نقل النقل الثابت للترحيل من DMVPN إلى FlexVPN على محور مختلف

المحتويات

المقدمة

يقدم هذا المستند معلومات حول كيفية الترحيل من شبكة DMVPN (Dynamic Multipoint VPN) موجودة حاليا إلى FlexVPN على أجهزة موزع مختلفة. عمليات التكوين لكلا الإطارين موجودة على الأجهزة. في هذا المستند، يتم عرض السيناريو الأكثر شيوعا فقط - DMVPN باستخدام المفتاح المشترك مسبقا للمصادقة وبروتوكول توجيه العبارة الداخلي المحسن (EIGRP) كبروتوكول توجيه. في هذا المستند، يتم عرض الترحيل إلى بروتوكول العبارة الحدودية (BGP)، وهو بروتوكول التوجيه الموصى به، ويتم عرض بروتوكول EIGRP الأقل رغبة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- DMVPN
- FlexVPN

المكونات المستخدمة

ملاحظة: لا تدعم جميع البرامج والأجهزة الإصدار 2 من تبادل مفتاح الإنترنت (IKEv2). راجع متصفح ميزة Cisco للحصول على مزيد من المعلومات.

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

- Cisco Integrated Service Router (ISR)، الإصدار 15.2(4)M1 أو الأحدث
- سلسلة موجه خدمات التجميع طراز 1000 (ASR1K) الإصدار 3.6.2 15.2(2)S2 أو إصدار أحدث من Cisco

إحدى مزايا النظام الأساسي والبرامج الأحدث هي القدرة على إستخدام الجيل التالي من التشفير، مثل وضع العداد/معيار التشفير المتقدم (AES) للتشفير في أمان بروتوكول الإنترنت (IPsec)، كما هو موضح في طلب التعليقات (RFC) 4106. يتيح لك AES GCM الوصول إلى سرعة تشفير أسرع بكثير على بعض الأجهزة. لعرض توصيات Cisco حول إستخدام تشفير الجيل التالي والترحيل إليه، ارجع إلى مقالة التشفير من الجيل التالي.

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

إجراءات الهجرة

وفي الوقت الحالي، تتمثل الطريقة الموصى بها للترحيل من شبكة DMVPN إلى شبكة FlexVPN في عدم عمل الإطارين في نفس الوقت. تمت جدولة هذا القيد لإزالته بسبب ميزات الترحيل الجديدة التي سيتم تقديمها في إصدار ASR 3.10، والتي تم تعقبها بموجب طلبات التعزيز متعدد اللغات على جانب Cisco، والتي تتضمن معرف تصحيح الأخطاء من Cisco CSCuc08066. وينبغي إتاحة هذه السمات في أواخر حزيران/يونيه 2013.

ويشار إلى عملية الترحيل التي يتعايش فيها كلا الإطارين ويعملان في نفس الوقت على الأجهزة نفسها على أنها **ترحيل ميسر**، مما يشير إلى الحد الأدنى من التأثير والتغلب السلس على الفشل من إطار إلى آخر. ويشار إلى عملية الترحيل التي تتعايش فيها التكوينات الخاصة بكل من الإطارين، ولكنها لا تعمل في نفس الوقت، على أنها **عملية ترحيل**

صعبة. وهذا يشير إلى أن التحول من إطار عمل إلى آخر يعني عدم الاتصال عبر الشبكة الخاصة الظاهرية (VPN)، حتى ولو كان الحد الأدنى.

الهجرة الصعبة بين مركزين مختلفين

في هذا المستند، تتم مناقشة الترحيل من لوحة وصل DMVPN المستخدمة حاليا إلى موزع FlexVPN جديد. يتيح هذا الترحيل إمكانية الاتصال البيني بين المحولات التي تم ترحيلها بالفعل إلى FlexVPN، وتلك التي لا تزال تعمل على DMVPN ويمكن تنفيذها على مراحل متعددة، حيث يتم التحدث كل منها على حدة.

شريطة تعبئة معلومات التوجيه بشكل صحيح، يجب أن يبقى الاتصال بين الفروع التي تم ترحيلها أو التي لم يتم ترحيلها ممكنا. ومع ذلك، يمكن ملاحظة زمن وصول إضافي لأن الأزقة المرسلة وغير المنقولة لا تبني أنفاقا عبر الهاتف بين بعضها البعض. وفي الوقت نفسه، يجب أن تكون الفروع المهاجرة قادرة على إنشاء أنفاق مباشرة يتم الحديث إليها فيما بينها. نفس الشيء ينطبق على الباقات غير المرحلة.

إلى أن تتوفر ميزة الترحيل الجديدة هذه، أكمل الخطوات التالية لتنفيذ عمليات الترحيل باستخدام محور مختلف من DMVPN و FlexVPN:

1. تحقق من الاتصال عبر DMVPN.
2. قم بإضافة تكوين FlexVPN، وأغلق النفق الذي ينتمي إلى التكوين الجديد.
3. (أثناء إطار الصيانة) أغلق نفق DMVPN الواحد تلو الآخر.
4. في الخطوة نفسها، قم بإلغاء تشغيل واجهات نفق FlexVPN.
5. تحقق من الاتصال عبر لوحة الوصل.
6. تحقق من الاتصال عبر المحادثة داخل FlexVPN.
7. تحقق من الاتصال عبر المحادثة باستخدام DMVPN من FlexVPN.
8. كرر الخطوات من 3 إلى 7 لكل خطوة تحدث بشكل منفصل.
9. إذا واجهت أي مشاكل مع عمليات التحقق الموضحة في الخطوات 5 أو 6 أو 7، فقم بإيقاف تشغيل واجهة FlexVPN، وأغلق واجهات DMVPN للعودة إلى DMVPN.
10. تحقق من الاتصال عبر مركز البيانات عبر DMVPN الذي تم نسخه إحتياطيا.
11. تحقق من الاتصال عبر المحادثة عبر DMVPN المدعوم.

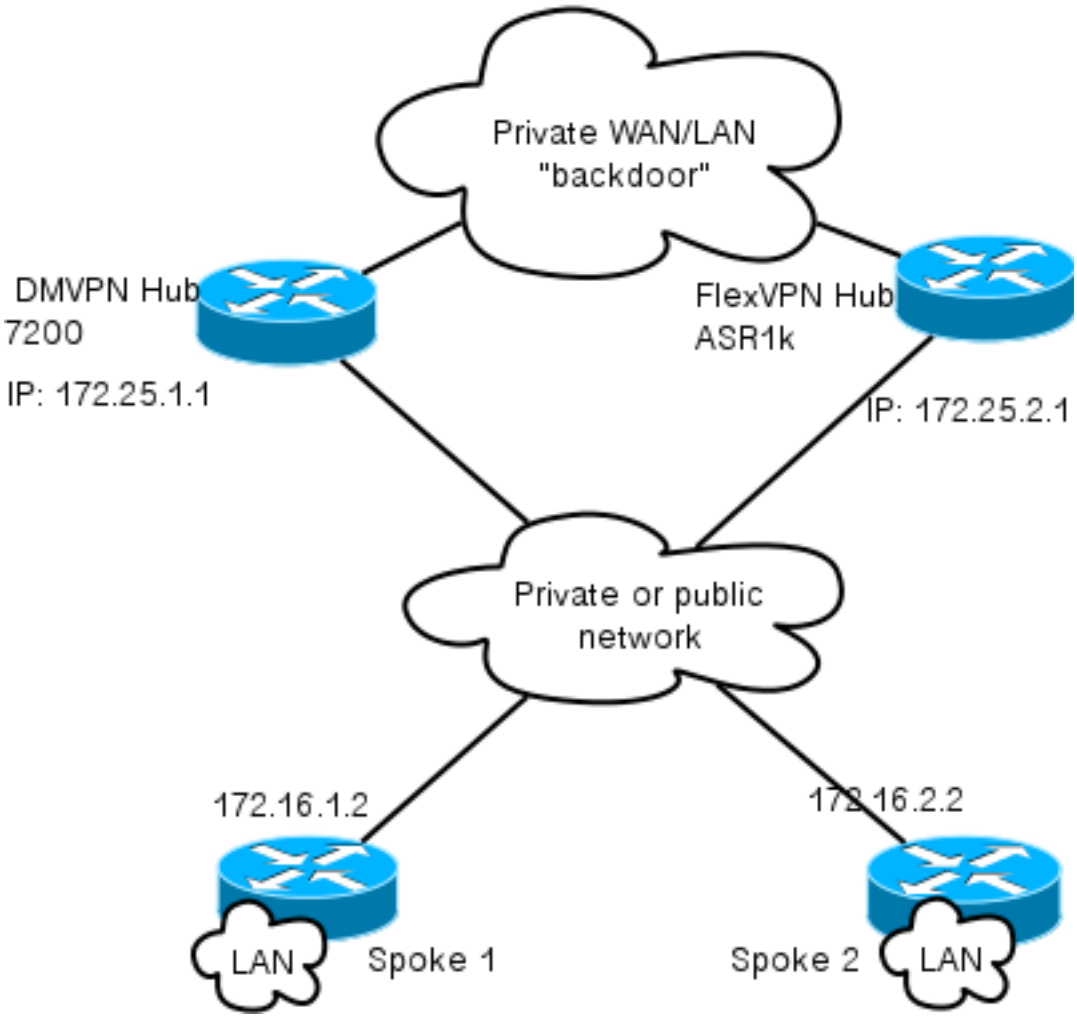
نهج مخصص

إذا كان النهج السابق قد لا يكون الحل الأفضل لك نظرا لشبكتك أو تعقيدات التوجيه، فعليك بدء مناقشة مع ممثل Cisco الخاص بك قبل الترحيل. إن أفضل شخص يمكن أن يناقش معه عملية ترحيل مخصصة هو مهندس النظام أو مهندس الخدمات المتقدمة لديك.

مخطط الشبكة

مخطط شبكة النقل

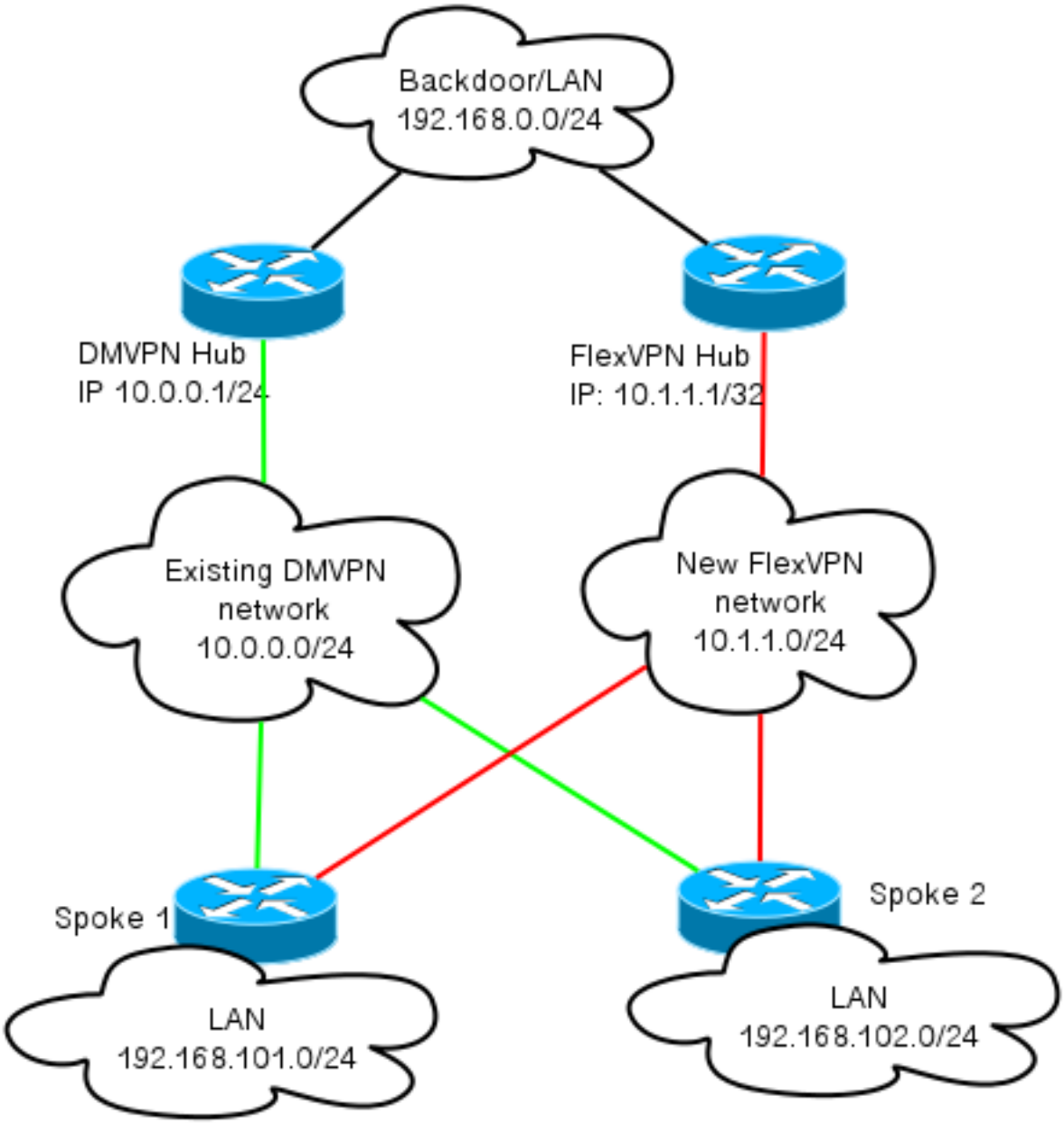
يوضح هذا المخطط مخطط الاتصال النموذجي للمضيفين على الإنترنت. يتم إستخدام عنوان IP الخاص بالموجه **loopback0** (**172.25.1.1**) لإنهاء جلسة IPsec ل DMVPN. يتم إستخدام عنوان IP على الموزع الجديد (**172.25.2.1**) ل FlexVPN.



لاحظ الرابط بين المركزين. يعد هذا الارتباط أمرا بالغ الأهمية للسماح بالاتصال بين FlexVPN وسحابة DMVPN أثناء الترحيل. وهو يسمح للمعلمات التي تم ترحيلها بالفعل إلى FlexVPN بالاتصال بشبكات DMVPN والعكس بالعكس.

مخطط الشبكة المتفرعة

يوضح الرسم التخطيطي هذا غموسين منفصلين يتم إستخدامهما للتغشية: DMVPN (توصيلات خضراء) و FlexVPN (إتصالات حمراء). يتم عرض بادئات LAN للمواقع المقابلة. لا تمثل الشبكة الفرعية **24/10.1.1.0** شبكة فرعية فعلية من حيث عنونة الواجهة، ولكنها تمثل مجموعة من مساحة IP المخصصة لسحابة FlexVPN. ستتم مناقشة الأساس المنطقي وراء هذا لاحقا في قسم **تكوين FlexVPN**.



التكوين

يصف هذا القسم تكوينات DMVPN و FlexVPN.

تكوين DMVPN

يصف هذا القسم التكوين الأساسي لموزع DMVPN وتكلم.

يتم إستخدام المفتاح المشترك مسبقا (PSK) لمصادقة IKEv1. بمجرد إنشاء IPsec، يتم إجراء تسجيل بروتوكول تحليل الخطوة (Hop) التالية (NHRP) من قائمة تحويل إلى محور حتى يمكن للموزع التعرف على عنونة Non-Broadcast Multiaccess (NBMA) الخاصة بالخوادم بشكل ديناميكي.

عندما تقوم NHRP بالتسجيل على المتصل والمحور، يمكن إنشاء توجيه التجاور، ويمكن تبادل المسارات. في هذا المثال، يتم إستخدام EIGRP كبروتوكول توجيه أساسي للشبكة المتداخلة.

تحدث تكوين DMVPN

هنا يمكنك العثور على مثال أساسي لتكوين DMVPN مع مصادقة PSK و EIGRP كبروتوكول التوجيه.

```
crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport

crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

interface Tunnel0

ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.102.0
passive-interface default
no passive-interface Tunnel0
```

تكوين Hub DMVPN

في تكوين الصرة، يتم الحصول على النفق من **loopback0** بعنوان **172.25.1.1** IP. الباقي هو نشر قياسي لموزع DMVPN مع EIGRP كبروتوكول توجيه.

```
crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport
crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
```

```
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0
```

تكوين FlexVPN

تستند FlexVPN إلى نفس التقنيات الأساسية التالية:

- **IPsec**: على عكس الإعداد الافتراضي في DMVPN، يتم إستخدام IKEv2 بدلا من IKEv1 للتفاوض على اقترانات أمان IPsec (SAs). يوفر IKEv2 تحسينات عبر IKEv1، مثل المرونة وعدد الرسائل المطلوبة لإنشاء قناة بيانات محمية.

- **GRE**: على عكس DMVPN، يتم إستخدام الواجهات الثابتة والحركية من نقطة إلى نقطة، وليس واجهة GRE واحدة ثابتة ل Multpoint. تتيح هذه التهيئة مرونة إضافية، خاصة لسلوك كل موزع/كل موزع.

- **NHRP**: في FlexVPN، يستخدم NHRP في المقام الأول لإنشاء الاتصال عن طريق التخاطب. لا يتم التسجيل إلى الصرة.

- **التوجيه**: نظرا لأن المحولات الفرعية لا تقوم بتسجيل NHRP إلى الموزع، يجب عليك الاعتماد على الآليات الأخرى للتأكد من إمكانية اتصال المحولات والأقسام الفرعية بشكل ثنائي الإتجاه. مماثل ل DMVPN، يمكن إستخدام بروتوكولات التوجيه الديناميكية. ومع ذلك، يتيح لك FlexVPN إستخدام IPsec لتقديم معلومات التوجيه. الإعداد الافتراضي هو تقديم مسار **AS/32** لعنوان IP على الجانب الآخر من النفق، والذي يسمح بالاتصال المباشر من مركز الحديث.

في عملية ترحيل صعبة من DMVPN إلى FlexVPN، لا يعمل النظامان في نفس الوقت على نفس الأجهزة. ومع ذلك، يوصى بإبقائها منفصلة.

افصلها على عدة مستويات:

- NHRP - إستخدام معرف شبكة NHRP مختلف (مستحسن).
- التوجيه - إستخدام عمليات توجيه منفصلة (مستحسن).
- التوجيه الظاهري وإعادة التوجيه (VRF) - يسمح فصل التردد اللاسلكي (VRF) بمرونة إضافية ولكن لا تتم مناقشته هنا (إختياري).

تحدث عن تكوين FlexVPN

أحد الفروق في التكوين الذي يتم التحدث به في FlexVPN مقارنة ب DMVPN هو أنه من المحتمل أن يكون لديك

واجهتان. هناك نفق مطلوب للاتصال بين مراكز التواصل ونفق إختياري للأنفاق التي يتم التحدث بها. إذا أخترت عدم وجود اتصال نفقي ديناميكي خاص بالمحادثة وتفضل أن يمر كل شيء عبر جهاز الوصل، يمكنك إزالة واجهة القالب الظاهري، وإزالة تبديل إختصار NHRP من واجهة النفق.

لاحظت أن النفق يستلم قارن ساكن إستاتيكي عنوان يؤسس على تفاوض. وهذا يسمح للموزع بتوفير عنوان IP لواجهة النفق إلى مكبر الصوت بشكل ديناميكي دون الحاجة إلى إنشاء عنونة ثابتة في سحابة FlexVPN.

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn spoke.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

ملاحظة: بشكل افتراضي، يتم تعيين الهوية المحلية لاستخدام عنوان IP. لذلك يجب أن تتطابق جملة المطابقة المطابقة المطابقة المطابقة على النظير استنادا إلى العنوان أيضا. إذا كان المتطلب أن يتطابق على أساس الاسم المميز (DN) في الشهادة، فيجب أن يتم التطابق باستخدام خريطة شهادة.

cisco يوصي أن يستعمل أنت AES GCM مع جهاز أن يدعمه.

```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport

crypto ipsec profile default
set ikev2-profile Flex_IKEv2
set transform-set IKEv2 !

interface Tunnel1
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
shutdown
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

البنية الأساسية للمفتاح العام (PKI) هي الطريقة الموصى بها لإجراء مصادقة على نطاق واسع في IKEv2. ومع ذلك، لا يزال بإمكانكم إستعمال PSK ما دمتم على علم بقيوده.

هنا مثال على التكوين الذي يستخدم Cisco كPSK.

```
crypto ikev2 keyring Flex_key
peer Spokes
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco
pre-shared-key remote cisco
crypto ikev2 profile Flex_IKEv2
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

تكوين موزع FlexVPN

بشكل نموذجي، لا يقوم الموزع إلا بإنهاء أنفاق تحويل البيانات إلى موزع الديناميكية. هذا هو السبب أنت لا يجد ثابت نفق قارن ل FlexVPN في الصرة تشكيل. وبدلا من ذلك، يتم إستخدام واجهة قالب ظاهري.

ملاحظة: على جانب الموزع، يجب أن تشير إلى عناوين المجموعة التي سيتم تعيينها للكلمات.

تتم إضافة العناوين من هذا التجمع لاحقا في جدول التوجيه كمسارات /32 لكل محدث.

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 authorization policy default
pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn hub.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

cisco يوصي أن يستعمل أنت AES GCM مع جهاز أن يدعمه.

```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport
```

ملاحظة: في هذا التكوين، تم التعليق على عملية AES GCM.

```
crypto ipsec profile default
set ikev2-profile Flex_IKEv2
set transform-set IKEv2 !

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
interface Loopback100
```

```
ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip nhrp network-id 2
ip nhrp redirect
tunnel path-mtu-discovery
tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

مع المصادقة في IKEv2، يطبق المبدأ نفسه على الموزع كما في المتكلم. لضمان قابلية التطوير والمرونة، أستخدم التراخيص. ومع ذلك، يمكنك إعادة إستخدام التكوين نفسه ل PSK كما هو الحال في المحادثة.

ملاحظة: يوفر IKEv2 المرونة من حيث المصادقة. يمكن لجانب المصادقة مع PSK بينما يستخدم الجانب الآخر توقيع ناشف-شامير-أدلمان (RSA-SIG).

إذا كان المتطلب هو إستخدام مفاتيح تم تعليمها مسبقا للمصادقة، فإن تغييرات التكوين تكون مماثلة لتلك الموضحة للموجه الذي يتم التحدث به هنا.

اتصال BGP بين الموزع

تأكد من أن لوحات التوزيع تعرف أين توجد البادئات المحددة. ويتزايد أهمية هذا الأمر نظرا لترحيل بعض المحددات إلى FlexVPN بينما تظل بعض المحددات الأخرى موجودة على DMVPN.

هنا ال inter-hub BGP توصيل يؤسس على ال DMVPN صرة تشكيل:

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

ترحيل حركة المرور

الترحيل إلى BGP كبروتوكول توجيه التغشية [مستحسن]

BGP هو بروتوكول توجيه يستند إلى تبادل البث الأحادي. ونظرا لخصائصه، فإنه بروتوكول القياس الأفضل في شبكات DMVPN.

في هذا المثال، يتم إستخدام بروتوكول BGP الداخلي (iBGP).

تكوين BGP الذي تحدث

تتألف هجرة المحادثات من جزأين. أولا، قم بتمكين BGP كتوجيه ديناميكي:

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
```

بعد ظهور مجاور BGP (راجع القسم التالي) وتعلم بادئات جديدة عبر BGP، يمكنك تحويل حركة مرور البيانات من سحابة DMVPN الحالية إلى سحابة FlexVPN جديدة.

تكوين Hub BGP

لوحة وصل FlexVPN - تكوين BGP كامل

على لوحة الوصل، من أجل تجنب الحفاظ على ترتيب الجوار لكل محادثة على حدة، قم بتكوين مستمعين ديناميكيين. في هذا الإعداد، لا يقوم BGP ببدء إتصالات جديدة، ولكنه يقبل الاتصالات من مجموعة عناوين IP المقدمة. في هذه الحالة، يكون التجمع المذكور هو **24/10.1.1.0**، وهو جميع العناوين في سحابة FlexVPN الجديدة.

هناك نقطتان تجدر الإشارة إليهما:

- يقوم مركز FlexVPN بالإعلان عن بادئات معينة لوزع DMVPN، وبالتالي يتم إستخدام خريطة unsupress.
- قم بالإعلان عن الشبكة الفرعية FlexVPN من **24/10.1.1.0** إلى جدول التوجيه، أو تأكد من أن موزع DMVPN يرى موزع FlexVPN على أنه الخطوة التالية.

وتبين هذه الوثيقة النهج الأخير.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

router bgp 65001
network 192.168.0.0
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

محور DMVPN - تكوين BGP بالكامل و EIGRP

التكوين على لوحة وصل DMVPN أساسي، لأنه يستقبل فقط بادئات معينة من لوحة وصل FlexVPN ويعلن عن البادئات التي يتعلمها من EIGRP.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

ترحيل حركة المرور إلى BGP/FlexVPN

وكما تمت مناقشته من قبل، يجب عليك إيقاف تشغيل وظائف شبكة DMVPN وتحديث FlexVPN لإجراء الترحيل.

يضمن هذا الإجراء الحد الأدنى من التأثير:

1. في كل محادثة، قم بإدخال ما يلي بشكل منفصل:

```
interface tunnel 0
shut
```

عند هذه النقطة، تأكد من عدم إنشاء جلسات IKEv1 لهذه المحادثة. يمكن التحقق من هذا الإجراء إذا قمت بالتحقق من إخراج الأمر **show crypto isakmp sa** ورسائل syslog التي تم إنشاؤها بواسطة الأمر **crypto logging session**. وبمجرد التأكد من ذلك، يمكنك المتابعة لعرض FlexVPN.

2. في نفس المحادثة، أدخل ما يلي:

```
interface tunnel 1
no shut
```

خطوات التحقق

إستقرار IPsec

أفضل طريقة لتقييم إستقرار IPsec هي مراقبة سجلات النظام باستخدام أمر تكوين **جلسة عمل التشفير** الذي تم تمكينه. إذا رأيت جلسات العمل التي تتنقل لأعلى ولأسفل، فقد يشير ذلك إلى مشكلة على مستوى IKEv2/FlexVPN يجب تصحيحها قبل بدء الترحيل.

معلومات BGP المأهولة

إذا كان IPsec مستقرا، فتأكد من أن جدول BGP مملوء بإدخالات من الفروع (على الصرة) والموجز من الصرة (على الفروع). في حالة BGP، يمكن عرض هذا باستخدام الأوامر التالية:

```
show bgp
or !
show bgp ipv4 unicast
or !
show ip bgp summary
```

هنا مثال على المعلومات الصحيحة من لوحة وصل FlexVPN:

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1 01:35:58 0 0 16 123 112 65001 4 10.1.1.100*
4 01:24:12 0 0 16 99 97 65001 4 192.168.0.1
```

تظهر المخرجات أن الصرة تعلمت بادئة واحدة من كل من المسلسلات، وكلا البابين ديناميكي ويميز بعلامة نجمية (*). كما توضح أنه يتم تلقي إجمالي أربع بادئات من الاتصال بين المحولات.

هنا مثال لمعلومات مماثلة من الحديث:

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
2 01:33:23 0 0 57 109 120 65001 4 10.1.1.1
```

تلقى المدون بادئين من الصرة. في حالة هذا الإعداد، يجب أن تكون إحدى البادئات هي الملخص المعلن عنه على

لوحة وصل FlexVPN. والآخر هو شبكة DMVPN **10.0.0.0/24** التي أعيد توزيعها على DMVPN الذي يتم التحدث عنه في BGP.

الترحيل إلى أنفاق جديدة باستخدام EIGRP

يعد بروتوكول EIGRP خيارا شائعا في شبكات DMVPN نظرا لما يتميز به من نشر بسيط نسبيا وإمكانية تقارب سريعة. ومع ذلك، فإنه يقيس بشكل أسوأ من بروتوكول BGP، ولا يقدم العديد من الآليات المتقدمة التي يمكن إستخدامها من قبل بروتوكول BGP بمجرد إخراجه من العبوة. يصف القسم التالي إحدى طرق النقل إلى FlexVPN باستخدام عملية EIGRP جديدة.

التكوين الذي تم تحديثه

تتم إضافة نظام مستقل جديد (AS) مع عملية EIGRP منفصلة:

```
router eigrp 200
network 10.1.1.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel1
```

ملاحظة: من الأفضل عدم إنشاء تجاور بروتوكول التوجيه عبر الأنفاق التي يتم التحدث بها. لذلك، فقط أجعل واجهة **النفق 1** (talk-to-hub) ليست خاملة.

تكوين موزع FlexVPN المحدث

وبالمثل، بالنسبة لموزع FlexVPN، قم بإعداد بروتوكول التوجيه في قاعدة معلومات الإدارة (AS) المناسبة، ليتطابق مع بروتوكول تم تكوينه على الفروع.

```
router eigrp 200
network 10.1.1.0 0.0.0.255
```

هناك طريقتان تستخدمان لتقديم ملخص للكلمة.

- إعادة توزيع مسار ثابت يشير إلى **null0** (الخيار المفضل).

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY

router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

يتيح هذا الخيار التحكم في الملخص وإعادة التوزيع دون إدخال تعديلات على تكوين تقنية المحاكاة الظاهرية

(VT) للموزع. هذا مهم، لأن الصرة VT تشكيل يستطيع لا يكون عدلت إن هناك نشط فعلي منفذ ظاهري مرتبط به.

- إعداد عنوان ملخص نمط DMVPN على قالب ظاهري.

لا يوصى بهذا التكوين، بسبب المعالجة الداخلية والنسخ المتماثل للملخص المذكور لكل وصول ظاهري. وهو ظاهر هنا كمرجع.

```
interface Virtual-Template1 type tunnel
ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

هناك جانب آخر للحساب الخاص به وهو تبادل التوجيه بين المحاور. يمكن القيام بذلك إذا قمت بإعادة توزيع مثيلات EIGRP على iBGP.

موزع DMVPN - تكوين BGP المحدث

يبقى التكوين أساسيا. يجب عليك إعادة توزيع بادئات معينة من EIGRP إلى BGP:

```
router bgp 65001
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

FlexVPN Hub - تكوين BGP المحدث

على غرار موزع DMVPN، في FlexVPN، يجب عليك إعادة توزيع بادئات عملية EIGRP الجديدة إلى BGP:

```
router bgp 65001
redistribute eigrp 200 redistribute static
neighbor 192.168.0.1 remote-as 65001
```

ترحيل حركة المرور إلى FlexVPN

يجب عليك إيقاف تشغيل وظيفة شبكة DMVPN ورفع FlexVPN على كل كلمة، واحدة في كل مرة، من أجل إجراء الترحيل. يضمن هذا الإجراء الحد الأدنى من التأثير:

1. في كل محادثة، قم بإدخال ما يلي بشكل منفصل:

```
interface tunnel 0
shut
```

عند هذه النقطة، تأكد من عدم إنشاء جلسات IKEv1 على هذه المحادثة. يمكن التحقق من هذا الإجراء إذا قمت بالتحقق من إخراج الأمر **show crypto isakmp sa** ورسائل syslog التي تم إنشاؤها بواسطة الأمر **crypto logging session**. وبمجرد التأكد من ذلك، يمكنك المتابعة لعرض FlexVPN.
2. في نفس المحادثة، أدخل ما يلي:

```
interface tunnel 1
        no shut
```

خطوات التحقق

إستقرار IPsec

كما في حالة BGP، يجب عليك تقييم ما إذا كان IPsec مستقرا. أفضل طريقة للقيام بذلك هي مراقبة سجلات النظام باستخدام أمر تكوين **جلسة عمل التشفير** الذي تم تمكينه. إذا كنت ترى جلسات العمل تذهب صعودا ونزولا، فقد يشير ذلك إلى مشكلة على مستوى IKEv2/FlexVPN يجب تصحيحها قبل بدء الترحيل.

معلومات EIGRP في جدول المخطط

تأكد من أن جدول مخطط EIGRP معبأ بإدخالات LAN التي يتم التحدث بها على الموزع والموجز على الفروع. يمكن التحقق من هذا الإجراء إذا قمت بإدخال هذا الأمر على الموزع (الموجهات) والكلام (التبليغات):

show ip eigrp [AS_NUMBER] topology

هنا مثال من المخرج من الحديث:

```
Spoke1#show ip eigrp 200 topology
(EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1
,Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
(via Rstatic (26112000/0
via 10.1.1.1 (26240000/128256), Tunnel1

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0

P 192.168.0.0/16, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

يوضح الإخراج أن المتحدث يعرف عن الشبكة المحلية (LAN) الفرعية (*بالخط المائل*) والملخصات الخاصة بتلك (**بالخط الأسود**).

هنا مثال من إنتاج من الصرة:

```
hub2# show ip eigrp 200 topology
(EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1
,Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
via Connected, Loopback200
```

```
P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
(via Rstatic (2562560/0

P 10.1.1.0/24, 1 successors, FD is 2562560
(via Rstatic (2562560/0
```

يوضح الإخراج أن الصرة تعلم بشبكات LAN الفرعية الخاصة بالخوادم الفرعية (*italic*)، والبادئة الموجزة التي أعلن عنها (**بخط غامق**)، وعنوان IP المعين لكل محادثة عبر التفاوض.

اعتبارات إضافية

أنفاق تتحدث مع الآخرين موجودة بالفعل

نظرا لأن إيقاف تشغيل واجهة نفق DMVPN يتسبب في إزالة إدخالات NHRP، سيتم تقسيم الأنفاق التي يتم التحدث بها والتي توجد بالفعل.

مسح إدخالات NHRP

لا يعتمد محور FlexVPN على عملية تسجيل NHRP من البيانات لمعرفة كيفية توجيه حركة المرور إلى الخلف. ومع ذلك، تعتمد الأنفاق الديناميكية التي يتم التحدث بها على إدخالات NHRP.

في DMVPN، إذا تم مسح NHRP على الصرة، هو يستطيع سبت قصير العمر موصولية مشكلة. في FlexVPN، سيؤدي مسح NHRP على المحولات الفرعية إلى تدمير جلسة عمل FlexVPN IPsec، المتعلقة بأنفاق تتحدث إلى. لا يؤثر مسح NHRP على الصرة على جلسة FlexVPN.

وذلك نظرا لأنه، في FlexVPN بشكل افتراضي:

- لا تتسجل المحددات إلى لوحات التوزيع.
- تعمل الموزعات فقط كمراجعات NHRP، ولا تقم بتثبيت إدخالات NHRP.
- يتم تثبيت إدخالات إختصار NHRP على شبكات للأنفاق التي يتم التحدث بها كما أنها ديناميكية.

المحاذير المعروفة

قد تتأثر حركة مرور البيانات التي يتم الحديث عنها بمعرف تصحيح الأخطاء من CSCub07382 Cisco .

معلومات ذات صلة

- مثال تكوين ترحيل DMVPN إلى FlexVPN السهل
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).