نقل النقل الثابت للترحيل من DMVPN إلى FlexVPN على الأجهزة نفسها

المحتويات

المقدمة

يوفر هذا المستند معلومات حول كيفية الترحيل من شبكة DMVPN الموجودة إلى FlexVPN على نفس الأجهزة.

سوف تتعايش عمليات تكوين كلا الإطارين معا على الأجهزة.

في هذا المستند، يتم عرض السيناريو الأكثر شيوعا فقط: DMVPN باستخدام مفتاح مشترك مسبقا للمصادقة وبروتوكول EIGRP كبروتوكول توجيه.

يوضح هذا المستند الترحيل إلى BGP (بروتوكول التوجيه الموصى به) وبروتوكول EIGRP الأقل مرغوب.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن القارئ يعرف المفاهيم الأساسية ل DMVPN و FlexVPN.

المكونات المستخدمة

لاحظ أنه لا تدعم جميع البرامج والأجهزة الإصدار الثاني من بروتوكول IKEv2. راجع متصفح ميزة Cisco للحصول على معلومات. من الناحية المثالية، إصدارات البرامج التي سيتم إستخدامها هي:

- ISR - 15.2(4)M1 أو أحدث
- ASR1k - 3.6.2 الإصدار S2(2)15.2 أو إصدار أحدث

من بين مزايا النظام الأساسي والبرامج الأحدث إمكانية إستخدام تشفير الجيل التالي، على سبيل المثال، AES GCM للتشفير في IPsec. ويناقش هذا في RFC 4106.

يتيح AES GCM الوصول إلى سرعة تشفير أسرع بكثير على بعض الأجهزة.

لعرض توصيات Cisco حول إستخدام تشفير الجيل التالي والترحيل إليه، ارجع إلى:

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

الاصطلاحات

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

إجراءات الهجرة

وفي الوقت الحالي، تتمثل الطريقة الموصى بها للترحيل من شبكة DMVPN إلى شبكة FlexVPN في عدم عمل الإطارين في نفس الوقت.

ستتم إزالة هذا القيد بسبب ميزات الترحيل الجديدة التي سيتم تقديمها في إصدار ASR 3.10، والتي يتم تتبعها بموجب طلبات التحسين المتعددة تحت جانب Cisco، بما في ذلك CSCuc08066. وينبغي إتاحة هذه السمات في أواخر حزيران/يونيه 2013.

وسيشار إلى عملية الترحيل التي يتعايش فيها كلا الإطارين ويعملان في نفس الوقت على الأجهزة نفسها على أنها عملية ترحيل ميسرة، مما يشير إلى الحد الأدنى للأثر والتغلب السلس على الفشل من إطار إلى آخر.

ويشار إلى عملية الترحيل التي يوجد فيها تكوين كلا الإطارين معا، ولكنها لا تعمل في نفس الوقت، على أنها ترحيل ثابت. وهذا يشير إلى أن التحول من إطار عمل إلى آخر يعني نقص الاتصال عبر VPN، حتى ولو كان الحد الأدنى.

الترحيل الثابت على نفس الأجهزة

في هذا المستند تتم مناقشة الترحيل من شبكة DMVPN موجودة إلى شبكة FlexVPN جديدة على الأجهزة نفسها.

يتطلب هذا الترحيل ألا يعمل كلا الإطارين في نفس الوقت على الأجهزة، مما يتطلب بشكل أساسي تعطيل وظيفة شبكة DMVPN عبر اللوحة قبل تمكين FlexVPN.

إلى أن تتوفر ميزة الترحيل الجديدة، فإن طريقة إجراء عمليات الترحيل باستخدام نفس الأجهزة هي:

1. تحقق من الاتصال عبر DMVPN.
2. قم بإضافة تكوين FlexVPN في مكانه وإيقاف تشغيل واجهات النفق والقالب الظاهري التي تنتمي إلى تكوين جديد.
3. (أثناء أحد إطارات الصيانة) قم بإيقاف تشغيل جميع واجهات نفق DMVPN على جميع المحولات الفرعية والمحورية قبل الانتقال إلى الخطوة 4.
4. واجهات نفق FlexVPN غير المغلقة.
5. تحقق من الاتصال بالموجه.
6. تحقق من الاتصال الذي تم التحدث إليه.
7. *إذا لم تتم عملية التحقق من الصحة في النقطة 5 أو 6 بشكل صحيح ثم الارتداد إلى DMVPN من خلال إيقاف تشغيل واجهة FlexVPN وواجهات DMVPN التي لا يتم إغلاقها.*
8. *تحقق من التحدث إلى اتصال مركز البيانات.*
9. *تحقق من صحة مكالمة تم التحدث إليها.*

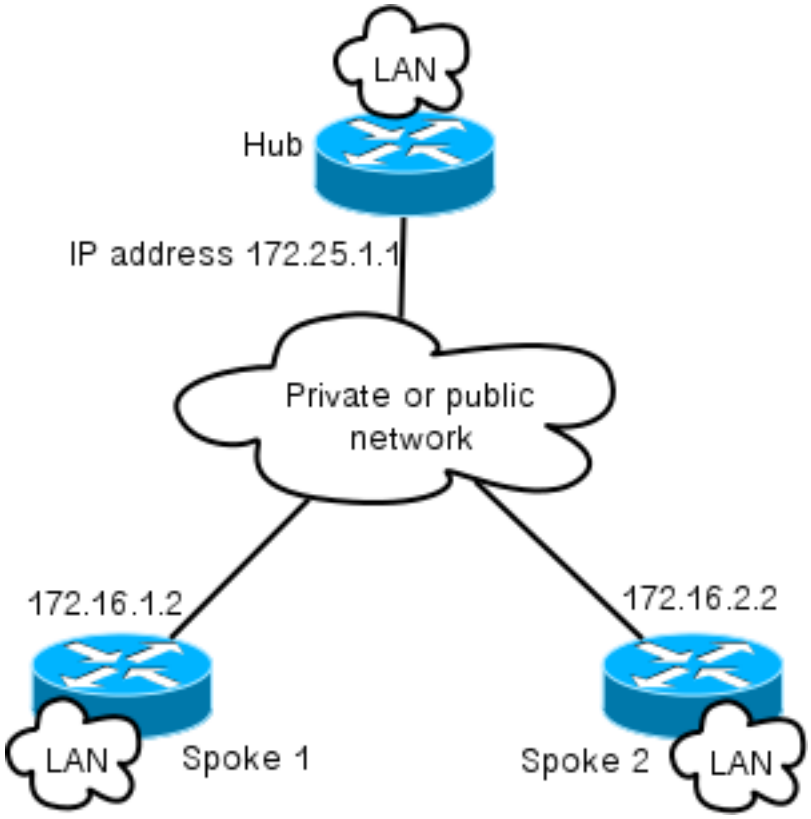
أسلوب مخصص

إذا، نظرا لشبكتك أو تعقيدات التوجيه، قد لا يكون هذا النهج هو الفكرة الأفضل لك، فابدأ مناقشة مع ممثل Cisco الخاص بك قبل الترحيل. يعد مهندس النظام أو مهندس الخدمات المتقدمة هو الشخص الأفضل لمناقشة عملية الترحيل المخصصة.

طوبولوجيا الشبكة

مخطط شبكة النقل

يوضح هذا المخطط مخطط إتصالات نموذجي للمضيفين على الإنترنت. في هذا المستند، يتم إستخدام عنوان IP الخاص بالموجه ل 172.25.1.1) loopback0) لإنهاء جلسة عمل IPsec.

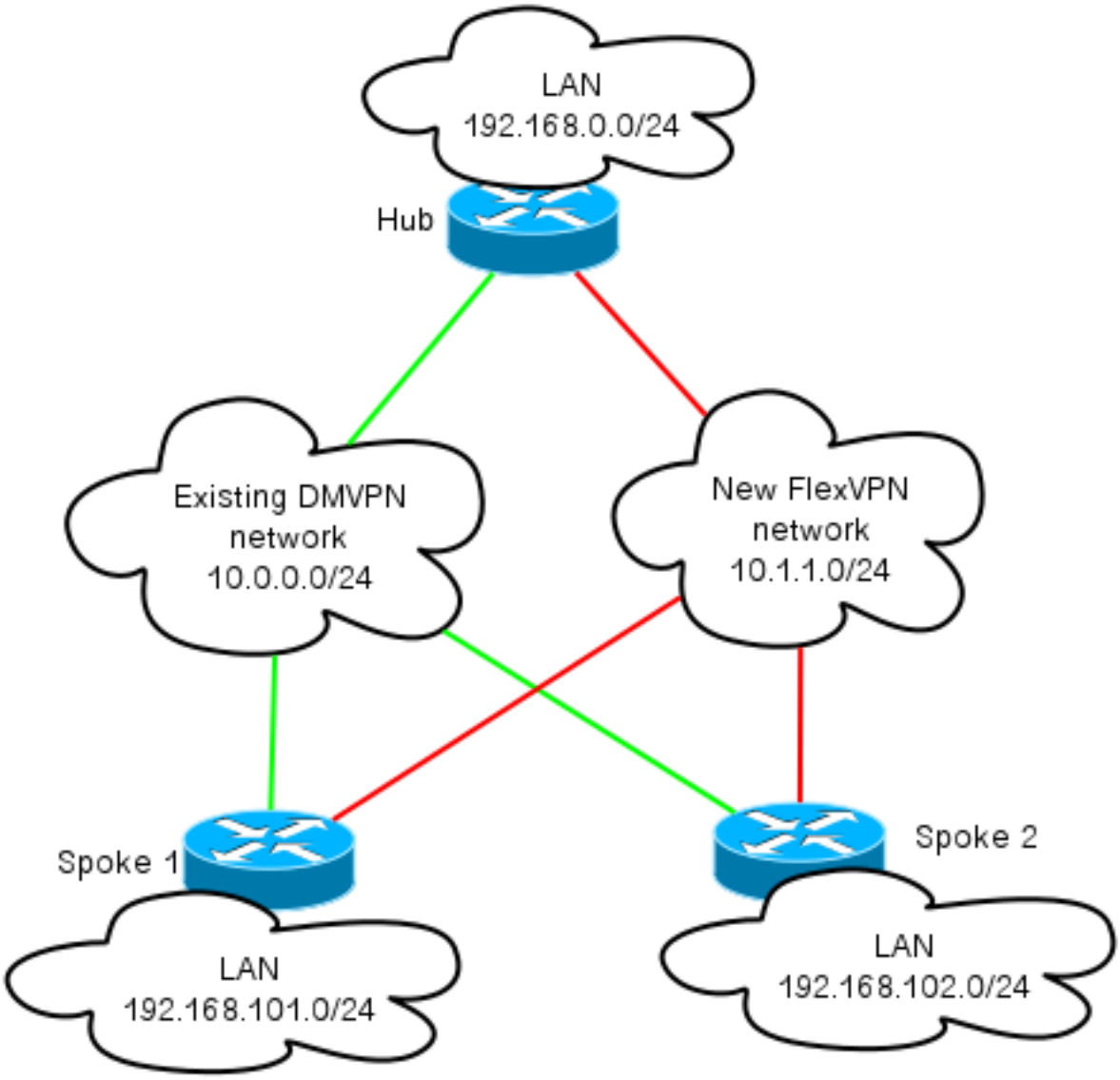


مخطط الشبكة المتفرعة

يوضح الرسم التخطيطي هذا غموسين منفصلين يتم إستخدامهما للتغشية: إتصالات DMVPN (الخضراء) و FlexVPN.

يتم عرض بادئات شبكة المنطقة المحلية للجوانب المقابلة.

لا تمثل الشبكة الفرعية 24/10.1.1.0 شبكة فرعية فعلية من حيث عنونة الواجهة، ولكن بدلا من ذلك مجموعة من مساحة IP المخصصة لسحابة FlexVPN. ستتم مناقشة الأساس المنطقي الذي يكمن وراء ذلك لاحقا في قسم تكوين FlexVPN.



التكوين

تكوين DMVPN

يحتوي هذا القسم على تكوين أساسي لموزع DMVPN وتكلم.

يتم إستخدام المفتاح المشترك مسبقا (PSK) لمصادقة IKEv1.

بمجرد إنشاء IPsec، يتم إجراء تسجيل NHRP من Talk to Hub، حتى يمكن للموزع التعرف على عنونة NBMA الخاصة بالمحولات ديناميكيا.

عندما تقوم NHRP بالتسجيل على متصل وموزع، يمكن أن ينشئ توجيه التجاور والمسارات المتبادلة. في هذا المثال، يتم إستخدام EIGRP كبروتوكول توجيه أساسي لشبكة التراكب.

تحدث تكوين DMVPN

هذا مثال أساسي على تكوين DMVPN مع مصادقة المفتاح المشترك مسبقا و EIGRP كبروتوكول توجيه.

```
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 المحور، يتم الحصول على النفق من loopback0 بعنوان IP بقيمة 172.25.1.1.

الباقي هو النشر القياسي 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 حول IPsec SAs. يوفر IKEv2 تحسينات عبر IKEv1، بدءا بمرونة الرسائل وانتهاء بعدد الرسائل المطلوبة لإنشاء قناة بيانات محمية.
- GRE: على عكس DMVPN، يتم إستخدام واجهات نقطة إلى نقطة ثابتة وحركية، وليس فقط على واجهات GRE متعددة النقاط الثابتة. تتيح هذه التهيئة مرونة إضافية، خاصة لسلوك كل موزع/كل موزع.
- NHRP: في FlexVPN، يستخدم NHRP في المقام الأول لإنشاء اتصال عبر الهاتف. لا يتم تسجيل المحولات إلى الموزع.
- التوجيه: نظرا لأن المحولات لا تقوم بتسجيل NHRP إلى الموزع، يلزمك الاعتماد على آليات أخرى 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 باسم /32 لعنوان IP على الجانب الآخر من النفق، والذي سيسمح بالاتصال المباشر من مركز "التحدث إلى".

في الترحيل الثابت من DMVPN إلى FlexVPN، لا يعمل نظامان الإطارات في نفس الوقت على الأجهزة نفسها. ومع ذلك، يوصى بإبقائها منفصلة.

افصلها على عدة مستويات:

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

تحدث عن تكوين FlexVPN

أحد الفروق في تكوين الكلام في FlexVPN مقارنة ب DMVPN، هو أنه من المحتمل أن يكون لديك واجهتان.

هناك نفق ضروري للتواصل مع مركز قناة و نفق إختياري للتحاور عبر الأنفاق. إذا أخترت عدم إجراء Dynamic Speech إلى Tunneling المتحرك وكنت تفضل أن يتم كل شيء من خلال جهاز صرة، يمكنك إزالة واجهة القالب الظاهري وإزالة تبديل إختصار NHRP من واجهة النفق.

ستلاحظ أيضا أن واجهة النفق الثابت تحتوي على عنوان IP تم إستقباله استنادا إلى التفاوض. وهذا يسمح للموزع بتوفير عنوان IP لواجهة النفق للتكلم 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
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
```

توصي Cisco باستخدام AES GCM في الأجهزة التي تدعمها.

```
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 172.25.1.1
           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
```

PKI هي الطريقة الموصى بها لإجراء مصادقة على نطاق واسع في IKEv2.

ومع ذلك، لا يزال يمكنك إستخدام مفتاح مشترك مسبقا طالما كنت مدركا لحدوده.

هنا مثال تشكيل يستعمل "cisco" ك PSK:

```
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
```

تكوين موزع FlexVPN

عادة مركز هو فقط ينهي ديناميكي يتحدث إلى صرة أنفاق. هذا هو السبب في الصرة تشكيل أنت لن تجد نفق قارن ساكن إستاتيكي ل FlexVPN، بدلا من أن يكون استعملت قالب قارن. وسينتج عن ذلك واجهة وصول ظاهري لكل اتصال.

لاحظ أنه على جانب الموزع تحتاج إلى الإشارة إلى عناوين التجمع التي سيتم تعيينها إلى الفروع.

ستتم إضافة العناوين من هذا التجمع لاحقا في جدول التوجيه مع وجود /32 مسارا لكل كلمة.

```
                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
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
```

توصي Cisco باستخدام AES GCM في الأجهزة التي تدعمها.

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

لاحظ أنه قد تم التعليق في التكوين أسفل عملية AES GCM.

```
crypto ipsec profile default
set ikev2-profile Flex_IKEv2
set transform-set IKEv2 !
interface Loopback0
description DMVPN termination
ip address 172.25.1.1 255.255.255.255
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
shutdown
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 هو الحال على.

لضمان قابلية التطوير والمرونة، أستخدم التراخيص. ومع ذلك، يمكنك إعادة إستخدام التكوين نفسه ل PSK كما هو موضح.

ملاحظة: يوفر IKEv2 المرونة من حيث المصادقة. ويمكن لجانب المصادقة باستخدام PSK بينما يمكن لجانب RSA-SIG الآخر.

ترحيل حركة المرور

الترحيل إلى BGP كبروتوكول توجيه ترابي [مستحسن]

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

في هذا المثال، يتم إستخدام iBGP.

تكوين BGP الذي تحدث

تتألف هجرة المحادثات من جزأين. تمكين 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 جارة BGP (راجع تكوين BGP المحوري في هذا القسم من الترحيل) وتعلم البادئات الجديدة عبر BGP، يمكنك تحويل حركة مرور البيانات من سحابة DMVPN الموجودة إلى سحابة FlexVPN جديدة.

تكوين Hub BGP

عند المنتصف لتجنب الحفاظ على تهيئة الجوار لكل محادثة بشكل منفصل، يتم تكوين مستمعين ديناميكيين.

في هذا الإعداد لن يقوم BGP ببدء إتصالات جديدة، ولكنه سيقبل الاتصال من مجموعة عناوين IP المتوفرة. في هذه الحالة، يكون التجمع المذكور هو 24/10.1.1.0، وهو جميع العناوين في سحابة FlexVPN الجديدة.

```
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
```

ترحيل حركة المرور إلى FlexVPN

كما تمت الإشارة إليه قبل الترحيل، يجب القيام بذلك من خلال إيقاف تشغيل وظائف شبكة DMVPN والنهوض بشبكة FlexVPN.

ويكفل هذا الإجراء الحد الأدنى من الأثر.

1. على كل الجبهات:
```
interface tunnel 0
 shut
```
2. على الموزع:
```
interface tunnel 0
 shut
```
عند هذه النقطة تأكد من عدم وجود جلسات عمل IKEv1 تم إنشاؤها لهذا الموزع من الفروع.يمكن التحقق من هذا الإجراء من خلال التحقق من إخراج الأمر **show crypto isakmp sa** ومراقبة رسائل syslog التي تم إنشاؤها بواسطة جلسة عمل تسجيل التشفير.بمجرد التأكد من هذا الإجراء، يمكنك المتابعة إلى عرض FlexVPN.
3. متابعة على الموزع:
```
interface Virtual-template 1
 no shut
```
4. على الأصفاد:
```
interface tunnel 1
 no shut
```

خطوات التحقق

إستقرار IPsec

أفضل طريقة لتقييم إستقرار IPsec هي مراقبة سجلات النظام باستخدام أمر التكوين هذا الذي تم تمكينه:

```
crypto logging session
```
إذا كنت ترى جلسات العمل تسير صعودا ونزولا، فقد يشير ذلك إلى مشكلة على مستوى IKEv2/FlexVPN يلزم تصحيحها قبل بدء الترحيل.

معلومات BGP المأهولة

إذا كان IPsec مستقرا، فتأكد من ملء جدول BGP بإدخالات من الفروع (على لوحة الوصل) والموجز من لوحة الوصل (على الفروع).

في حالة بروتوكول BGP، يمكن عرض ذلك من خلال التنفيذ:

```
show bgp
or !
show bgp ipv4 unicast
or !
show ip bgp summary
```
مثال للمعلومات الصحيحة من الموزع:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1 01:10:46 0 0 13 82 83 65001 4 10.1.1.101*
1 00:00:44 0 0 13 7 7 65001 4 10.1.1.102*
```

يمكنك أن ترى أن الصرة علمت أن 1 بادئة من كل من القبيين وكل من القبيين تكون ديناميكية (علمت بعلامة نجمية (*).

مثال على معلومات مماثلة من التكلم:

```
Spoke1#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
1 00:03:43 0 0 6 11 11 65001 4 10.1.1.1
```

تلقى "تم التحدث" بادئة واحدة من الموزع. في حالة هذا الإعداد، يجب أن تكون هذه البادئة هي الملخص المعلن عنه على الموزع.

الترحيل إلى أنفاق جديدة باستخدام EIGRP

يعتبر بروتوكول EIGRP خيارا شائعا في شبكات DMVPN نظرا لأنه يتسم بعملية نشر بسيطة نسبيا وإمكانية تقارب سريعة.

ومع ذلك، فإن نطاقه سيكون أسوأ من نطاق بروتوكول BGP ولا يقدم العديد من الآليات المتقدمة التي يمكن أن يستخدمها بروتوكول BGP بمجرد إخراجه من العبوة.

يصف هذا القسم التالي إحدى طرق النقل إلى FlexVPN باستخدام عملية EIGRP جديدة.

التكوين الذي تم تحديثه

في هذا المثال، تتم إضافة AS جديد باستخدام 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: يجب تجنب إنشاء تجاور بروتوكول التوجيه عبر الأنفاق التي يتم التحدث بها، وبالتالي جعل واجهة النفق 1 (يتم التحدث إلى الصرة) فقط غير خاملة.

تم تحديث تكوين الموزع

وعلى نحو مماثل، ينبغي أن تظل شبكة DMVPN هي الطريقة المفضلة لتبادل حركة المرور. ومع ذلك، يجب أن تقوم FlexVPN بالإعلان عن نفس البادئات وتعلمها بالفعل.

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

هناك طريقتان لإعادة الملخص إلى المحادثة.

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

```
ip route 192.168.0.0 255.255.0.0 null 0
ip access-list standard EIGRP_SUMMARY
permit 192.168.0.0 0.0.255.255
router eigrp 200
distribute-list EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500
```

يتيح هذا الخيار التحكم في الملخص وإعادة التوزيع بدون لمس تكوين VT الخاص بالموجه.

- أو يمكنك إعداد عنوان ملخص على نمط DMVPN على القالب الظاهري. لا يوصى بهذا التكوين بسبب المعالجة الداخلية والنسخ المتماثل للملخص المذكور لكل وصول ظاهري. ويظهر هنا من أجل المرجع:

```
interface Virtual-Template1 type tunnel
ip summary-address eigrp 200 172.16.1.0 255.255.255.0
ip summary-address eigrp 200 192.168.0.0 255.255.0.0
delay 2000
```

ترحيل حركة المرور إلى FlexVPN

يلزم القيام بالترحيل من خلال إيقاف تشغيل وظائف شبكة DMVPN والنهوض بشبكة FlexVPN.

ويكفل الإجراء التالي الحد الأدنى من الأثر.

1. على كل الجبهات:

```
interface tunnel 0
shut
```

2. على الموزع:

```
interface tunnel 0
shut
```

عند هذه النقطة تأكد من عدم وجود جلسات عمل IKEv1 تم إنشاؤها لهذا الموزع من الفروع.يمكن التحقق من هذا الإجراء من خلال التحقق من إخراج الأمر **show crypto isakmp sa** ومراقبة رسائل syslog التي تم إنشاؤها بواسطة جلسة عمل تسجيل التشفير.بمجرد التأكد من هذا الإجراء، يمكنك المتابعة إلى عرض

.FlexVPN

3. متابعة على الموزع:

```
interface Virtual-template 1
 no shut
```

4. على كل الجبهات:

```
interface tunnel 1
 no shut
```

خطوات التحقق

إستقرار IPsec

كما في حالة بروتوكول BGP، يلزمك تقييم ما إذا كان بروتوكول IPsec مستقرا. وأفضل طريقة للقيام بذلك هي مراقبة sylog باستخدام أمر التكوين هذا الذي تم تمكينه:

```
crypto logging session
```

إذا كنت ترى جلسات العمل تسير صعودا ونزولا، فقد يشير ذلك إلى مشكلة على مستوى IKEv2/FlexVPN يلزم تصحيحها قبل بدء الترحيل.

معلومات EIGRP في جدول المخطط

تأكد من أن لديك جدول مخطط EIGRP الخاص بك معبأ بإدخالات LAN التي يتم التحدث بها على الموزع والملخص على الفروع. يمكن التحقق من هذا الإجراء من خلال إصدار هذا الأمر على محور (جهات) ومتحدثي (محولات).

```
show ip eigrp topology
```

مثال لمخرجات ملائمة من الكلام:

```
Spoke1#sh ip eigrp topology
(EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1
,Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
r - reply Status, s - sia Status
(... omitted as output related to DMVPN cloud...)
(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

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 (26114560/1709056), Tunnel1

P 10.1.1.107/32, 1 successors, FD is 26112000
via Connected, Tunnel1
```

ستلاحظ أن المتكلم يعرف عن شبكته الفرعية للشبكة المحلية (مائل) وملخصات تلك (**بخط غامق**).

مثال للمخرجات الصحيحة من لوحة الوصل.

```
Hub#sh ip eigrp topology
(EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1
,Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
(EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1
,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, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056
(via Rstatic (1709056/0

P 10.1.1.107/32, 1 successors, FD is 1709056
(via Rstatic (1709056/0


P 10.1.1.106/32, 1 successors, FD is 1709056
(via Rstatic (1709056/0


P 0.0.0.0/0, 1 successors, FD is 1709056
(via Rstatic (1709056/0

P 192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

ستلاحظ أن الموزع يعرف حول الشبكات الفرعية لشبكة LAN الخاصة بالخوادم الفرعية (مائل)، وبادئة الملخص التي يقوم بإعلانها (**بالخط** الغامق) وعنوان IP المعين لكل كلمة عبر التفاوض.

اعتبارات إضافية

الموجود يتحدث إلى الأنفاق

نظرا لأن إيقاف تشغيل واجهة نفق DMVPN يتسبب في إزالة إدخالات NHRP، سيتم تدمير الأنفاق التي يتم التحدث بها حاليا.

مسح إدخالات NHRP

وكما تمت الإشارة مسبقا، لن يعتمد محور FlexVPN على عملية تسجيل NHRP من خلال التحدث لمعرفة كيفية توجيه حركة المرور إلى الخلف. ومع ذلك، تعتمد Dynamic Talk إلى الأنفاق المحولة على إدخالات NHRP.

في DMVPN حيث كان من الممكن أن يؤدي مسح NHRP على الموزع إلى مشاكل اتصال قصيرة العمر.

في مسح FlexVPN، سيتسبب بروتوكول NHRP على الخوادم في تعطيل جلسة عمل FlexVPN IPsec، المرتبطة بالأنفاق التي يتم التحدث بها،. في مسح NHRP، لن يكون لأي محور تأثير على FlexVPN جلسة.

وهذا يرجع إلى حقيقة أنه في FlexVPN، بشكل افتراضي:

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

المحاذير المعروفة

تحدث إلى حركة المرور المتداولة قد تتأثر ب CSCub07382.

معلومات ذات صلة

- 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).