access-list 101 permit gre host 172.16.<n>.1 host
                                                      172.17.0.1
                                                             !
```

على الموجهات التي يتم التحدث بها، تم تغيير قناع الشبكة الفرعية، وتمت إضافة أوامر NHRP أسفل واجهة النفق. تعد أوامر NHRP ضرورية نظرا لأن موجه الموزع يستخدم الآن NHRP لتعيين عنوان IP لواجهة النفق المتصل إلى عنوان IP للواجهة المادية التي يتم التحدث بها.

.ip address 10.0.0

```
                                              ip mtu 1400
                                    ip nhrp authentication test
                                ip nhrp map 10.0.0.1 172.17.0.1
                                     ip nhrp network-id 100000
                                         ip nhrp holdtime 300
                                         ip nhrp nhs 10.0.0.1
                                                         ...
                                          tunnel key 100000
```

الشبكة الفرعية الآن هي /24 بدلا من /30، لذلك تكون جميع العقد في الشبكة الفرعية نفسها، بدلا من شبكات فرعية مختلفة. كما أن المتحدث ما يزال يرسل عن طريق الصرة حركة مرور تحدث عبر الصرة حيث أنهم يستخدمون واجهة نفق نقطة إلى نقطة GRE. يتم إستخدام أوامر **مصادقة IP nhrp ... وip nhrp network-id ... ومفتاح النفق ...** لتعيين حزم النفق وحزم NHRP إلى واجهة نفق GRE متعددة النقاط الصحيحة وشبكة NHRP عندما يتم استقبالها على الصرة. يتم إستخدام الأوامر **ip nhrp map ... وip nhrp nhs** ... بواسطة NHRP على المكبر للإعلان عن تعيين NHRP للخادم (172.16.<n>.1<1+n> —> 10.0.0.0<1+n>) إلى الموزع. يتم إسترداد عنوان 10.0.0.0<1+n> من **الأمر ip address ...** الأمر الموجود على واجهة النفق و 172.16.<n>.1 العنوان يتم إسترداده من **وجهة النفق ...** الأمر الموجود على واجهة النفق.

في حالة وجود موجهات طريقة 300، سيؤدي هذا التغيير إلى تقليل عدد خطوط التكوين على الموزع من 3900 سطر إلى 16 سطر (تخفيض 3884 سطر). ستتم زيادة التكوين في كل موجه يتم التحدث إليه بمقدار 6 خطوط.

دعم العناوين الديناميكية على القنوات

على موجه Cisco، يلزم تكوين كل نظير IPsec باستخدام عنوان IPsec الخاص بنظير IPsec الآخر قبل إمكانية تحميل نفق IPsec. هناك مشكلة في القيام بهذا إذا كان للموجه الذي يتم التحدث به عنوان ديناميكي على الواجهة المادية الخاصة به، وهو شائع للموجات التي يتم توصيلها عبر DSL أو روابط الكبلات.

يسمح TED لنظير IPsec بالبحث عن نظير IPsec آخر من خلال إرسال حزمة خاصة لاقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) إلى عنوان وجهة IP لحزمة البيانات الأصلية التي يلزم تشفيرها. يكمن الافتراض في أن هذه الحزمة ستعبر الشبكة المتداخلة على نفس المسار كما هو الحال بواسطة حزمة نفق IPsec. سيتم التقاط هذه الحزمة من قبل نظير IPsec الآخر، والذي سيقوم بالاستجابة إلى النظير الأول. بعد ذلك، سيقوم الموجهان بالتفاوض بين اقترانات أمان ISAKMP و IPsec (SAs) وتمهيد نفق IPsec. سيعمل هذا فقط إذا كانت حزم البيانات التي سيتم تشفيرها تحتوي على عناوين IP قابلة للتوجيه.

يمكن إستخدام TED بالاشتراك مع أنفاق GRE كما تم تكوينها في القسم السابق. لقد تم إختبار هذا الأمر ويعمل، على الرغم من وجود خطأ في الإصدارات السابقة من برنامج Cisco IOS حيث فرض TED تشفير جميع حركات مرور IP بين نظاري IPsec، وليس فقط حزم نفق GRE. يوفر حل DMVPN هذه الإمكانيات الإضافية دون أن تضطر الأجهزة المضيفة إلى إستخدام عناوين IP القابلة للتوجيه عبر الإنترنت ودون الاضطرار إلى إرسال حزم أستكشاف واستجابة. مع تعديل بسيط، يمكن إستخدام التكوين من القسم الأخير لدعم الموجهات التي تحتوي على عناوين IP ديناميكية على الواجهات المادية الخارجية الخاصة بها.

موجه الموزع (لا تغيير)

```
crypto ipsec profile vpnprof
  set transform-set trans2
  !
interface Tunnel0
  bandwidth 1000
ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
  ip nhrp holdtime 600
no ip split-horizon eigrp 1
  delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
  tunnel key 100000
tunnel protection ipsec profile vpnprof
  !
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
```

تم التحدث<Router n> (قديم)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
set transform-set trans2
  match address 101
  !
...
  !
.access-list 101 permit gre host 172.16
```

تم التحدث<Router n> (جديد)

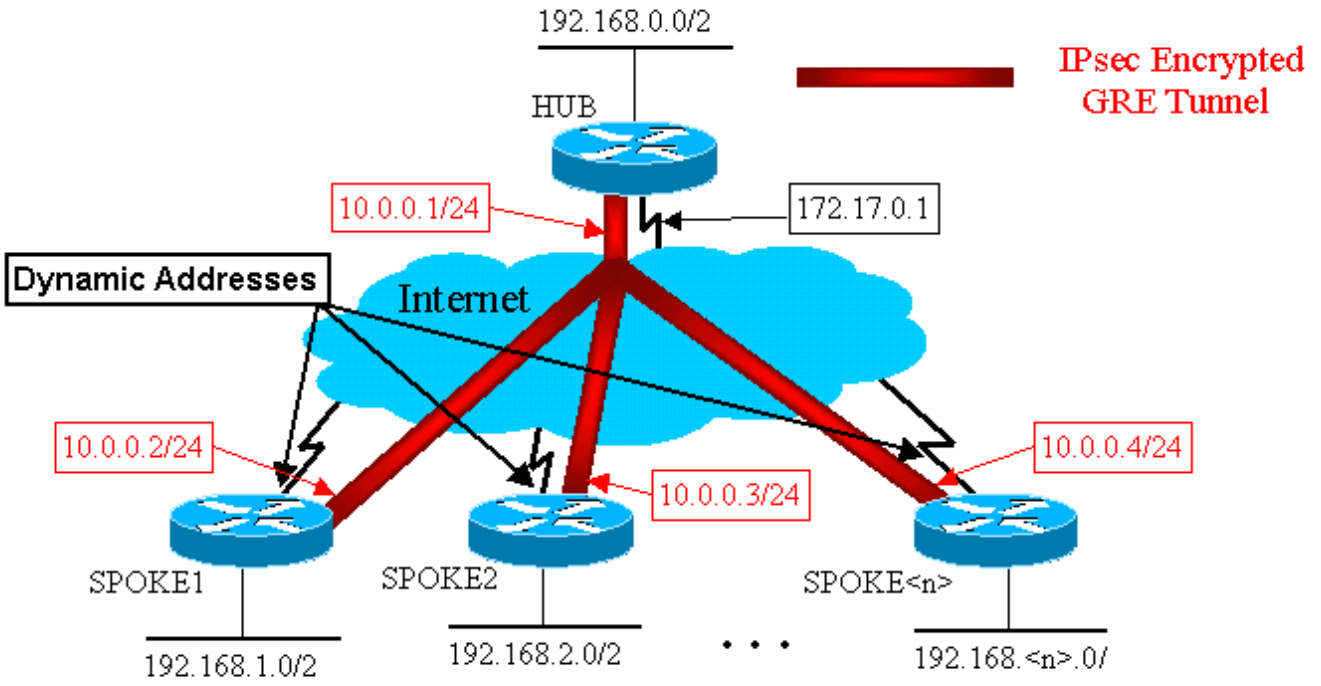
```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
```

```
 set transform-set trans2
 set security-association level per-host
 match address 101
 !
 ...
 !
access-list 101 permit gre any host 172.17.0.1
```

تكون الوظيفة المستخدمة في تكوين الكلام الجديد كما يلي.

- عند ظهور واجهة نفق GRE، ستبدأ في إرسال حزم تسجيل NHRP إلى موجه الموزع. ستؤدي حزم تسجيل NHRP هذه إلى بدء تشغيل IPsec. في الموجه المتصل، يتم تكوين أوامر <peer-address> و**match<acl>** **ip access-list**. تقوم قائمة التحكم في الوصول (ACL) بتحديد GRE كبروتوكول، وأي للمصدر، وعنوان IP للموزع للوجهة.**ملاحظة:** من المهم ملاحظة أنه يتم إستخدام أي منها كمصدر في قائمة التحكم في الوصول (ACL)، ويجب أن يكون هذا هو الحال نظرا لأن عنوان IP الخاص بالموجه المتصل ديناميكي، وبالتالي، غير معروف قبل أن تكون الواجهة المادية نشطة. يمكن إستخدام شبكة IP فرعية للمصدر في قائمة التحكم في الوصول (ACL) إذا تم تقييد عنوان الواجهة التي تتحدث الديناميكية إلى عنوان داخل هذه الشبكة الفرعية.
- يتم إستخدام الأمر **set security-association level per-host** حتى يكون مصدر IP في وكيل IPsec للخادم الفرعي مجرد عنوان الواجهة المادية الحالي (/32)، بدلا من "any" من قائمة التحكم في الوصول (ACL). إذا تم إستخدام "any" من قائمة التحكم في الوصول (ACL) كمصدر في وكيل IPsec، فإنها ستمنع أي موجه آخر تم التحدث عنه من إعداد نفق IPsec+GRE أيضا باستخدام هذا الصرة. وذلك لأن وكيل IPsec الناتج على الموزع سيكون مكافئا **للسماح بالمضيف 172.17.0.1 على أي**. وهذا يعني أنه سيتم تشفير جميع حزم أنفاق GRE الموجهة إلى أي كلمة وإرسالها إلى المحادثة الأولى التي قامت بإنشاء نفق مع الصرة، نظرا لأن وكيل IPsec الخاص به يطابق حزم GRE لكل كلمة.
- بمجرد إعداد نفق IPsec، تنتقل حزمة تسجيل NHRP من الموجه المتصل إلى خادم الخطوة التالية (NHS) الذي تم تكوينه. NHS هو موجه المركز لهذه الشبكة hub-and-talk. توفر حزمة تسجيل NHRP المعلومات لموجه الموزع لإنشاء تعيين NHRP للموجه الذي يتم التحدث به هذا. باستخدام هذا التعيين، يمكن لموجه الموزع بعد ذلك إعادة توجيه حزم بيانات IP للبث الأحادي إلى الموجه الذي يتم التحدث به هذا عبر نفق mGRE+IPsec. أيضا، يضيف الصرة الموجه الموجه الموجه إلى قائمة خرائط NHRP للبث المتعدد. بعد ذلك سيبدأ الموزع بإرسال حزم البث المتعدد للتوجيه الديناميكي ل IP إلى المحادثة (إذا تم تكوين بروتوكول توجيه ديناميكي). عندئذ سيصبح المحادثة أحد جيران بروتوكول التوجيه للمحور، وسيتبادلون تحديثات التوجيه.

IPsec + محور mGRE وتكلم



موجه الموزع

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
```

```
 ip address 192.168.0.1 255.255.255.0
                                      !
                          router eigrp 1
                 network 10.0.0.0 0.0.0.255
               network 192.168.0.0 0.0.0.255
                        no auto-summary
                                      !
```

لاحظ في تكوين الموزع أعلاه أنه لم يتم تكوين عناوين IP الخاصة بالموجهات التي يتم التحدث بها. يتم التعرف بشكل ديناميكي على الواجهة المادية الخارجية للواجهة الكلامية وتخطيط عناوين IP الخاصة بواجهة النفق التي تم التحدث عنها بواسطة الموزع عبر NHRP. وهذا يسمح بتعيين عنوان IP للواجهة المادية الخارجية الخاصة بالمحادثة بشكل ديناميكي.

الموجه TALK1

```
                                 version 12.3
                                      !
                               hostname Spoke1
                                      !
                          crypto isakmp policy 1
                        authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
                                      !
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
                               mode transport
                                      !
          crypto map vpnmap1 local-address Ethernet0
                  crypto map vpnmap1 10 IPsec-isakmp
                           set peer 172.17.0.1
            set security-association level per-host
                         set transform-set trans2
                                match address 101
                                      !
                           interface Tunnel0
                             bandwidth 1000
                  ip address 10.0.0.2 255.255.255.0
                                 ip mtu 1400
              ip nhrp authentication test
            ip nhrp map 10.0.0.1 172.17.0.1
                 ip nhrp network-id 100000
                      ip nhrp holdtime 300
                      ip nhrp nhs 10.0.0.1
                                delay 1000
                    tunnel source Ethernet0
              tunnel destination 172.17.0.1
                         tunnel key 100000
                                      !
                        interface Ethernet0
                  ip address dhcp hostname Spoke1
                         crypto map vpnmap1
                                      !
                        interface Ethernet1
          ip address 192.168.1.1 255.255.255.0
                                      !
                           router eigrp 1
                 network 10.0.0.0 0.0.0.255
               network 192.168.1.0 0.0.0.255
                        no auto-summary
                                      !
  access-list 101 permit gre 172.16.1.0 0.0.0.255 host
```

172.17.0.1

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
set peer 172.17.0.1
set security-association level per-host
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.3 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
ip address dhcp hostname Spoke2
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre 172.16.2.0 0.0.0.255 host
172.17.0.1
```

الأشياء الأساسية التي يجب ملاحظتها حول التكوينات التي يتم التحدث بها هي:

- عنوان IP للواجهة المادية الخارجية (Ethernet0) ديناميكي عبر DHCP.**عنوان ip dhcp hostname talk2**
- تحدد قائمة التحكم في الوصول (ACL) للتشفير (101) شبكة فرعية كمصدر لوكيل IPsec.**قائمة الوصول 101 قائمة السماح 172.16.2.0.0.0.255 GRE المضيف 172.17.0.1**
- يحدد الأمر التالي في خريطة تشفير IPsec أن اقتران الأمان سيكون لكل مضيف.**تعيين مستوى اقتران الأمان لكل مضيف**
- تعد جميع الأنفاق جزءا من الشبكة الفرعية نفسها، نظرا لأنها جميعا تتصل عبر واجهة GRE متعددة النقاط

نفسها على موجه الموزع.**عنوان IP 10.0.0.2 255.255.255.0**
يؤدي الجمع بين هذه الأوامر الثلاثة إلى عدم ضرورة تكوين عنوان IP للواجهة المادية الخارجية الخاصة بالمحادثة. سيكون وكيل IPsec الذي يتم إستخدامه مستندا إلى المضيف بدلا من اعتماده على الشبكات الفرعية.

يحتوي التكوين الموجود على الموجهات التي يتم التحدث بها على عنوان IP الخاص بموجه الصرة الذي تم تكوينه، نظرا لأنه يحتاج إلى بدء نفق IPsec+GRE. لاحظ التشابه بين تكوينات Talk1 و Talk2. لا يوجد هذان التماثلان فقط، ولكن جميع تكوينات الموجه الموجه الذي يتم التحدث به ستكون متشابهة. في معظم الحالات، تحتاج جميع الفروع ببساطة عناوين IP فريدة على الواجهات الخاصة بها، وسوف تكون بقية التكوينات الخاصة بها هي نفسها. وهذا يجعل من الممكن تكوين العديد من الموجهات التي يتم نطقها ونشرها بسرعة.

تبدو بيانات NHRP كما يلي على لوحة الوصل.

موجه الموزع

```
Hub#show ip nhrp
via 10.0.0.2, Tunnel0 created 01:25:18, 10.0.0.2/32
                                        expire 00:03:51
       Type: dynamic, Flags: authoritative unique
                                                registered
                          NBMA address: 172.16.1.4
via 10.0.0.3, Tunnel0 created 00:06:02, 10.0.0.3/32
                                        expire 00:04:03
       Type: dynamic, Flags: authoritative unique
                                                registered
                        NBMA address: 172.16.2.10
                                                    ...
     n>/32 via 10.0.0.<n>, Tunnel0 created>.10.0.0
                                00:06:00, expire 00:04:25
       Type: dynamic, Flags: authoritative unique
                                                registered
                      NBMA address: 172.16.<n>.41
```

الموجه TALK1

```
Spoke1#sho ip nhrp
   via 10.0.0.1, Tunnel0 created 4d08h, 10.0.0.1/32
                                          never expire
              Type: static, Flags: authoritative
                          NBMA address: 172.17.0.1
```

الموزع الديناميكي متعدد النقاط

لا يعتمد التكوين على الموجهات التي يتم التحدث بها أعلاه على ميزات من حل DMVPN، لذلك يمكن أن تقوم الموجهات التي يتم التحدث بها بتشغيل إصدارات برنامج Cisco IOS software قبل الإصدار 12.2(13)T. يعتمد التكوين على موجه الموزع على ميزات DMVPN، لذلك يجب أن تقوم بتشغيل Cisco IOS، الإصدار 12.2(13)T أو الأحدث. يتيح لك هذا بعض المرونة في تحديد الوقت الذي تحتاج فيه إلى ترقية الموجهات التي يتم التحدث بها والتي تم نشرها بالفعل. إذا كانت الموجهات التي تتحدث عنها تعمل أيضا بنظام التشغيل Cisco IOS الإصدار 12.2(13)T أو إصدار أحدث، فيمكنك تبسيط التكوين الذي يتم التحدث به كما يلي.

تحدث<n> الموجه (قبل Cisco IOS 12.2(13)T)

```
crypto map vpnmap1 10 IPsec-isakmp
```

```
set peer 172.17.0.1
set security-association level per-host
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
<ip address dhcp hostname Spoke<n
crypto map vpnmap1
!
. . .
!
access-list 101 permit gre any host 172.17.0.1
```

تحدث<n> الموجه (بعد Cisco IOS 12.2(13)T)

```
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
<ip address dhcp hostname Spoke<n
!
```

لاحظ أننا قمنا بما يلي:

1. تمت إزالة الأمر **crypto map vpnmap1 10 ipSec-isakmp** واستبداله ب **crypto ipSec profile vpnprof**.
2. تمت إزالة الأمر **crypto map vpnmap1** من واجهات Ethernet0 ووضع الأمر **tunnel protection ipSec profile vpnprof** على واجهة Tunnel0.
3. تمت إزالة قائمة التحكم في الوصول (ACL) للتشفير، **ويسمح قائمة الوصول 101 بأي مضيف 172.17.0.1**.

في هذه الحالة، يتم اشتقاق عناوين ووكلاء نظير IPsec تلقائيا من **مصدر النفق** ...**ووجهة النفق** ... التكوين. تكون النظراء والوكلاء كما يلي (كما هو موضح في الأمر الناتج من **show crypto ipSec**):

```
...
(local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0
(remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

باختصار، تتضمن التكوينات الكاملة التالية جميع التغييرات التي تم إجراؤها حتى هذه النقطة من التكوين الأساسي (محور IPsec+GRE والمتكلم).

موجه الموزع

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.1 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.0.255
no auto-summary
!
```

لا توجد تغييرات في تكوين الصرة.

الموجه TALK1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke2
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
```

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.3 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
```

```
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
```

Dynamic Multipoint IPsec VPN

تظهر المفاهيم والتكوين في هذا القسم القدرات الكاملة ل DMVPN. يوفر NHRP إمكانية الموجهات التي يتم التحدث بها للتعرف بشكل ديناميكي على عنوان الواجهة المادية الخارجية للموجهات الأخرى التي يتم التحدث بها في شبكة VPN. وهذا يعني أن الموجه الذي يتم التحدث به سيتوفر على معلومات كافية لبناء نفق IPsec+mGRE بشكل ديناميكي للوصول مباشرة إلى الموجهات التي يتم التحدث بها الأخرى. وهذا أمر مفيد نظرا لأنه، إذا تم إرسال حركة مرور البيانات التي يتم التحدث بها هذه عبر موجه الموزع، فيجب تشفيرها/فك تشفيرها، مما يزيد التأخير مرتين والحمل على موجه الموزع. لاستخدام هذه الميزة، يلزم تبديل الموجهات التي يتم التحدث بها من واجهات نفق GRE من نقطة إلى نقطة (p-pGRE) إلى GRE متعدد النقاط (mGRE). كما يحتاجون إلى تعلم الشبكات (الفرعية) المتوفرة خلف القنوات الأخرى باستخدام عنوان IP للخطوة التالية في النفق الخاص بعنوان IP الخاص بالموجه الآخر الذي يتم التحدث به. تتعرف الموجهات التي يتم التحدث عليها على هذه الشبكات (الفرعية) عبر بروتوكول توجيه IP الديناميكي الذي يعمل عبر نفق IPsec+mGRE مع الصرة.

يمكن تكوين بروتوكول توجيه IP الديناميكي الذي يتم تشغيله على موجه المحور ليعكس المسارات التي تم تعلمها من أحدهم عبر نفس الواجهة إلى جميع المحولات الأخرى، ولكن الخطوة التالية ل IP على هذه المسارات ستكون عادة موجه المحور، وليس الموجه الذي يتم التحدث والذي تعلم منه الصرة هذا المسار.

ملاحظة: يعمل بروتوكول التوجيه الديناميكي فقط على إرتباطات المحولات والمحطات، ولا يعمل على إرتباطات المحادثات المباشرة الديناميكية.

يلزم تكوين بروتوكولات التوجيه الديناميكية (RIP و OSPF و EIGRP) على موجه الموزع للإعلان عن المسارات من واجهة نفق MGRE ولتعيين الخطوة التالية ل IP إلى الموجه الذي يتم إصداره للمسارات التي يتم التعرف عليها من أحد المتكلمين عند الإعلان عن المسار مرة أخرى إلى الخوادم الفرعية الأخرى.

فيما يلي متطلبات لتكوينات بروتوكول التوجيه.

شق

أنت تحتاج أن يلتفت أفق انقسام على واجهة نفق mGRE على الصرة، وإلا فإن RIP لن يعلن عن المسارات التي تم التعرف عليها عبر واجهة mGRE ستخرج تلك الواجهة نفسها.

```
no ip split-horizon
```

لا توجد تغييرات أخرى ضرورية. يستخدم RIP تلقائيا المرحلة التالية من IP الأصلية على الموجهات التي يعلن عنها في نفس الواجهة حيث تعلم هذه الموجهات.

EIGRP

أنت تحتاج أن يلتفت أفق منقسم على ال mGRE نفق قارن على الصرة، خلاف ذلك EIGRP لن يعلن الطريق يعلم عن طريق ال mGRE قارن back to نفسه قارن.

```
no ip split-horizon eigrp
```

سيقوم EIGRP، بشكل افتراضي، بتعيين IP Next-hop إلى موجه المحور للمسارات التي يقوم بالإعلان عنها، حتى عند الإعلان عن هذه المسارات مرة أخرى من نفس الواجهة التي تتعلمها بها. لذلك في هذه الحالة، تحتاج إلى أمر التكوين التالي لتوجيه EIGRP لاستخدام الخطوة التالية الأصلية IP عند الإعلان عن هذه المسارات.

```
no ip next-hop-self eigrp
```

ملاحظة: سيكون **الأمر no ip next-hop-self eigrp <as>** متوفرا بدءا من Cisco IOS الإصدار 12.3(2). بالنسبة لإصدارات Cisco IOS بين 12.2(13)T و 12.3(2)، يجب القيام بما يلي:

- إذا كانت الأنفاق الديناميكية التي يتم التحدث إليها غير مطلوبة، فلا حاجة إلى الأمر أعلاه.
- إذا كانت الأنفاق الديناميكية التي يتم التحدث بها مطلوبة، فيجب عليك إستخدام تحويل العملية على واجهة النفق على الموجهات التي يتم التحدث بها.
- وإلا، ستحتاج إلى إستخدام بروتوكول توجيه مختلف عبر DMVPN.

بروتوكول أقصر مسار أولاً (OSPF)

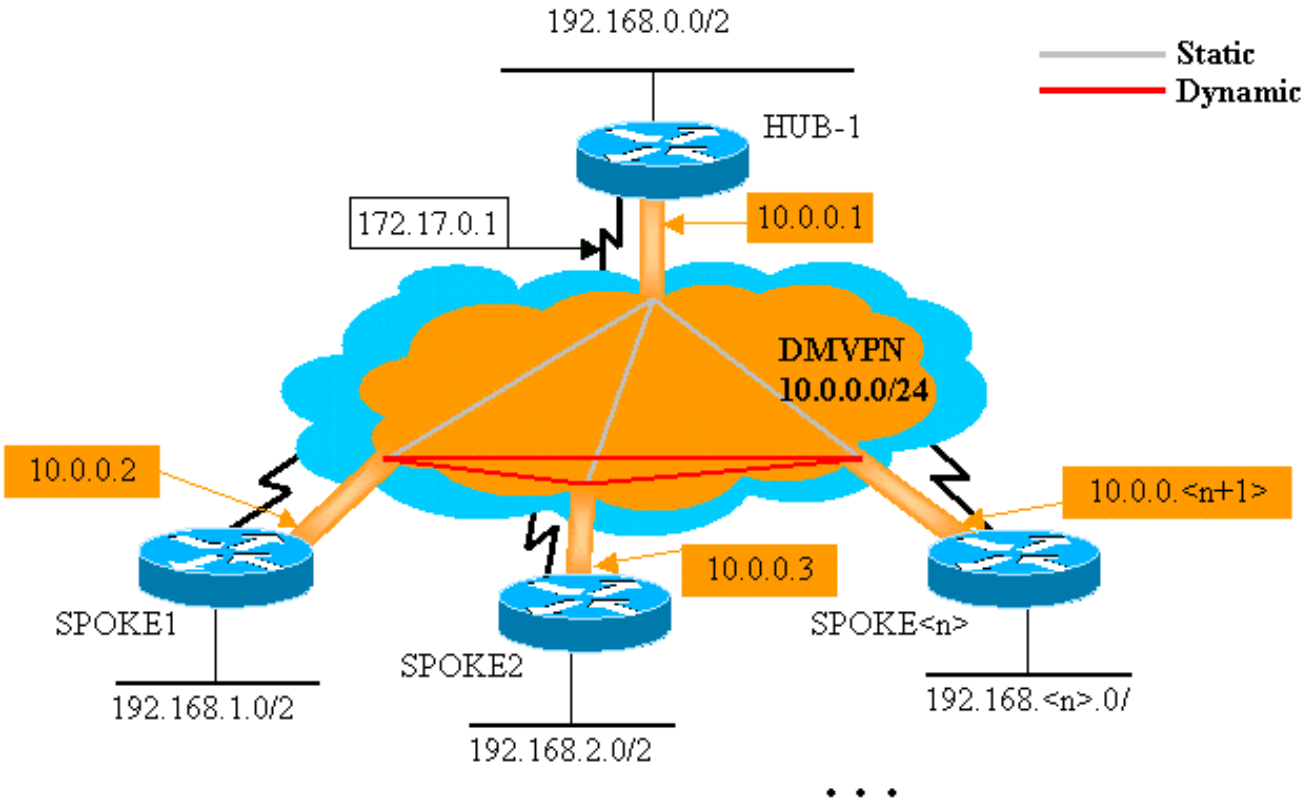
بما أن OSPF هو بروتوكول توجيه حالة الارتباط، فلا توجد أي مشاكل في أفق التقسيم. عادة لواجهات النقاط المتعددة، تقوم بتكوين نوع شبكة OSPF ليكون من نقطة إلى عدة نقاط، ولكن هذا قد يتسبب في قيام OSPF بإضافة مسارات مضيف إلى جدول التوجيه على الموجهات التي يتم التحدث بها. وستتسبب مسارات المضيفين هذه في إعادة توجيه الحزم الموجهة إلى الشبكات خلف الموجهات الأخرى عبر الصرة، بدلا من إعادة توجيهها مباشرة إلى الموصلات الأخرى. للالتفاف حول هذه المشكلة، قم بتكوين نوع شبكة OSPF للبث باستخدام الأمر.

```
ip ospf network broadcast
```

تحتاج أيضا إلى التأكد من أن موجه الموزع سيكون الموجه المعين (DR) لشبكة IPsec+mGRE. ويتم القيام بذلك من خلال تعيين أولوية OSPF لتكون أكبر من 1 على الموزع و 0 على القبضات.

- الموزع: أولوية IP OSPF 2
- تم التحدث: أولوية IP OSPF 0

الموزع الواحد DMVPN



موجه الموزع

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip ospf network broadcast
 ip ospf priority 2
 delay 1000
 tunnel source Ethernet0
```

```
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
```

التغيير الوحيد في تكوين الصرة هو أن OSPF هو بروتوكول التوجيه بدلا من EIGRP. لاحظ أنه تم تعيين نوع شبكة OSPF على البث وتم تعيين الأولوية على 2. سيؤدي تعيين نوع شبكة OSPF على البث إلى قيام OSPF بتثبيت المسارات للشبكات خلف الموجهات الفرعية باستخدام عنوان IP للخطوة التالية كعنوان نفق GRE للموجه الذي يتحدث.

الموجه TALK1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router ospf 1
```

```
network 10.0.0.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
!
```

التشكيل على ال يتحدث مسحاج تخديد الآن جدا مماثل إلى التشكيل على الصرة. والاختلافات هي كما يلي:

- يتم تعيين أولوية OSPF على 0. لا يمكن السماح للموجهات التي يتم التحدث بها لتصبح DR لشبكة NBMA للوصول المتعدد غير للبث لشبكة mGRE. يتلقى فقط موجه الموزع إتصالات ثابتة مباشرة إلى كل الموجهات التي يتم التحدث بها. يجب أن يتمتع DR بإمكانية الوصول إلى جميع أعضاء شبكة NBMA.
- هناك تعيينات بث NHRP الأحادي والبث المتعدد التي تم تكوينها لموجه الموزع.

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

في التكوين السابق، لم يكن الأمر **ip nhrp map multicast ...** مطلوبا نظرا لأن نفق GRE كان من نقطة إلى نقطة. في تلك الحالة، multicast غلف ربط تلقائيا من خلال النفق إلى الواحد يمكن غاية. هذا أمر ضروري الآن لأن نفق GRE للمعلمات قد تغير إلى متعدد النقاط وهناك أكثر من واحد ممكن غاية.

- عند ظهور الموجه الذي يتم التحدث به، يجب أن يبدأ اتصال النفق مع الصرة، نظرا لعدم تكوين موجه الصرة بأي معلومات حول الموجهات التي يتم التحدث بها، وقد تكون الموجهات التي يتم التحدث بها قد تم تعيين عناوين IP بشكل ديناميكي. كما يتم تكوين الموجهات التي يتم التحدث بها باستخدام الموزع كوحدات NHRP الخاصة بها.

```
ip nhrp nhs 10.0.0.1
```

باستخدام الأمر أعلاه، سيقوم الموجه الذي يتحدث بإرسال حزم تسجيل NHRP من خلال نفق mGRE+IPsec إلى موجه الموزع على فواصل زمنية منتظمة. توفر حزم التسجيل هذه معلومات تعيين NHRP التي يتم التحدث بها والتي تكون مطلوبة من قبل موجه الموزع لنفق الحزم مرة أخرى إلى الموجهات التي يتم التحدث بها.

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
```

```
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.3.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

تم التحديث<Router n>

```
version 12.3
!
<hostname Spoke<n
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+1> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 <ip address dhcp hostname Spoke<n
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 .network 192.168
!
```

لاحظ أن تكوينات جميع الموجهات التي يتم الحديث عنها متشابهة للغاية. الفروق الوحيدة هي عناوين IP على الواجهات المحلية. يساعد ذلك عند نشر عدد كبير من الموجهات التي يتم التحدث عنها. يمكن تكوين جميع الموجهات التي يتم التحدث بها بشكل متماثل، ويلزم إضافة عناوين واجهة IP المحلية فقط.

عند هذه النقطة، ألق نظرة على جداول التوجيه وجداول خرائط NHRP على الموجهات Hub، Talk1، و Talk2 للاطلاع على الشروط الأولية (بعد ظهور موجهات Talk1 و Talk2 مباشرة) والظروف بعد Talk1 و Talk2 خلقت رابط ديناميكي بينها.

الشروط الأولية

معلومات موجه الموزع

```
Hub#show ip route
          is subnetted, 1 subnets 172.17.0.0/24
C       172.17.0.0 is directly connected, Ethernet0
          is subnetted, 1 subnets 10.0.0.0/24
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet1
O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:19:53,
                                                Tunnel0
O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:19:53,
                                                Tunnel0
Hub#show ip nhrp
    via 10.0.0.2, Tunnel0 created 00:57:27, 10.0.0.2/32
                                          expire    00:04:13
Type: dynamic, Flags: authoritative unique registered
                              NBMA address: 172.16.1.24
    via 10.0.0.3, Tunnel0 created 07:11:25, 10.0.0.3/32
                                          expire    00:04:33
Type: dynamic, Flags: authoritative unique registered
                              NBMA address: 172.16.2.75
Hub#show crypto engine connection active
         ID  Interface   IP-Address    State Algorithm
                                           Encrypt Decrypt
Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB 204
                                                0       0
Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB 205
                                                0       0
          Tunnel0     10.0.0.1       set  HMAC_MD5 2628
                                                0     402
          Tunnel0     10.0.0.1       set  HMAC_MD5 2629
                                              357       0
          Tunnel0     10.0.0.1       set  HMAC_MD5 2630
                                                0     427
          Tunnel0     10.0.0.1       set  HMAC_MD5 2631
                                              308       0
```

معلومات الموجه TALK1

```
Spoke1#show ip route
          is subnetted, 1 subnets 172.16.0.0/24
C       172.16.1.24 is directly connected, Ethernet0
          is subnetted, 1 subnets 10.0.0.0/24
C       10.0.0.0 is directly connected, Tunnel0
O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:31:46,
                                                Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet1
O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:31:46,
```

```
                                                    Tunnel0
                                        Spoke1#show ip nhrp
    via 10.0.0.1, Tunnel0 created 01:42:00, 10.0.0.1/32
                                                  never expire
              Type: static, Flags: authoritative used
                                  NBMA address: 172.17.0.1
            Spoke1#show crypto engine connection active
         ID  Interface   IP-Address    State Algorithm
                                                Encrypt Decrypt
Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB 2
                                                      0       0
          Tunnel0     10.0.0.2       set  HMAC_MD5 2064
                                                      0     244
          Tunnel0     10.0.0.2       set  HMAC_MD5 2065
                                                    276       0
```

معلومات الموجه TALK2

```
                                        Spoke2#show ip route
             is subnetted, 1 subnets 172.16.0.0/24
    C       172.16.2.0 is directly connected, Ethernet0
               is subnetted, 1 subnets 10.0.0.0/24
        C       10.0.0.0 is directly connected, Tunnel0
    O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:38:52,
                                                    Tunnel0
    O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:38:52,
                                                    Tunnel0
   C    192.168.2.0/24 is directly connected, Ethernet1
                                        Spoke2#show ip nhrp
    via 10.0.0.1, Tunnel0 created 01:32:10, 10.0.0.1/32
                                                  never expire
              Type: static, Flags: authoritative used
                                  NBMA address: 172.17.0.1
            Spoke2#show crypto engine connection active
         ID  Interface   IP-Address    State Algorithm
                                                Encrypt Decrypt
Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB 17
                                                      0       0
          Tunnel0     10.0.0.3       set  HMAC_MD5 2070
                                                      0     279
          Tunnel0     10.0.0.3       set  HMAC_MD5 2071
                                                    316       0
```

عند هذه النقطة، نقفز من 192.168.1.2 إلى 192.168.2.3. تكون هذه العناوين لمضيفين وراء الموجهات Talk1 و Talk2، على التوالي. يتم تنفيذ تسلسل الأحداث التالي لبناء نفق mGRE+IPsec الذي يتم التحدث إليه مباشرة.

1. يستلم موجه Talk1 حزمة إختبار الاتصال مع الوجهة 192.168.2.3. تبحث عن هذه الوجهة في جدول التوجيه وتجد أنها تحتاج إلى إعادة توجيه هذه الحزمة خارج واجهة Tunnel0 إلى واجهة 10.0.0.3، IP Nexthop.
2. يتحقق الموجه Talk1 من جدول تعيين NHRP للوجهة 10.0.0.3 ويجد أنه لا يوجد إدخال. يقوم الموجه Talk1 بإنشاء حزمة طلب تحليل NHRP وإرسالها إلى NHS (موجه الموزع).
3. يتحقق الموجه الموزع من جدول تعيين NHRP الخاص به للوجهة 10.0.0.3 ويجد أنه يترجم إلى العنوان 172.16.2.75. يقوم موجه الموزع بإنشاء حزمة رد على تحليل NHRP وإرسالها إلى الموجه Talk1.
4. يتلقى الموجه Talk1 الرد على تحليل NHRP، ويدخل تعيين 10.0.0.3 —>172.16.2.75 في جدول خرائط NHRP الخاص به. تؤدي إضافة تعيين NHRP إلى تشغيل IPsec لبدء نفق IPsec مع النظير 172.16.2.75.
5. يقوم موجه Talk1 ببدء ISAKMP باستخدام 172.16.2.75 والتفاوض على وكيل خدمة ISAKMP و IPsec. يتم اشتقاق وكيل IPsec من أمر **<address>مصدر النفق0** وتخطيط NHRP.

```
(local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0
```

```
(remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0
```

6. بمجرد انتهاء بناء نفق IPsec، يتم إرسال جميع حزم البيانات الإضافية إلى الشبكة الفرعية 24/192.168.2.0 مباشرة إلى Talk2.
7. بعد إعادة توجيه الحزمة الموجهة إلى 192.168.2.3 إلى المضيف، سيقوم هذا المضيف بإرسال حزمة إرجاع إلى 192.168.1.2. عندما يستقبل موجه TALK2 هذه الحزمة الموجهة إلى 192.168.1.2، سيقوم بالبحث عن هذه الوجهة في جدول التوجيه والعثور على أنه يحتاج إلى إعادة توجيه هذه الحزمة من واجهة Tunnel0 إلى الخطوة التالية 10.0.0.2، IP.
8. يتحقق الموجه Talk2 من جدول تعيين NHRP للوجهة 10.0.0.2 ويجد أنه لا يوجد إدخال. يقوم الموجه TALK2 بإنشاء حزمة طلب تحليل NHRP وإرسالها إلى NHS (موجه الموزع).
9. يتحقق الموجه الموزع من جدول تعيين NHRP الخاص به للوجهة 10.0.0.2 ويجد أنه يترجم إلى العنوان 172.16.1.24. يقوم موجه الموزع بإنشاء حزمة رد على دقة NHRP وإرسالها إلى الموجه TALK2.
10. يتلقى الموجه TALK2 الرد على تحليل NHRP، ويدخل تعيين 10.0.0.2 —> 172.16.1.24 في جدول خرائط NHRP الخاص به. تؤدي إضافة تعيين NHRP إلى تشغيل IPsec لبدء نفق IPsec مع النظير 172.16.1.24، ولكن هناك بالفعل نفق IPsec مع النظير 172.16.1.24، وبالتالي لا يلزم القيام بأي شيء آخر.
11. يمكن الآن للخطين TALK1 و TALK2 إعادة توجيه الحزم مباشرة إلى بعضها البعض. عند عدم إستخدام تعيين NHRP لإعادة توجيه الحزم لوقت الرفض، سيتم حذف تعيين NHRP. سيؤدي حذف إدخال تعيين NHRP إلى تشغيل IPsec لحذف شبكات IPsec الخاصة بهذا الارتباط المباشر.

شروط بعد إنشاء إرتباط ديناميكي بين Talk1 و Talk2

معلومات الموجه TALK1

```
Spoke1#show ip nhrp
10.0.0.1, Tunnel0 created 02:34:16, 10.0.0.1/32 via
                                            never expire
          Type: static, Flags: authoritative used
                       NBMA address: 172.17.0.1
10.0.0.3, Tunnel0 created 00:00:05, 10.0.0.3/32 via
                                          expire 00:03:35
          Type: dynamic, Flags: router unique used
                       NBMA address: 172.16.2.75
Spoke1#show crypto engine connection active
     ID  Interface   IP-Address     State Algorithm
                                          Encrypt Decrypt
Ethernet0   172.16.1.24     set  HMAC_SHA+DES_56_CB 2
                                             0       0
Ethernet0   172.16.1.24     set  HMAC_SHA+DES_56_CB 3
                                             0       0
         Tunnel0     10.0.0.2       set  HMAC_MD5 2064
                                             0     375
         Tunnel0     10.0.0.2       set  HMAC_MD5 2065
                                           426       0
         Tunnel0     10.0.0.2       set  HMAC_MD5 2066
                                             0      20
         Tunnel0     10.0.0.2       set  HMAC_MD5 2067
                                            19       0
```

معلومات الموجه TALK2

```
Spoke2#show ip nhrp
10.0.0.1, Tunnel0 created 02:18:25, 10.0.0.1/32 via
                                            never expire
```

```
            Type: static, Flags: authoritative used
                                  NBMA address: 172.17.0.1
    via 10.0.0.2, Tunnel0 created 00:00:24, 10.0.0.2/32
                                                expire 00:04:35
            Type: dynamic, Flags: router unique used
                                  NBMA address: 172.16.1.24
          Spoke2#show crypto engine connection active
        ID  Interface   IP-Address      State Algorithm
                                                Encrypt Decrypt
Ethernet0   172.16.2.75     set  HMAC_SHA+DES_56_CB 17
                                                      0       0
Ethernet0   172.16.2.75     set  HMAC_SHA+DES_56_CB 18
                                                      0       0
          Tunnel0     10.0.0.3        set  HMAC_MD5 2070
                                                      0     407
          Tunnel0     10.0.0.3        set  HMAC_MD5 2071
                                                    460       0
          Tunnel0     10.0.0.3        set  HMAC_MD5 2072
                                                      0      19
          Tunnel0     10.0.0.3        set  HMAC_MD5 2073
                                                     20       0
```

من الإخراج أعلاه يمكنك أن ترى أن Talk1 و Talk2 حصلا على تعيينات NHRP لبعضهما البعض من موجه الموزع، وقد قاما ببناء نفق mGRE+IPsec واستخدامه. ستنتهي صلاحية تعيينات NHRP بعد خمس دقائق (القيمة الحالية لوقت NHRP = 300 ثانية). إذا تم إستخدام تعيينات NHRP في الدقيقة الأخيرة قبل انتهاء صلاحيتها، فسيتم إرسال طلب تحليل NHRP ورد لتحديث الإدخال قبل حذفه. وإلا، سيتم حذف تعيين NHRP وسيؤدي ذلك إلى تشغيل IPsec لمسح شبكات IPsec.

الشبكة الخاصة الظاهرية (VPN) متعددة النقاط الديناميكية من IPsec مع لوحات التوزيع المزدوجة

من خلال عدد قليل من خطوط التكوين الإضافية للموجهات التي يتم التحدث بها، يمكنك إعداد موجهات جهات جهات مزدوجة (أو متعددة)، لإتاحة إمكانية التكرار. هناك طريقتان لتكوين شبكات DMVPN مزدوجة المحور.

- تحدثت شبكة DMVPN واحدة مع كل منها باستخدام واجهة نفق GRE متعددة النقاط الواحدة، وأشارت إلى محورين مختلفين على أنهما خادمها التالي (NHS).سيكون لموجهات الصرة واجهة نفق GRE واحدة متعددة النقاط فقط.
- تحدثت شبكات DMVPN المزدوجة مع كل منها عن وجود واجهات GRE Tunnel (إما من نقطة إلى نقطة أو متعددة النقاط) وكل نفق GRE متصل بموجه محور مختلف.مرة أخرى، سيكون لموجهات الموزع فقط واجهة نفق GRE متعددة النقاط.

ستنظر الأمثلة التالية في تكوين هذين السيناريوهين المختلفين لشبكات DMVPN مزدوجة الوجهات. في كلتا الحالتين، تكون الفروق المبرزة مرتبطة بتكوين محور DMVPN المفرد.

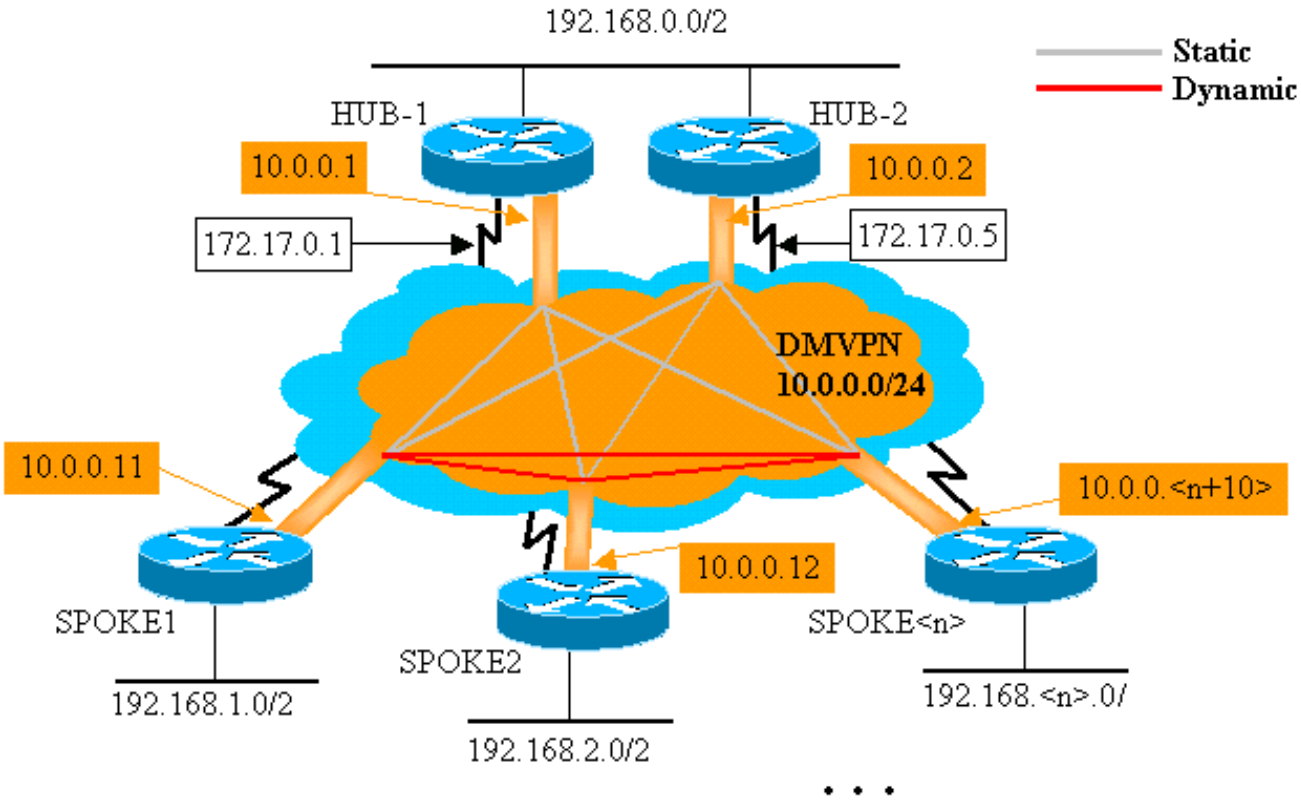
الموزع المزدوج - تخطيط DMVPN أحادي

من السهل إلى حد ما إعداد الموزع المزدوج المزود بتخطيط DMVPN واحد، ولكنه لا يمنحك التحكم في التوجيه عبر DMVPN بنفس قدر التحكم الذي يمنحك إياه الموزع المزدوج المزود بتخطيط DMVPN المزدوج. تتمثل الفكرة في هذه الحالة في وجود "سحابة" واحدة لشبكة DMVPN تتضمن جميع المحاور (إثنان في هذه الحالة) وجميع المحولات المتصلة بهذه الشبكة الفرعية ("السحابة"). تحدد تعيينات NHRP الثابتة من الفروع إلى المحاور روابط IPsec+mGRE الثابتة التي سيعمل عليها بروتوكول التوجيه الديناميكي. لن يتم تشغيل بروتوكول التوجيه الديناميكي عبر إرتباطات IPsec+mGRE الديناميكية بين الفروع. بما أن الموجهات التي يتم التحدث بها تقوم بتوجيه الجيران باستخدام موجهات المحور عبر واجهة نفق MGRE نفسها، فلا يمكنك إستخدام إختلافات الارتباطات أو الواجهات (مثل المقياس أو التكلفة أو التأخير أو النطاق الترددي) لتعديل مقاييس بروتوكول التوجيه الديناميكي لتفضيل موزع واحد

على الموزع الآخر عندما تكون كلا الموجهين فوق. إن يحتاج هذا تفضيل يكون، بعد ذلك تقنيات داخلي إلى التشكيل من التوجيه بروتوكول ينبغي استعملت. لهذا السبب، قد يكون من الأفضل إستخدام EIGRP أو RIP بدلا من OSPF لبروتوكول التوجيه الديناميكي.

ملاحظة: عادة ما تكون المشكلة المذكورة أعلاه مشكلة فقط في حالة وجود موجهات المحاور في موقع واحد. عندما لا تكون موجودة في الموقع المشترك، من المرجح أن ينتهي الأمر بالتوجيه الديناميكي العادي إلى تفضيل موجه المحولات الصحيح، حتى إذا كان من الممكن الوصول إلى الشبكة الوجهة عبر أي من موجهات المحولات.

الموزع المزدوج - تخطيط DMVPN أحادي



موجه الموزع

```
version 12.3
!
hostname Hub1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
```

```
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip ospf network broadcast
 ip ospf priority 2
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
 !
 router ospf 1
 network 10.0.0.0 0.0.0.255 area 1
 network 192.168.0.0 0.0.0.255 area 0
 !
```

الموجه Hub2 Router

```
version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 900
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map  multicast 172.17.0.1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
 ip address 172.17.0.5 255.255.255.0
 !
 interface Ethernet1
```

```
 ip address 192.168.0.2 255.255.255.0
                                    !
                          router ospf 1
                  network 10.0.0.0 0.0.0.255 area 1
                network 192.168.0.0 0.0.0.255 area 0
                                    !
```

التغيير الوحيد في تكوين Hub1 هو تغيير OSPF لاستخدام منطقتين. يتم إستخدام المنطقة 0 للشبكة الموجودة خلف المحورين، كما يتم إستخدام المنطقة 1 لشبكة DMVPN والشبكات الموجودة خلف الموجهات التي يتم التحدث بها. يمكن أن يستخدم OSPF منطقة واحدة، ولكن تم إستخدام منطقتين هنا لبيان تكوين مناطق OSPF متعددة.

التكوين ل Hub2 هو أساسا نفس تكوين Hub1 مع تغييرات عنوان IP المناسبة. يكمن الاختلاف الرئيسي الوحيد في أن Hub2 هو أيضا موزع (أو عميل) Hub1، يجعل Hub1 هو الموزع الرئيسي و Hub2 هو الموزع الثانوي. ويتم القيام بذلك حتى يكون Hub2 مجاور OSPF مع Hub1 عبر نفق mGRE. بما أن Hub1 هو OSPF DR، فيجب أن يكون له اتصال مباشر مع جميع موجهات OSPF الأخرى عبر واجهة mGRE (شبكة NBMA). بدون الارتباط المباشر بين Hub1 و Hub2، لن يشارك Hub2 في توجيه OSPF عندما يكون Hub1 قيد التشغيل أيضا. عندما يكون Hub1 معطلا، سيكون Hub2 هو OSPF DR for the DMVPN (شبكة NBMA). عندما يعود Hub1، سيأخذ على عاتقه أن يكون OSPF DR ل DMVPN.

سوف تستخدم الموجهات خلف Hub1 و Hub1 Hub2 لإرسال الحزم إلى الشبكات التي تم التحدث بها لأن النطاق الترددي لواجهة نفق GRE تم تعيينه على 1000 كيلوبت/ثانية مقابل 900 كيلوبت/ثانية على Hub2. في المقابل، ستقوم الموجهات التي يتم التحدث بها بإرسال حزم للشبكات الموجودة خلف موجهات الصرة إلى كل من Hub1 و Hub2، نظرا لوجود واجهة نفق MGRE واحدة فقط على كل موجه يتم التحدث إليه وسيكون هناك طريقان متساويان للتكلفة. إذا تم إستخدام موازنة الحمل لكل حزمة، فقد يؤدي ذلك إلى عدم ترتيب الحزم.

الموجه TALK1

```
                                version 12.3
                                    !
                              hostname Spoke1
                                    !
                          crypto isakmp policy 1
                           authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
                                    !
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
                             mode transport
                                    !
                        crypto ipsec profile vpnprof
                           set transform-set trans2
                                    !
                                interface Tunnel0
                                  bandwidth 1000
                ip address 10.0.0.11 255.255.255.0
                                     ip mtu 1400
                          ip nhrp authentication test
                    ip nhrp map multicast 172.17.0.1
                     ip nhrp map 10.0.0.1 172.17.0.1
                    ip nhrp map multicast 172.17.0.5
                     ip nhrp map 10.0.0.2 172.17.0.5
                           ip nhrp network-id 100000
                                ip nhrp holdtime 300
                                    ip nhrp nhs 10.0.0.1
                                    ip nhrp nhs 10.0.0.2
                           ip ospf network broadcast
                                 ip ospf priority 0
                                         delay 1000
                          tunnel source Ethernet0
```

```
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
 ip address dhcp hostname Spoke1
 !
 interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
 !
 router ospf 1
 network 10.0.0.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.255 area 1
 !
```

فيما يلي الاختلافات في التكوين على الموجهات التي يتم التحدث عنها:

- في التشكيل جديد، شكلت ال تحدثت مع ساكن إستاتيكي NHRP تعيين ل Hub2 و Hub2 أضفت كالتالي جنجل نادل.الأصل:

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp nhs 10.0.0.1
```

جديد:

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.5
ip nhrp map 10.0.0.2 172.17.0.5
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.0.2
```

- تم تغيير مناطق OSPF في الموجهات التي يتم التحدث بها إلى المنطقة 1.

تذكر أنه بتعريف خريطة NHRP الثابتة و NHS على مسحاج تخديد شفوي لصرة، أنت ذاهب إلى تشغيل بروتوكول التوجيه الديناميكي عبر هذا النفق. هذا يعرف الصرة ويتحدث التوجيه أو الشبكة المجاورة. لاحظ أن Hub2 هو مركز لكل الفروع، وهو أيضا يتحدث ل Hub1. وهذا يجعل من السهل تصميم الشبكات متعددة الطبقات المحورية والمتصلة وتكوينها وتعديلها عند إستخدام حل DMVPN.

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
```

```
                                        ip mtu 1400
                                ip nhrp authentication test
                          ip nhrp map multicast 172.17.0.1
                           ip nhrp map 10.0.0.1 172.17.0.1
                          ip nhrp map multicast 172.17.0.5
                           ip nhrp map 10.0.0.2 172.17.0.5
                                ip nhrp network-id 100000
                                     ip nhrp holdtime 300
                                     ip nhrp nhs 10.0.0.1
                                     ip nhrp nhs 10.0.0.2
                                ip ospf network broadcast
                                       ip ospf priority 0
                                               delay 1000
                                  tunnel source Ethernet0
                                tunnel mode gre multipoint
                                        tunnel key 100000
                        tunnel protection ipsec profile vpnprof
                                                       !
                                        interface Ethernet0
                                 ip address dhcp hostname Spoke1
                                                       !
                                        interface Ethernet1
                            ip address 192.168.2.1 255.255.255.0
                                                       !
                                              router ospf 1
                                network 10.0.0.0 0.0.0.255 area 0
                               network 192.168.2.0 0.0.0.255 area 0
                                                       !
```

تم التحدث<Router n>

```
                                             version 12.3
                                                       !
                                          <hostname Spoke<n
                                                       !
                                       crypto isakmp policy 1
                                     authentication pre-share
                        crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
                                                       !
        crypto ipsec transform-set trans2 esp-des esp-md5-hmac
                                           mode transport
                                                       !
                                    crypto ipsec profile vpnprof
                                       set transform-set trans2
                                                       !
                                        interface Tunnel0
                                          bandwidth 1000
                   ip address 10.0.0.<n+10> 255.255.255.0
                                        ip mtu 1400
                                ip nhrp authentication test
                          ip nhrp map multicast 172.17.0.1
                           ip nhrp map 10.0.0.1 172.17.0.1
                          ip nhrp map multicast 172.17.0.5
                           ip nhrp map 10.0.0.2 172.17.0.5
                                ip nhrp network-id 100000
                                     ip nhrp holdtime 300
                                     ip nhrp nhs 10.0.0.1
                                     ip nhrp nhs 10.0.0.2
                                ip ospf network broadcast
                                       ip ospf priority 0
                                               delay 1000
                                  tunnel source Ethernet0
```

```
                                tunnel mode gre multipoint
                                     tunnel key 100000
                tunnel protection ipsec profile vpnprof
                                                      !
                                    interface Ethernet0
                         <ip address dhcp hostname Spoke<x
                                                      !
                                    interface Ethernet1
                  ip address 192.168.<n>.1 255.255.255.0
                                                      !
                                        router ospf 1
                     network 10.0.0.0 0.0.0.255 area 0
                                    .network 192.168
                                                      !
```

عند هذه النقطة، يمكنك إلقاء نظرة على جداول التوجيه، وجداول خرائط NHRP، واتصالات IPsec على موجهات Talk1 ،Hub2 ،Hub1، و Talk2 للاطلاع على الشروط الأولية (بعد ظهور موجهات Talk1 و Talk2 مباشرة).

الشروط والتغييرات الأولية

معلومات الموجه Hub1 Router

```
                                    Hub1#show ip route
                 is subnetted, 1 subnets 172.17.0.0/24
    C       172.17.0.0 is directly connected, Ethernet0
                 is subnetted, 1 subnets 10.0.0.0/24
        C       10.0.0.0 is directly connected, Tunnel0
   C    192.168.0.0/24 is directly connected, Ethernet1
   O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17,
                                                  Tunnel0
   O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17,
                                                  Tunnel0
                                    Hub1#show ip nhrp
 via 10.0.0.2, Tunnel0 created 1w3d, expire 10.0.0.2/32
                                                00:03:15
Type: dynamic, Flags: authoritative unique registered
                                NBMA address: 172.17.0.5
      via 10.0.0.11, Tunnel0 created 1w3d, 10.0.0.11/32
                                              expire 00:03:49
Type: dynamic, Flags: authoritative unique registered
                              NBMA address: 172.16.1.24
      via 10.0.0.12, Tunnel0 created 1w3d, 10.0.0.12/32
                                              expire 00:04:06
Type: dynamic, Flags: authoritative unique registered
                              NBMA address: 172.16.2.75
               Hub1#show crypto engine connection active
         ID  Interface   IP-Address    State Algorithm
                                              Encrypt Decrypt
Ethernet0    172.17.0.1      set  HMAC_SHA+DES_56_CB 4
                                                   0       0
Ethernet0    172.17.0.1      set  HMAC_SHA+DES_56_CB 5
                                                   0       0
Ethernet0    172.17.0.1      set  HMAC_SHA+DES_56_CB 6
                                                   0       0
Tunnel0      10.0.0.1        set  HMAC_MD5+DES_56_CB 3532
```

```
                                                        0      232
Tunnel0     10.0.0.1        set  HMAC_MD5+DES_56_CB 3533
                                                      212        0
Tunnel0     10.0.0.1        set  HMAC_MD5+DES_56_CB 3534
                                                        0       18
Tunnel0     10.0.0.1        set  HMAC_MD5+DES_56_CB 3535
                                                       17        0
Tunnel0     10.0.0.1        set  HMAC_MD5+DES_56_CB 3536
                                                        0        7
Tunnel0     10.0.0.1        set  HMAC_MD5+DES_56_CB 3537
                                                        7        0
```

معلومات الموجه Hub2 Router

```
                                              Hub2#show ip route
             is subnetted, 1 subnets 172.17.0.0/24
    C       172.17.0.0 is directly connected, Ethernet0
               is subnetted, 1 subnets 10.0.0.0/24
         C       10.0.0.0 is directly connected, Tunnel0
   C    192.168.0.0/24 is directly connected, Ethernet1
   O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15,
                                                    Tunnel0
   O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15,
                                                    Tunnel0
                                             Hub2#show ip nhrp
  via 10.0.0.1, Tunnel0 created 1w3d, never 10.0.0.1/32
                                                     expire
              Type: static, Flags: authoritative used
                                   NBMA address: 172.17.0.1
      via 10.0.0.11, Tunnel0 created 1w3d, 10.0.0.11/32
                                                 expire 00:03:15
Type: dynamic, Flags: authoritative unique registered
                                 NBMA address: 172.16.1.24
  via 10.0.0.12, Tunnel0 created 00:46:17, 10.0.0.12/32
                                                 expire 00:03:51
Type: dynamic, Flags: authoritative unique registered
                                 NBMA address: 172.16.2.75
               Hub2#show crypto engine connection active
         ID Interface   IP-Address    State Algorithm
                                                 Encrypt Decrypt
Ethernet0   171.17.0.5      set  HMAC_SHA+DES_56_CB 4
                                                        0        0
Ethernet0   171.17.0.5      set  HMAC_SHA+DES_56_CB 5
                                                        0        0
Ethernet0   171.17.0.5      set  HMAC_SHA+DES_56_CB 6
                                                        0        0
Tunnel0     10.0.0.2        set  HMAC_MD5+DES_56_CB 3520
                                                        0      351
Tunnel0     10.0.0.2        set  HMAC_MD5+DES_56_CB 3521
                                                      326        0
Tunnel0     10.0.0.2        set  HMAC_MD5+DES_56_CB 3522
                                                        0      311
Tunnel0     10.0.0.2        set  HMAC_MD5+DES_56_CB 3523
                                                      339        0
Tunnel0     10.0.0.2        set  HMAC_MD5+DES_56_CB 3524
                                                        0       25
Tunnel0     10.0.0.2        set  HMAC_MD5+DES_56_CB 3525
                                                       22        0
```

معلومات الموجه TALK1

```
                                        Spoke1#show ip route
          is subnetted, 1 subnets 172.16.0.0/24
   C       172.16.1.0 is directly connected, Ethernet0
             is subnetted, 1 subnets 10.0.0.0/24
      C       10.0.0.0 is directly connected, Tunnel0
  O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31,
                                                Tunnel0
  via 10.0.0.2, 00:39:31, [110/11]
                                                Tunnel0
  C    192.168.1.0/24 is directly connected, Ethernet1
  O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:37:58,
                                                Tunnel0
                                      Spoke1#show ip nhrp
   via 10.0.0.1, Tunnel0 created 00:56:40, 10.0.0.1/32
                                              never expire
            Type: static, Flags: authoritative used
                                NBMA address: 172.17.0.1
   via 10.0.0.2, Tunnel0 created 00:56:40, 10.0.0.2/32
                                              never expire
            Type: static, Flags: authoritative used
                                NBMA address: 172.17.0.5
          Spoke1#show crypto engine connection active
       ID  Interface   IP-Address    State Algorithm
                                           Encrypt Decrypt
Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB 1
                                             0       0
Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB 2
                                             0       0
Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB 2010
                                             0     171
Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB 2011
                                           185       0
Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB 2012
                                             0      12
Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB 2013
                                            13       0
```

معلومات الموجه TALK2

```
                                        Spoke2#show ip route
          is subnetted, 1 subnets 172.16.0.0/24
   C       172.16.2.0 is directly connected, Ethernet0
             is subnetted, 1 subnets 10.0.0.0/24
      C       10.0.0.0 is directly connected, Tunnel0
  O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56,
                                                Tunnel0
  via 10.0.0.2, 00:57:56, [110/11]
                                                Tunnel0
  O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:56:14,
                                                Tunnel0
  C    192.168.2.0/24 is directly connected, Ethernet1
                                      Spoke2#show ip nhrp
 via 10.0.0.1, Tunnel0 created 5w6d, never 10.0.0.1/32
                                              expire
            Type: static, Flags: authoritative used
                                NBMA address: 172.17.0.1
 via 10.0.0.2, Tunnel0 created 6w6d, never 10.0.0.2/32
                                              expire
            Type: static, Flags: authoritative used
                                NBMA address: 172.17.0.5
          Spoke2#show crypto engine connection active
       ID  Interface   IP-Address    State Algorithm
```

```
                                                    Encrypt Decrypt
Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB 2
                                                          0       0
Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB 3
                                                          0       0
Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB 3712
                                                          0     302
Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB 3713
                                                        331       0
Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB 3716
                                                          0     216
Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB 3717
                                                        236       0
```

هناك عدد من المسائل المثيرة للاهتمام التي يمكن ملاحظتها حول جداول التوجيه على Talk1، Hub2، Hub1، و Talk2:

- كلا موجهات المحوري لها مسارات تكلفة متساوية للشبكات الموجودة خلف الموجهات التي يتم التحدث عنها.الموزع 1:

```
O     192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0
O     192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0
```

الموزع 2:

```
O     192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0
O     192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0
```

هذا يعني أن Hub1 و Hub2 سيعلن ال نفسه تكلفة للشبكات خلف ال يمثل مسحاج تخديد إلى المسحاج تخديد في الشبكة خلف الصرة مسحاج تخديد. على سبيل المثال، قد يبدو جدول التوجيه على الموجه، R2، المتصل مباشرة بشبكة 192.168.0.0/24 LAN كما يلي:R2:

```
O     IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
via 192.168.0.2, 00:00:27, Ethernet1/0/3O [110/12]
O     IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
via 192.168.0.2, 00:00:27, Ethernet1/0/3 [110/12]
```

- تحتوي الموجهات التي يتم التحدث عنها على مسارات متساوية التكلفة عبر كل من موجهات المحولات إلى الشبكة خلف موجهات المحولات.تم التحدث 1:

```
O     IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
via 10.0.0.2, 00:39:31, Tunnel0 [110/11]
```

تحدث 2:

```
O     IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
via 10.0.0.2, 00:57:56, Tunnel0 [110/11]
```

إذا كانت الموجهات التي يتم التحدث بها تقوم بموازنة الحمل لكل حزمة، حينئذ يمكنك الحصول على الحزم التي لم يتم طلبها.

لتجنب تنفيذ التوجيه غير المتماثل أو موازنة الحمل لكل حزمة عبر الارتباطات إلى المركزين، تحتاج إلى تكوين بروتوكول التوجيه لتفضيل مسار واحد متصل بالموجه في كلا الاتجاهين. إذا كنت تريد أن يكون Hub1 هو الأساسي و Hub2 هو النسخ الاحتياطي، بعد ذلك يمكنك تعيين تكلفة OSPF على واجهات نفق Hub لتكون مختلفة.

الموزع 1:

```
interface tunnel0
...
 ip ospf cost 10
...
```

الموزع 2:

```
interface tunnel0
...
 ip ospf cost 20
```

...
الطرق تبدو كما يلي:

الموزع 1:

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

الموزع 2:

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2:

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

يشتمل موجهات المحورين الآن على تكاليف مختلفة على المسارات للشبكات الموجودة خلف الموجهات التي يتم التحدث عنها. هذا يعني أنه سيتم تفضيل Hub1 لإعادة توجيه حركة المرور إلى الموجهات التي يتم التحدث بها، كما هو الحال على الموجه R2. سيعتني ذلك بمشكلة التوجيه غير المتماثل الموصوفة في النقطة الأولى أعلاه.

أما التوجيه غير المتماثل في الإتجاه الآخر، كما هو موضح في النقطة الثانية أعلاه، فلا يزال موجودا. عند إستخدام OSPF كبروتوكول التوجيه الديناميكي، يمكنك إصلاح هذا الحل من خلال حل بديل باستخدام الأمر **distance ...** تحت **الموجه OSPF 1** على المحولات لتفضيل المسارات التي تم التعرف عليها عبر Hub1 على المسارات التي تم تعلمها عبر Hub2.

تم التحدث 1:

```
router ospf 1
distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

تحدث 2:

```
router ospf 1
distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

الطرق تبدو كما يلي:

تم التحدث 1:

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

تحدث 2:

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

سيحمي تكوين التوجيه المذكور أعلاه من التوجيه غير المتماثل، بينما يسمح في الوقت نفسه بتجاوز الفشل إلى Hub2 إذا انخفض Hub1. هذا يعني أنه عندما يكون كلا المركزين في وضع التشغيل، يتم إستخدام Hub1 فقط. إذا كنت ترغب في إستخدام كلا المحورين عن طريق موازنة المحوري عبر المحاور، مع حماية التغلب على الأعطال وعدم توفر توجيه غير متناظر، عندئذ يمكن أن تصبح تهيئة التوجيه معقدة، وخاصة عند إستخدام OSPF. ولهذا السبب، قد يكون الموزع المزدوج التالي مع تخطيط DMVPN المزدوج خيارا أفضل.

لوحة وصل مزدوجة - تخطيط DMVPN مزدوج

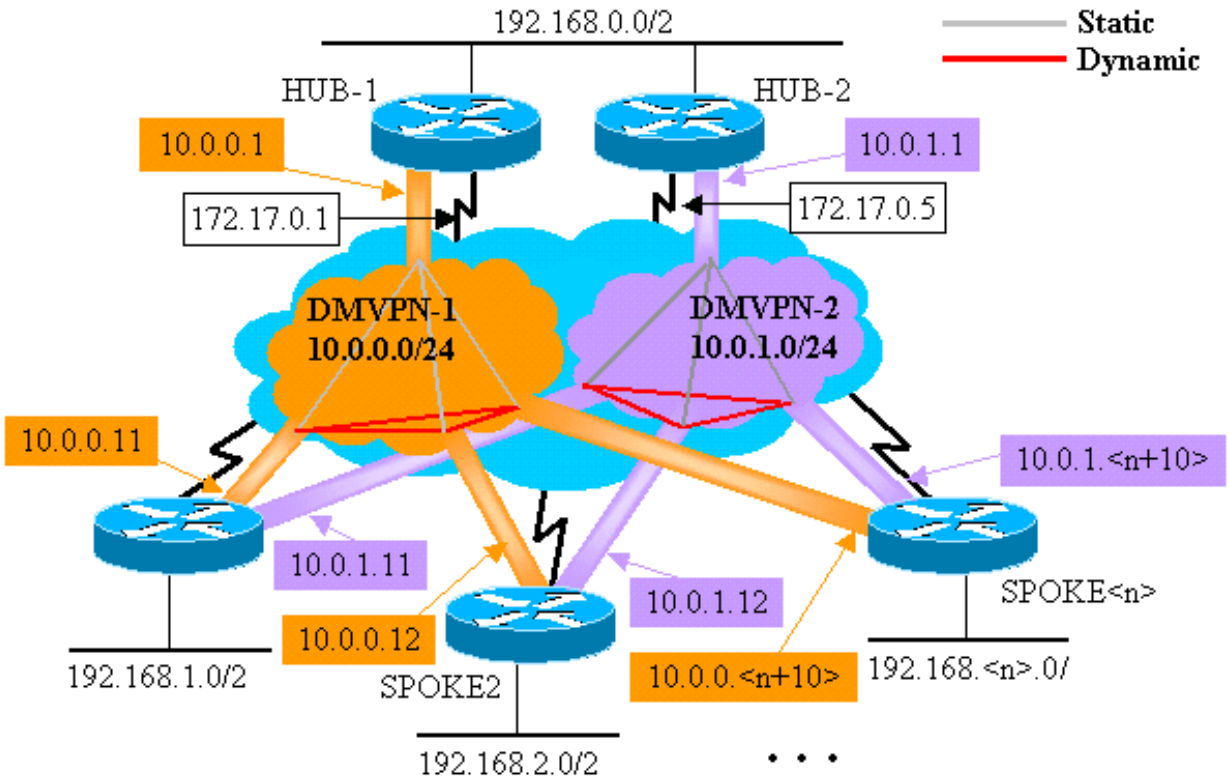
يكون إعداد الموزع المزدوج مع تخطيط DMVPN المزدوج أكثر صعوبة، ولكنه يمنحك تحكم أفضل في التوجيه عبر DMVPN. تتمثل الفكرة في وجود "غيوم" منفصلة خاصة بشبكة DMVPN. يتم توصيل كل موزع (إثنان في هذه الحالة) بشبكة DMVPN فرعية ("cloud")، كما يتم توصيل الخوادم الفرعية بكلا الشبكتين الفرعيتين ل DMVPN cloud")"). ونظرا لأن الموجهات التي يتم التحدث بها تقوم بتوجيه الجهات المجاورة باستخدام موجهات المحور عبر واجهات نفق GRE، فيمكنك إستخدام إختلافات تكوين الواجهة (مثل النطاق الترددي والتكلفة والتأخير) لتعديل مقاييس بروتوكول التوجيه الديناميكي لتفضيل موجه واحد على الموزع الآخر عندما تكون كلا الموجهين فوق.

ملاحظة: عادة ما تكون المسألة المذكورة أعلاه ذات صلة فقط إذا كانت موجهات المحاور مشتركة في الموقع. عندما لا تكون موجودة في الموقع المشترك، من المرجح أن ينتهي الأمر بالتوجيه الديناميكي العادي إلى تفضيل موجه المحولات الصحيح، حتى إذا كان من الممكن الوصول إلى الشبكة الوجهة عبر أي من موجهات المحولات.

يمكنك إستخدام واجهات نفق p-pGRE أو mGRE على الموجهات المنطوقة. يمكن أن تستخدم واجهات P-GRE المتعددة على موجه تكلمي نفس **مصدر النفق ...** عنوان IP، ولكن يجب أن يكون لواجهات mGRE المتعددة على الموجه الذي يتم التحدث به **مصدر نفق** فريد **...** عنوان IP. وهذا يرجع لأن الحزمة الأولى، عند بدء بروتوكول IPsec، هي حزمة ISAKMP يلزم اقترانها بأحد أنفاق mGRE. تحتوي حزمة ISAKMP فقط على عنوان IP للوجهة (عنوان النظير IPsec البعيد) الذي سيتم إجراء هذا الاقتران به. تتم مطابقة هذا العنوان مع **مصدر النفق ...** عنوان، ولكن نظرا لأن كلا النفقين لديهما **مصدر النفق** نفسه **...**عنوان، يتم مطابقة واجهة نفق mGRE الأولى دائما. وهذا يعني أنه قد يتم ربط حزم بيانات البث المتعدد الواردة بواجهة mGRE الخطأ، مما يؤدي إلى كسر أي بروتوكول توجيه ديناميكي.

لا تواجه حزم GRE نفسها هذه المشكلة نظرا لأنها تمتلك **مفتاح النفق ...** قيمة للتمييز بين واجهات mGRE. بدءا من الإصدار 12.3(5) من برنامج Cisco IOS Software و 12.3(7)T، تم إدخال معلمة إضافية للتغلب على هذا التحديد: **حماية النفق...مشترك**. تشير الكلمة الأساسية **المشتركة** إلى أن واجهات mGRE متعددة ستستخدم تشفير IPSec مع نفس عنوان IP للمصدر. إذا كان لديك إصدار أقدم، فيمكنك إستخدام أنفاق p-pGRE في هذا المركز المزدوج مع تخطيط DMVPN مزدوج. في حالة نفق p-pGRE، كل من **مصدر النفق**.. **ووجهة النفق ...** يمكن إستخدام عناوين IP للمطابقة. على سبيل المثال، سيتم إستخدام أنفاق p-pGRE في هذا المحور المزدوج مع تخطيط DMVPN مزدوج وعدم إستخدام المؤهل **المشترك**.

لوحة وصل مزدوجة - تخطيط DMVPN مزدوج



ترتبط التغييرات التالية المبرزة مع الموزع متعدد النقاط الديناميكي والتكوينات التي يتم التحدث بها والموضحة في وقت سابق في هذا المستند.

الموجه Hub1 Router

```
version 12.3
!
hostname Hub1
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.1 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
```

```
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
 ip address 172.17.0.1 255.255.255.252
 !
 interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
 !
```

الموجه Hub2 Router

```
version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100001
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.5 255.255.255.252
!
interface Ethernet1
ip address 192.168.0.2 255.255.255.0
!
router eigrp 1
network 10.0.1.0 0.0.0.255
network 192.168.0.0 0.0.0.255
no auto-summary
!
```

في هذه الحالة، ال hub1 و hub2 تشكيل مماثل. يكمن الاختلاف الرئيسي في أن كل منها يمثل مركزا لشبكة DMVPN مختلفة. يستخدم كل DMVPN شبكة مختلفة:

- شبكة IP الفرعية (24/10.0.0.0، 24/10.0.0.1)
- معرف شبكة NHRP (100000، 100001)
- مفتاح النفق (100000، 100001)

تم تحويل بروتوكول التوجيه الديناميكي من OSPF إلى EIGRP، نظرا لأنه من الأسهل إعداد شبكة NBMA وإدارتها باستخدام EIGRP، كما هو موضح لاحقا في هذا المستند.

الموجه TALK1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.11 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Tunnel1
bandwidth 1000
ip address 10.0.1.11 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.1.1 172.17.0.5
ip nhrp network-id 100001
ip nhrp holdtime 300
ip nhrp nhs 10.0.1.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke1
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
```

```
network 10.0.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
```

يتم تكوين كل موجه من الموجهات التي يتم التحدث بها باستخدام واجهة نفق P-GRE، بواقع واجهة واحدة في كل من شبكتي DMVPN. يتم إستخدام قيم **عنوان IP ...** و**ip nhrp network-id ...** و**مفتاح النفق ...** و**وجهة النفق ..** للتمييز بين النفقين. يتم تشغيل بروتوكول التوجيه الديناميكي، EIGRP، عبر كلا الشبكتين الفرعيتين لنفق p-pGRE ويتم إستخدامه لتحديد واجهة DMVPN) p-pGRE) واحدة عبر الأخرى.

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.12 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Tunnel1
bandwidth 1000
ip address 10.0.1.12 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.1.1 172.17.0.5
ip nhrp network-id 100001
ip nhrp holdtime 300
ip nhrp nhs 10.0.1.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke2
!
interface Ethernet1
ip address 192.168.2.1 255.255.255.0
```

```
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
no auto-summary
!
```

تم التحدث<Router n>

```
version 12.3
!
<hostname Spoke<n
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
.ip address 10.0.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Tunnel1
bandwidth 1000
.ip address 10.0.1
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.1.1 172.17.0.5
ip nhrp network-id 100001
ip nhrp holdtime 300
ip nhrp nhs 10.0.1.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
```

```
!
interface Ethernet0
<ip address dhcp hostname Spoke<x
!
interface Ethernet1
ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 192.168.<n>.0 0.0.0.255
no auto-summary
!
```

عند هذه النقطة، دعونا نلقي نظرة على جداول التوجيه، وجداول خرائط NHRP، واتصالات IPsec على موجهات Talk1، Hub2، Hub1 و Talk2 لرؤية الشروط الأولية (بعد ظهور موجهات Talk1 و Talk2 مباشرة).

الشروط والتغييرات الأولية

معلومات الموجه Hub1 Router

```
Hub1#show ip route
is subnetted, 1 subnets 172.17.0.0/30
C       172.17.0.0 is directly connected, Ethernet0
is subnetted, 2 subnets 10.0.0.0/24
C       10.0.0.0 is directly connected, Tunnel0
D       10.0.1.0 [90/2611200] via 192.168.0.2,
00:00:46, Ethernet1
C    192.168.0.0/24 is directly connected, Ethernet1
D    192.168.1.0/24 [90/2841600] via 10.0.0.11,
00:00:59, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12,
00:00:34, Tunnel0
Hub1#show ip nhrp
via 10.0.0.12, Tunnel0 created 23:48:32, 10.0.0.12/32
expire 00:03:50
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.2.75
via 10.0.0.11, Tunnel0 created 23:16:46, 10.0.0.11/32
expire 00:04:45
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.1.24
Hub1#show crypto engine connection active
ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
Ethernet0   172.17.63.18   set 15
HMAC_SHA+DES_56_CB      0        0
Ethernet0   10.0.0.1       set 16
HMAC_SHA+DES_56_CB      0        0
Tunnel0     10.0.0.1       set 2038
HMAC_MD5+DES_56_CB      0      759
Tunnel0     10.0.0.1       set 2039
HMAC_MD5+DES_56_CB    726        0
Tunnel0     10.0.0.1       set 2040
HMAC_MD5+DES_56_CB      0       37
Tunnel0     10.0.0.1       set 2041
HMAC_MD5+DES_56_CB     36        0
```

معلومات الموجه Hub2 Router

```
Hub2#show ip route
     is subnetted, 1 subnets 172.17.0.0/30
C       172.17.0.4 is directly connected, Ethernet0
     is subnetted, 2 subnets 10.0.0.0/24
D       10.0.0.0 [90/2611200] via 192.168.0.1,
                                    00:12:22, Ethernet1
C       10.0.1.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet1
D    192.168.1.0/24 [90/2841600] via 10.0.1.11,
                                    00:13:24, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.1.12,
                                    00:12:11, Tunnel0
Hub2#show ip nhrp
  via 10.0.1.12, Tunnel3 created 06:03:24, 10.0.1.12/32
                                    expire 00:04:39
Type: dynamic, Flags: authoritative unique registered
                        NBMA address: 172.16.2.75
  via 10.0.1.11, Tunnel3 created 23:06:47, 10.0.1.11/32
                                    expire 00:04:54
Type: dynamic, Flags: authoritative unique registered
                        NBMA address: 172.16.1.24
     Hub2#show crypto engine connection active
  ID Interface   IP-Address    State  Algorithm
                                  Encrypt  Decrypt
               Ethernet0   171.17.0.5     set 4
                 HMAC_SHA+DES_56_CB      0        0
               Ethernet0   171.17.0.5     set 6
                 HMAC_SHA+DES_56_CB      0        0
               Tunnel0     10.0.1.1       set 2098
                 HMAC_MD5+DES_56_CB      0      722
               Tunnel0     10.0.1.1       set 2099
                 HMAC_MD5+DES_56_CB    690        0
               Tunnel0     10.0.1.1       set 2100
                 HMAC_MD5+DES_56_CB      0      268
               Tunnel0     10.0.1.1       set 2101
                 HMAC_MD5+DES_56_CB    254        0
```

معلومات الموجه TALK1

```
Spoke1#show ip route
     is subnetted, 1 subnets 172.16.0.0/24
C       172.16.1.0 is directly connected, Ethernet0
     is subnetted, 1 subnets 10.0.0.0/24
C       10.0.0.0 is directly connected, Tunnel0
C       10.0.1.0 is directly connected, Tunnel1
D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
                                    00:26:30, Tunnel1
     via 10.0.0.1, [90/2841600]
                                    00:26:30, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet1
D    192.168.2.0/24 [90/3097600] via 10.0.1.1,
                                    00:26:29, Tunnel1
     via 10.0.0.1, [90/3097600]
                                    00:26:29, Tunnel0
Spoke1#show ip nhrp
  via 10.0.0.1, Tunnel0 created 23:25:46, 10.0.0.1/32
                                    never expire
               Type: static, Flags: authoritative
                        NBMA address: 172.17.0.1
  via 10.0.1.1, Tunnel1 created 23:24:40, 10.0.1.1/32
                                    never expire
```

```
                Type: static, Flags: authoritative
                                NBMA address: 172.17.0.5
        Spoke1#show crypto engine connection active
     ID Interface   IP-Address    State  Algorithm
                                          Encrypt  Decrypt
                  Ethernet0   172.16.1.24    set 16
                    HMAC_SHA+DES_56_CB      0        0
                  Ethernet0   172.16.1.24    set 18
                    HMAC_SHA+DES_56_CB      0        0
                  Tunnel0     10.0.0.11      set 2118
                    HMAC_MD5+DES_56_CB      0      181
                  Tunnel0     10.0.0.11      set 2119
                    HMAC_MD5+DES_56_CB    186        0
                  Tunnel1     10.0.1.11      set 2120
                    HMAC_MD5+DES_56_CB      0      105
                  Tunnel1     10.0.1.11      set 2121
                    HMAC_MD5+DES_56_CB    110        0
```

معلومات الموجه TALK2

```
                                      Spoke2#show ip route
          is subnetted, 1 subnets 172.16.0.0/24
   C       172.16.2.0 is directly connected, Ethernet0
             is subnetted, 2 subnets 10.0.0.0/24
      C       10.0.0.0 is directly connected, Tunnel0
      C       10.0.1.0 is directly connected, Tunnel1
       D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
                                          00:38:04, Tunnel1
       via 10.0.0.1, [90/2841600]
                                          00:38:04, Tunnel0
       D    192.168.1.0/24 [90/3097600] via 10.0.1.1,
                                          00:38:02, Tunnel1
       via 10.0.0.1, [90/3097600]
                                          00:38:02, Tunnel0
  C    192.168.2.0/24 is directly connected, Ethernet1
                                      Spoke2#show ip nhrp
via 10.0.0.1, Tunnel0 created 1d02h, never 10.0.0.1/32
                                                    expire
            Type: static, Flags: authoritative used
                                NBMA address: 172.17.0.1
via 10.0.1.1, Tunnel1 created 1d02h, never 10.0.1.1/32
                                                    expire
            Type: static, Flags: authoritative used
                                NBMA address: 172.17.0.5
        Spoke2#show crypto engine connection active
     ID Interface   IP-Address    State  Algorithm
                                          Encrypt  Decrypt
                  Ethernet0   172.16.2.75    set 8
                    HMAC_SHA+DES_56_CB      0        0
                  Ethernet0   172.16.2.75    set 9
                    HMAC_SHA+DES_56_CB      0        0
                  Tunnel0     10.0.0.12      set 2036
                    HMAC_MD5+DES_56_CB      0      585
                  Tunnel0     10.0.0.12      set 2037
                    HMAC_MD5+DES_56_CB    614        0
                  Tunnel1     10.0.1.12      set 2038
                    HMAC_MD5+DES_56_CB      0      408
                  Tunnel1     10.0.1.12      set 2039
                    HMAC_MD5+DES_56_CB    424        0
```

مرة أخرى، هناك بعض الأشياء المثيرة للاهتمام التي يمكن ملاحظتها حول جداول التوجيه على Hub1، Hub2، Talk1، و Talk2:

- كلا موجهات المحوري لها مسارات تكلفة متساوية للشبكات الموجودة خلف الموجهات التي يتم التحدث عنها.الموزع 1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0
```

الموزع 2:

```
D    192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0
```

هذا يعني أن Hub1 و Hub2 سيعلن ال نفسه تكلفة للشبكات خلف ال يمثل مسحاج تخديد إلى المسحاج تخديد في الشبكة خلف الصرة مسحاج تخديد. على سبيل المثال، قد يبدو جدول التوجيه على الموجه، R2، المتصل مباشرة بشبكة 192.168.0.0/24 LAN كما يلي:R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
via 192.168.0.2, 00:51:51, Ethernet1/0/3 [90/2867200]
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
via 192.168.0.1, 00:52:43, Ethernet1/0/3 [90/2867200]
```

- تحتوي الموجهات التي يتم التحدث عنها على مسارات متساوية التكلفة عبر كل من موجهات المحولات إلى الشبكة خلف موجهات المحولات.تم التحدث 1:

```
D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1
via 10.0.0.1, 00:26:30, Tunnel0 [90/3097600]
```

تحدث 2:

```
D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
via 10.0.0.1, 00:38:04, Tunnel0 [90/3097600]
```

إذا كانت الموجهات التي يتم التحدث بها تقوم بموازنة الحمل لكل حزمة، حينئذ يمكنك الحصول على الحزم التي لم يتم طلبها.

لتجنب تنفيذ التوجيه غير المتماثل أو موازنة الحمل لكل حزمة عبر الارتباطات إلى المركزين، تحتاج إلى تكوين بروتوكول التوجيه لتفضيل مسار واحد متصل بالموجه في كلا الاتجاهين. إن يريد أنت Hub1 أن يكون الأساسي و Hub2 أن يكون النسخة إحتياطية، بعد ذلك أنت يستطيع ثبتت التأخير على الصرة نفق قارن أن يكون مختلف.

الموزع 1:

```
interface tunnel0
...
delay 1000
...
```

الموزع 2:

```
interface tunnel0
...
delay 1050
...
```

ملاحظة: في هذا المثال، تمت إضافة 50 إلى التأخير على واجهة النفق على Hub2 لأنه أصغر من التأخير على واجهة Ethernet1 بين المركزين (100). من خلال القيام بهذا، سيظل Hub2 يرسل الحزم مباشرة إلى الموجهات المتصلة، ولكنه سيعلن عن مسار أقل مرغوب من Hub1 إلى الموجهات خلف Hub1 و Hub2. إذا زاد التأخير بأكثر من 100، بعد ذلك يقوم Hub2 بإعادة توجيه الحزم للموجهات عبر Hub1 عبر واجهة إيثرنت 1، رغم أن الموجهات خلف Hub1 و Hub2 لا تزال تفضل بشكل صحيح Hub-1 لإرسال الحزم إلى الموجهات التي يتم التحدث بها.

الطرق تبدو كما يلي:

الموزع 1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

الموزع 2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

:R2

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

ويختلف موجهات المحورين في تكاليف مسارات الشبكة خلف الموجهات التي يتم التحدث بها، لذلك، في هذه الحالة، سيفضل Hub1 لإعادة توجيه حركة مرور البيانات إلى الموجهات التي يتم التحدث بها، كما هو الحال في R2. وهذا يهتم بالقضية الموصوفة في النقطة الأولى أعلاه.

القضية الموصوفة في النقطة الثانية أعلاه لا تزال موجودة، ولكن نظرا لوجود واجهتي نفق p-pGRE، يمكنك تعيين **التأخير**... على واجهات النفق بشكل منفصل لتغيير مقياس EIGRP للطرق التي تم تعلمها من Hub1 مقابل Hub2.

تم التحدث 1:

```
interface tunnel0
     delay 1000
interface tunnel1
     delay 1050
```

تحدث 2:

```
interface tunnel0
     delay 1000
interface tunnel1
     delay 1050
```

الطرق تبدو كما يلي:

تم التحدث 1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

تحدث 2:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

سيحمي تكوين التوجيه المذكور أعلاه من التوجيه غير المتماثل، بينما يسمح في الوقت نفسه بتجاوز الفشل إلى Hub2 إذا انخفض Hub1. هذا يعني أنه عندما يكون كلا المركزين في وضع التشغيل، يتم إستخدام Hub1 فقط.

إذا كنت تريد إستخدام كلا المركبين عن طريق موازنة المحوري عبر المحاور، مع حماية تجاوز الفشل وعدم توفر توجيه غير متماثل، عندئذ يكون تكوين التوجيه أكثر تعقيدا، ولكن يمكنك القيام بذلك عند إستخدام EIGRP. ولإنجاز ذلك، قم بتعيين **التأخير** ... على واجهات النفق لموجهات المحولات على أن تعود إلى حالة المساواة ثم أستخدم الأمر **offset-list <acl> out <offset> <interface>**على الموجهات التي يتم التحدث بها لزيادة قياس EIGRP للمسارات المعلن عنها من واجهات نفق GRE إلى مركز النسخ الاحتياطي. لا يزال **التأخير** غير المتساوي بين واجهات Tunnel0 و Tunnel1 في المكبر صوت مستخدما، لذلك سيفضل الموجه الذي يتحدث موجه المحور الرئيسي الخاص به. التغييرات على الموجهات التي يتم التحدث بها هي كما يلي.

الموجه TALK1

```
version 12.3
!
hostname Spoke1
!
...
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1500
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
...
!
router eigrp 1
 offset-list 1 out 12800 Tunnel1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.1.0
 distribute-list 1 out
 no auto-summary
!
access-list 1 permit 192.168.1.0
!
```

الموجه TALK2

```
version 12.3
!
hostname Spoke2
!
...
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
```

```
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1500
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
 !
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
 !
...
 !
router eigrp 1
 offset-list 1 out 12800 Tunnel1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.2.0
 distribute-list 1 out
 no auto-summary
 !
access-list 1 permit 192.168.2.0
 !
```

ملاحظة: أضيفت القيمة المقابلة 12800 (50*256) إلى مقياس EIGRP لأنها أصغر من 25600 (100*256). هذه القيمة (25600)، هي ما تتم إضافته إلى مقياس EIGRP للمسارات التي تم التعرف عليها بين الموجهات المحورية. باستخدام 12800 في أمر **offset-list**، سيقوم موجه مركز النسخ الاحتياطي بإعادة توجيه الحزم مباشرة إلى الموجهات التي يتم التحدث بها، بدلا من إعادة توجيه هذه الحزم عبر الإيثرنت للانتقال من خلال موجه الموزع الرئيسي لتلك المسارات. سيظل المقياس على الموجهات التي يتم الإعلان عنها بواسطة موجهات المحولات على درجة تفضيل موجه المحولات الرئيسي الصحيح. تذكر أن نصف الجبهات لديها Hub1 كموجه أساسي، والنصف الآخر لديه Hub2 كموجه أساسي.

ملاحظة: إذا تمت زيادة قيمة الإزاحة بأكثر من 25600 (100*256)، فستقوم لوحات التوزيع بإعادة توجيه الحزم لنصف الموجهات التي يتم التحدث بها من خلال محور آخر عبر واجهة Ethernet1، على الرغم من أن الموجهات خلف لوحات التوزيع ستظل تفضل لوحة الوصل الصحيحة لإرسال الحزم إلى الموجهات التي يتم التحدث بها.

ملاحظة: تمت إضافة أمر **distribute-list 1 out** أيضا لأنه من الممكن أن يتم الإعلان عن الموجهات التي تم التعرف عليها من موجه محوري واحد عبر واجهة نفق واحدة على مكبر صوت مرة أخرى إلى الموزع الآخر عبر النفق الآخر. يضمن أمر **distribute-list ...** أن الموجه الذي يتم التحدث به يمكنه فقط الإعلان عن المسارات الخاصة به.

ملاحظة: إذا كنت تفضل التحكم في إعلانات التوجيه على موجهات جهات جهات الاتصال بدلا من الموجهات التي يتم التحدث بها، يمكن تكوين **إعلانات** التوجيه **على موجهات جهات جهات الاتصال، بعد ذلك** على **موجهات جهات جهات** الوصل **<acl1> في <interface> <value>** و**<acl2> distribute-list>** في الأوامر على موجهات جهات الوصل بدلا من تكوينها على الخوادم الفرعية. وسوف تقوم قائمة الوصول <acl2> بسرد الموجهات من خلف جميع الفروع، وستقوم قائمة الوصول <acl1> بسرد الموجهات فقط من خلف الفروع حيث يجب أن يكون موجه محوري آخر هو المركز الرئيسي.

مع هذه التغييرات تبدو المسارات كما يلي:

الموزع 1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

الموزع 2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

:R2

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

تم التحدث 1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

تحدث 2:

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

القرار

يوفر حل DMVPN الوظائف التالية لتطوير شبكات VPN الكبيرة والصغيرة عبر بروتوكول IPsec بشكل أفضل.

- يسمح DMVPN بالقياس بشكل أفضل في الشبكة الكاملة أو في شبكات IPsec VPN الجزئية.ويكون ذلك مفيدا بشكل خاص عندما تكون حركة المرور التي يجري الحديث إليها متقطعة (على سبيل المثال، لا يرسل كل شخص يتحدث باستمرار بيانات إلى كل شخص يتحدث). لا تسمح لمن يتحدث بإرسال البيانات مباشرة إلى أي شخص يتحدث، طالما هناك اتصال IP مباشر بين الفروع.
- يدعم DMVPN عقد IPsec بعناوين تم تعيينها بشكل ديناميكي (مثل الكبل و ISDN و DSL).ينطبق هذا على شبكات hub و-speaker بالإضافة إلى شبكات الشبكة المعشقة. يمكن أن يتطلب DMVPN تشغيل إرتباط -hub to-talk بشكل مستمر.
- يبسط DMVPN إضافة عقد VPN.عند إضافة موجه جديد، يجب عليك فقط تكوين الموجه الذي تم التحدث وتوصيله بالشبكة (على الرغم من ذلك، قد تحتاج إلى إضافة معلومات تخويل ISAKMP للموجه الجديد الذي يتم التحدث به على الصرة). سيتعلم الصرة ديناميكيا عن الحديث الجديد وسيعمل بروتوكول التوجيه الديناميكي على نشر التوجيه إلى الصرة وجميع الفروع الأخرى.
- يقلل DMVPN حجم التكوين المطلوب على جميع الموجهات في شبكة VPN.وهذا أيضا هو الحال لشبكات VPN الخاصة بمحور و اتصال GRE+IPsec.
- يستخدم DMVPN بروتوكول GRE، وبالتالي، فإنه يدعم بث IP المتعدد وحركة مرور التوجيه الديناميكي عبر شبكة VPN.وهذا يعني أنه يمكن إستخدام بروتوكول توجيه ديناميكي، ويمكن دعم "لوحات التوزيع" المكررة بواسطة البروتوكول. تطبيقات البث المتعدد مدعومة أيضا.
- يدعم DMVPN الاتصال النفقي المنقسم في المحولات الفرعية.

معلومات ذات صلة

- (Dynamic Multipoint VPN (DMVPN

- 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).