مثال تكوين ترحيل DMVPN إلى FlexVPN السهل

المحتويات

المقدمة

يوضح هذا المستند كيفية تنفيذ ترحيل *ناعم* حيث تعمل كل من DMVPN (Dynamic Multipoint VPN) و FlexVPN على جهاز في نفس الوقت دون الحاجة إلى حل بديل ويقدم مثالا على التكوين.

ملاحظة: يتوسع هذا المستند في المفاهيم الموضحة في الترحيل إلى FlexVPN: النقل الثابت من DMVPN إلى FlexVPN على الأجهزة نفسها وترحيل FlexVPN: النقل الثابت من DMVPN إلى FlexVPN على مقالات Cisco على هيئة محور مختلف. تصف كلا الوثيقتين عمليات الترحيل *الثابتة*، التي تتسبب في بعض التعطيل لحركة المرور أثناء الترحيل. ترجع القيود الواردة في هذه المقالات إلى نقص في برامج Cisco IOS® التي تم تصحيحها الآن.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- DMVPN
- FlexVPN

المكونات المستخدمة

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

- موجه الخدمة المتكاملة (ISR) من Cisco، الإصدار M(3)15.3 أو إصدار أحدث
- موجه الخدمة المجمعة (ASR1K) من Cisco 1000 Series الإصدار 3.10 أو إصدار أحدث

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

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.

معلومات أساسية

إحدى مزايا النظام الأساسي والبرنامج الأحدث من Cisco IOS هي القدرة على إستخدام تشفير الجيل التالي. والمثال على ذلك هو إستخدام معيار التشفير المتقدم (AES) في وضع الشبكات/العداد (GCM) للتشفير في IPsec، كما هو موضح في RFC 4106. يتيح AES GCM سرعات تشفير أسرع بكثير على بعض الأجهزة.

ملاحظة: للحصول على معلومات إضافية حول إستخدام تشفير الجيل التالي والترحيل إليه، راجع مقالة التشفير من الجيل التالي من Cisco.

التكوين

يركز مثال التكوين هذا على الترحيل من تكوين المرحلة 3 ل DMVPN إلى FlexVPN، نظرا لأن كلا التصميمين يعملان بشكل متماثل.

	المرحلة الثانية من DMVPN	المرحلة الثالثة من DMVPN	FlexVPN
النقل	GRE عبر IPsec	GRE عبر IPsec	GRE عبر IPsec و
إستخدام NHRP	التسجيل وحل المنازعات	التسجيل وحل المنازعات	قرار
الخطوة التالية من تحدث	محاور أو محاور أخرى	ملخص من الموزع	ملخص من الموزع
تبديل إختصار NHRP	لا	نعم	نعم (إختياري)
إعادة توجيه NHRP	لا	نعم	نعم
IKE و IPsec	IPsec إختياري و IKEv1 بشكل	IPsec إختياري و IKEv1 بشكل	IPsec و IKEv2

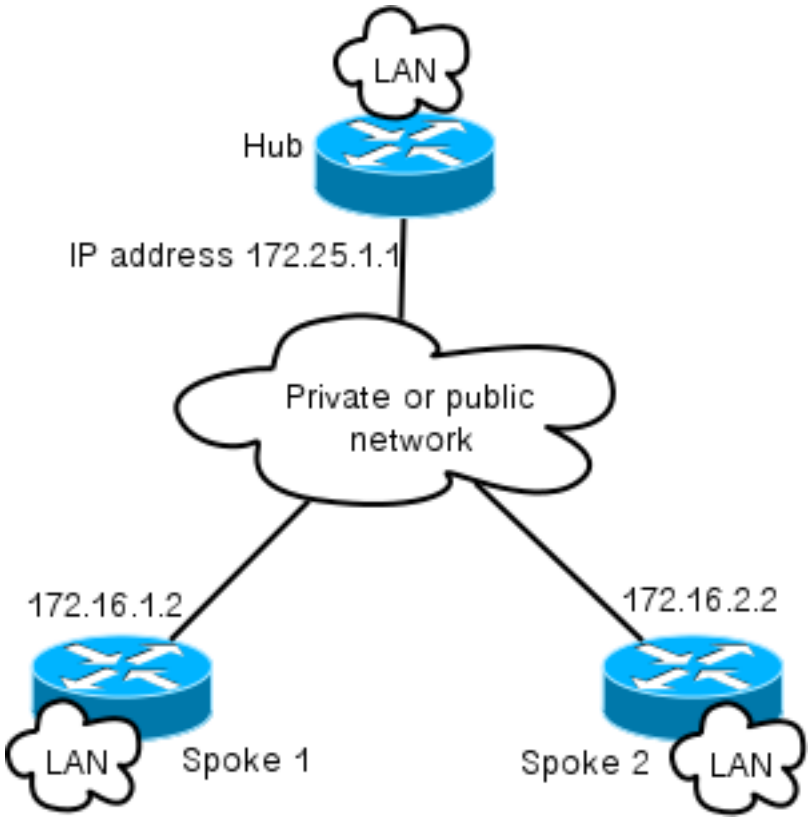
نموذجي نموذجي

مخططات الشبكة

يوفر هذا القسم مخططات شبكة النقل والتغشية على حد سواء.

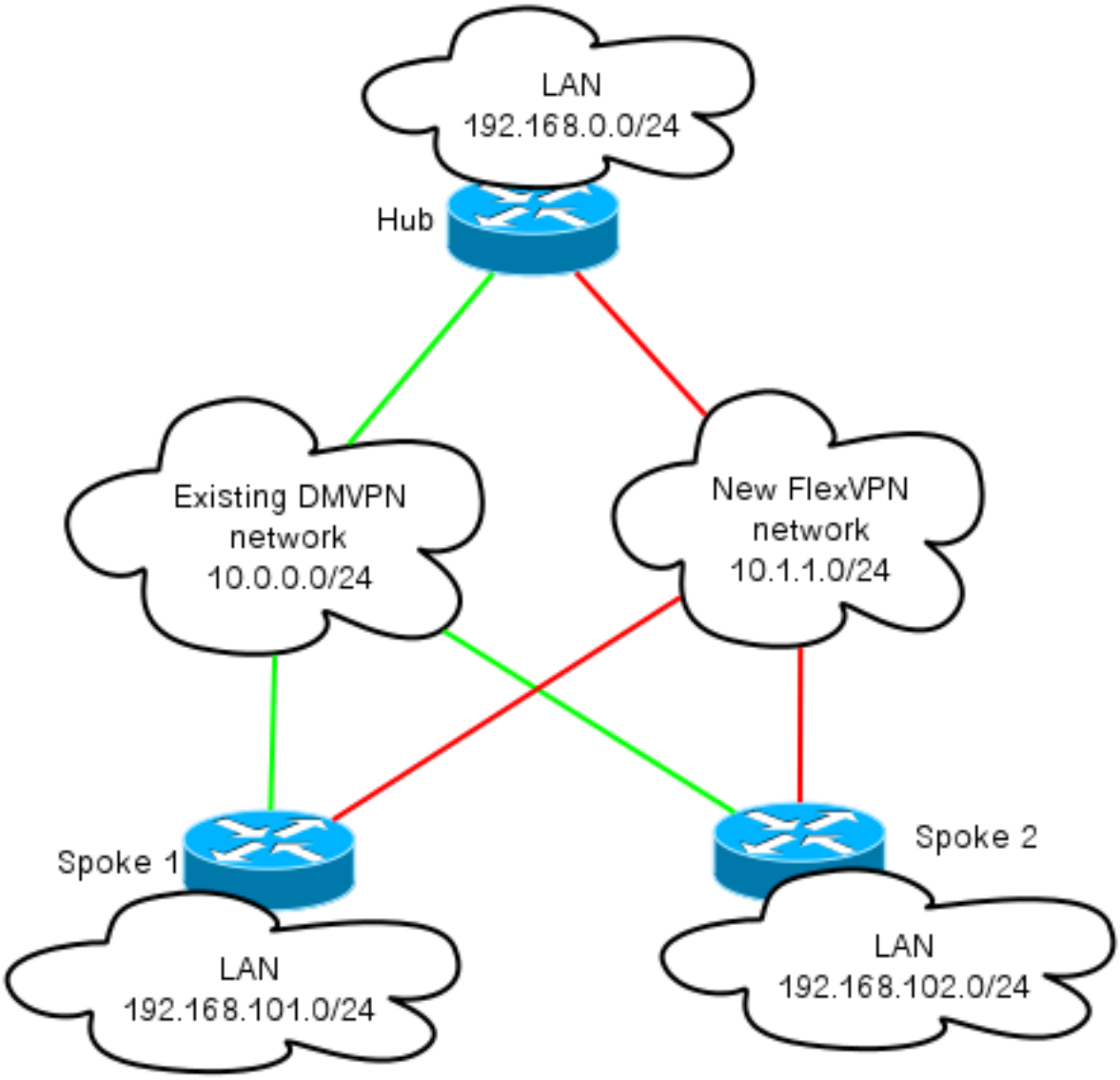
الرسم التخطيطي لشبكة النقل

تتضمن شبكة النقل المستخدمة في هذا المثال موصلا فرديا مع ربطين فردين. يتم توصيل جميع الأجهزة من خلال شبكة تحاكي الإنترنت.



الرسم التخطيطي لشبكة التراكب

تتضمن شبكة التغشية المستخدمة في هذا المثال موصلا فرديا مع ربطين فردين. تذكر أن كل من DMVPN و FlexVPN ينشطان في نفس الوقت، لكنهما يستخدمان مساحات عنوان IP مختلفة.



التكوينات

يقوم هذا التكوين بترحيل النشر الأكثر شيوعا ل DMVPN المرحلة 3 عبر بروتوكول توجيه العبارة الداخلي المحسن (EIGRP) إلى FlexVPN مع بروتوكول العبارة الحدودية (BGP). توصي Cisco باستخدام BGP مع FlexVPN، لأنها تسمح بعمليات النشر بالتوسع بشكل أفضل.

ملاحظة: تنهي الموزع جلسات عمل DMVPN) IKEv1) و FlexVPN) IKEv2) على نفس عنوان IP. لا يمكن تحقيق ذلك إلا مع إصدارات Cisco IOS الأخيرة.

التكوين الذي تم التحدث به

هذا تكوين أساسي للغاية، مع إستثنائين بارزين يسمحان بالتشغيل المشترك لكل من IKEv1 و IKEv2، بالإضافة إلى إطارين يستخدمان تضمين التوجيه العام (GRE) عبر IPsec للنقل من أجل التعايش.

ملاحظة: تم إبراز التغييرات ذات الصلة في تكوين رابطة أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) و IKEv2 بالخط العريض.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

crypto logging session

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

crypto isakmp policy 10
encr aes
authentication pre-share

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

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
desciption DMVPN tunnel
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 key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub tunnel
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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

يسمح لك الإصدار 15.3 من Cisco IOS بربط كل من توصيفات IKEv2 و ISAKMP معا في تكوين *حماية نفق*. وإلى جانب بعض التغييرات الداخلية التي طرأت على الرمز، يسمح ذلك ل IKEv1 و IKEv2 بالعمل على نفس الجهاز في نفس الوقت.

نظرا للطريقة التي يحدد بها Cisco IOS التوصيفات (IKEv1 أو IKEv2) في الإصدارات الأقدم من 15.3، فقد أدى إلى بعض المحاذير، مثل الحالات التي يتم فيها بدء IKEv1 إلى IKEv2 من خلال النظير. ويقوم الفصل بين هذه الفئة الآن على مستوى الشكل وليس على مستوى الواجهة، وهو ما يتم تحقيقه عن طريق واجهة سطر الأوامر الجديدة.

هناك ترقية أخرى في إصدار Cisco IOS الجديد هي إضافة *مفتاح النفق*. وهذا ضروري لأن على حد سواء DMVPN و FlexVPN يستخدم نفس واجهة المصدر ونفس عنوان IP للوجهة. مع وجود هذا في موضعه، لا توجد طريقة لنفق GRE لمعرفة واجهة النفق التي يتم إستخدامها لإزالة كبسلة حركة المرور. يتيح لك مفتاح النفق التمييز بين **النفق0** و**النفق 1** مع إضافة مستوى أعلى صغير (4 بايت). يمكن تكوين مفتاح مختلف على كلا الواجهات، ولكن عادة ما تحتاج إلى التمييز بين نفق واحد.

ملاحظة: لا يكون خيار حماية النفق المشترك مطلوبا عندما يقوم DMVPN و FlexVPN بمشاركة نفس الواجهة.

لذلك، يعد تكوين بروتوكول التوجيه المتصل أساسيا. يعمل بروتوكول EIGRP وبروتوكول بوابة الحدود (BGP) بشكل منفصل. يعلن EIGRP فقط عبر واجهة النفق لتجنب النظر عبر الأنفاق التي يتم التحدث بها، مما يحد من قابلية التطوير. يحتفظ BGP بعلاقة فقط مع موجه المحور (**10.1.1.1**) للإعلان عن الشبكة المحلية (**24/192.168.101.0**).

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

تكوين الموزع

يجب إجراء تغييرات مماثلة على تكوين جانب المحور كما هو موضح في قسم **التكوين** المتصل.

ملاحظة: تم إبراز التغييرات ذات الصلة بتكوين ISAKMP و IKEv2 بالخط العريض.

```
crypto ikev2 authorization policy default
 pool FlexSpokes
 route set interface

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

crypto isakmp policy 10
 encr aes
 authentication pre-share

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2


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 key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
 ip nhrp network-id 2
 ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

على جانب الموزع، يقع الربط بين ملف تعريف IKE وملف تعريف IPsec على مستوى ملف التعريف، بخلاف التكوين المتحرك، حيث يتم إكمال ذلك عبر أمر **حماية النفق**. وكلا النهجين هما أسلوبان قابلان للتطبيق لإتمام هذا الربط.

من المهم ملاحظة أن معرفات شبكة بروتوكول تحليل الخطوة (Hop) التالية (NHRP) مختلفة ل DMVPN و FlexVPN في السحابة. وفي معظم الحالات، يكون من غير المرغوب فيه أن تنشئ اللجنة الوطنية لحقوق الإنسان مجالا واحدا على كلا الإطارين.

ويميز مفتاح النفق بين أنفاق DMVPN و FlexVPN على مستوى GRE من أجل تحقيق الهدف نفسه المذكور في قسم **التكوين** الذي **يتحدث**.

تكوين التوجيه على الصرة أساسي إلى حد ما. يحتفظ الجهاز الموزع بعلاقتين مع أي من المحادثات المحددة، أحدهما يستخدم EIGRP والآخر يستخدم BGP. يستخدم تكوين BGP نطاق الإصغاء لتجنب تكوين طويل لكل محادثة.

يتم تقديم عناوين الملخص مرتين. يرسل تكوين EIGRP ملخصا باستخدام تكوين **النفق0** IP summary-address) EIGRP 100)، ويقدم BGP ملخصا باستخدام عنوان التجميع. يلزم توفر الملخصات لضمان حدوث إعادة توجيه NHRP، ومن أجل تبسيط تحديثات التوجيه. يمكنك إرسال إعادة توجيه NHRP (يشبه كثيرا إعادة توجيه بروتوكول رسائل التحكم في الإنترنت (ICMP) التي تشير إلى ما إذا كانت هناك خطوة أفضل لوجهة معينة، والتي تتيح إنشاء نفق تتحدث إليه. كما يتم إستخدام هذه الملخصات لتقليل مقدار تحديثات التوجيه التي يتم إرسالها بين الصرة وكل محكي، مما يسمح للمنظومات بالتوسع بشكل أفضل.

```
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

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

التحقق من الصحة

يتم تقسيم التحقق من مثال التكوين هذا إلى عدة أقسام.

فحوصات ما قبل الترحيل

بما أن كلا من DMVPN/EIGRP و FlexVPN/BGP يعملان في آن واحد، فيجب التحقق من أن المحادثة تحافظ على علاقة عبر IPsec مع كل من IKEv1 و IKEv2، وأنه يتم التعرف على البادئات المناسبة عبر EIGRP و BGP.

في هذا المثال، يظهر **Talk1** أنه يتم الحفاظ على جلستين باستخدام موجه الموزع، الأول يستخدم IKEv1/**Tunnel0** وواحد يستخدم IKEv2/**Tunnel1**.

ملاحظة: يتم الاحتفاظ باتحادي أمان IPsec (واحد وارد وواحد صادر) لكل نفق من الأنفاق.

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
 Profile: DMVPN_IKEv1
 Session status: UP-ACTIVE
 Peer: 172.25.1.1 port 500
  Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
 IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map
```

```
Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

عند التحقق من بروتوكولات التوجيه، يجب عليك التحقق من تكوين علاقات جوار ومن تعلم البادئات الصحيحة. يتم التحقق من هذا أولا باستخدام EIGRP. دققت أن يكون الصرة مرئي كجار، وأن 16/192.168.0.0 عنوان (الملخص) علمت من الصرة:

```
Spoke1#show ip eigrp neighbors
(EIGRP-IPv4 Neighbors for AS(100
H Address Interface Hold Uptime SRTT RTO Q Seq
sec) (ms) Cnt Num)
Tu0 10 00:04:02 7 1398 0 13 10.0.0.1 0

Spoke1#show 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

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 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

بعد ذلك، تحقق من بروتوكول BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1 00:06:56 0 0 3 11 13 65001 4 10.1.1.1
Spoke1#show bgp
BGP table version is 3, local router ID is 192.168.101.1
,Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
,r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter
,x best-external, a additional-path, c RIB-compressed
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

يظهر الإخراج أن الصرة FlexVPN عنوان (10.1.1.1) هي جارة والتي من خلالها يتلقى المحادثة بادئة واحدة (16/192.168.0.0). وبالإضافة إلى ذلك، يقوم بروتوكول BGP بإعلام المسؤول بحدوث فشل في قاعدة معلومات التوجيه (RIB) للبادئة 16/192.168.0.0. يحدث هذا الفشل بسبب وجود مسار أفضل لتلك البادئة الموجودة بالفعل في جدول التوجيه. تم إنشاء هذا المسار بواسطة EIGRP، ويمكن تأكيده إذا قمت بالتحقق من جدول التوجيه.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
```

```
Known via "eigrp 100", distance 90, metric 26880000, type internal
                                                Redistributing via eigrp 100
                                      Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
                                                        :Routing Descriptor Blocks
                                    from 10.0.0.1, 00:10:07 ago, via Tunnel0 ,10.0.0.1 *
                                      Route metric is 26880000, traffic share count is 1
                            Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
                                                Reliability 255/255, minimum MTU 1400 bytes
                                                        Loading 1/255, Hops 1
```

هجرة

تحقق القسم السابق من تكوين كل من IPsec وبروتوكولات التوجيه والعمل كما هو متوقع. تتمثل إحدى أسهل الطرق للترحيل من DMVPN إلى FlexVPN على نفس الجهاز في تغيير المسافة الإدارية (AD). في هذا المثال، يحتوي بروتوكول BGP الداخلي (iBGP) على إعلان بقيمة **200**، ويتكون بروتوكول EIGRP من إعلان بقيمة **90**.

لكي تتدفق حركة المرور عبر FlexVPN بشكل صحيح، يجب أن يحتوي BGP على AD أفضل. في هذا المثال، يتم تغيير إعلان EIGRP إلى **230** و**240** للمسارات الداخلية والخارجية، على التوالي. وهذا يجعل BGP AD (من **200**) أكثر تفضيلا لبادئة **16/192.168.0.0**.

وهناك طريقة أخرى تستخدم لتنفيذ هذا الإجراء وهي تقليل إعلان BGP. ومع ذلك، فإن البروتوكول الذي يتم تشغيله بعد الترحيل له قيم غير افتراضية، مما يمكن أن يؤثر على أجزاء أخرى من النشر.

في هذا المثال، يتم إستخدام الأمر **debug ip routing** للتحقق من العملية على الصوت.

ملاحظة: إذا كانت المعلومات الواردة في هذا القسم مستخدمة على شبكة إنتاج، تجنب إستخدام أوامر تصحيح الأخطاء، والاعتماد على أوامر show المدرجة في القسم التالي. كما يجب أن تعيد عملية EIGRP التي يتم التحدث عنها تأسيس التجاور مع الصرة.

```
                                                Spoke1#conf t
                                .Enter configuration commands, one per line. End with CNTL/Z
                                                Spoke1(config)#router eigrp 100
                                        Spoke1(config-router)# distance eigrp 230 240
                                                Spoke1(config-router)#^Z
                                                Spoke1#
                        Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console*
                        Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1*
                                                Tunnel0) is down: route configuration changed)

                                Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1*,
                                                [eigrp metric [90/26880000
                                Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush*
                                Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16*
                                        : (Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0*
                                                via 10.1.1.1

                        [Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0*
                                                Spoke1#
                        Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1*
                                                Tunnel0) is up: new adjacency)
```

هناك ثلاثة إجراءات مهمة ينبغي أن نلاحظها في هذا الناتج:

- يشير المتحدث إلى أن الإعلان تغير، وتعطيل التجاور.
- في جدول التوجيه، يتم إلغاء بادئة EIGRP، ويتم تقديم BGP.
- تتم إعادة التجاور إلى لوحة الوصل عبر EIGRP على الإنترنت.

عندما تقوم بتغيير AD على جهاز، فإنه يؤثر فقط على المسار من الجهاز إلى الشبكات الأخرى، ولا يؤثر على كيفية عمل الموجهات الأخرى للتوجيه. على سبيل المثال، بعد زيادة مسافة EIGRP على **Talk1** (وهو يستخدم FlexVPN على السحابة لتوجيه حركة المرور)، يحتفظ الموزع بأدوات AD التي تم تكوينها (الافتراضية). هذا يعني أنه يستخدم DMVPN لإعادة توجيه حركة مرور البيانات إلى **Talk1**.

في سيناريوهات معينة، قد يتسبب ذلك في حدوث مشاكل، مثل عندما تتوقع جدران الحماية حركة مرور العائدة على الواجهة نفسها. لذلك، يجب عليك تغيير AD على كل القفزات قبل أن تقوم بتغييره على الصرة. يتم ترحيل حركة مرور البيانات بالكامل بواسطة FlexVPN فقط بمجرد اكتمال ذلك.

ترحيل EIGRP إلى EIGRP

لا تتم مناقشة عملية الترحيل من DMVPN إلى FlexVPN التي تشغل بروتوكول EIGRP فقط بشكل متعمق في هذا المستند، ومع ذلك، يتم ذكرها هنا للحصول على اكتمالها.

من الممكن إضافة كل من DMVPN و EIGRP إلى مثيل توجيه النظام الذاتي ل EIGRP نفسه. مع وجود هذا في موضعه، يتم إنشاء توجيه التجاور على كلا نوعي السحب. وقد يؤدي ذلك إلى حدوث موازنة الأحمال، وهو ما لا يوصى به عادة.

لضمان إختيار FlexVPN أو DMVPN، يمكن للمسؤول تعيين قيم **تأخير** مختلفة لكل واجهة. ومع ذلك، فمن المهم تذكر أنه لا يمكن إجراء أي تغييرات على واجهات القالب الظاهري أثناء وجود واجهات الوصول الظاهري المطابقة.

فحوصات ما بعد الترحيل

كما هو الحال بالنسبة للعملية المستخدمة في قسم **عمليات التحقق قبل الترحيل**، يجب التحقق من بروتوكول IPsec وبروتوكول التوجيه.

تحقق أولا من IPsec:

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

وكما هو الحال من قبل، يتم عرض جلستين، لكل منهما وحدتا IPsec نشيطتان.

في المحادثة، يشير المسار الكلي (**16/192.168.0.0**) من المركز ويتم التعرف عليه عبر BGP.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
  Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
    Last update from 10.1.1.1 00:14:07 ago
    :Routing Descriptor Blocks
  from 10.1.1.1, 00:14:07 ago ,10.1.1.1 *
  Route metric is 0, traffic share count is 1
                                  AS Hops 0
                                MPLS label: none
```

وبالمثل، يجب أن تكون شبكة LAN التي يتم التحدث بها والتي تم تثبيتها مسبقا على الموزع معروفة عبر EIGRP. في هذا المثال، يتم التحقق من الشبكة الفرعية LAN Spoke2:

```
Hub#show ip route 192.168.102.0 255.255.255.0
    Routing entry for 192.168.102.0/24
Known via "bgp 65001", distance 200, metric 0, type internal
    Last update from 10.1.1.106 00:04:35 ago
    :Routing Descriptor Blocks
  from 10.1.1.106, 00:04:35 ago ,10.1.1.106 *
  Route metric is 0, traffic share count is 1
                                  AS Hops 0
                                MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

في الإخراج، يتم تحديث مسار إعادة التوجيه بشكل صحيح ويخرج نقاط من واجهة الوصول الظاهري.

اعتبارات إضافية

يصف هذا القسم بعض المناطق الإضافية ذات الأهمية ذات الصلة بمثال التكوين هذا.

أنفاق اتصال هاتفي موجودة

مع الانتقال من EIGRP إلى BGP، لا تتأثر الأنفاق التي يتم التحدث بها، لأن التبديل المختصر لا يزال قيد التشغيل. يدخل التبديل المختصر على مكبر الصوت مسار NHRP أكثر تحديدا مع إعلان يبلغ 250.

هنا مثال من هذا طريق:

```
Spoke1#show ip route 192.168.102.100
  Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
    :Routing Descriptor Blocks
from 10.1.1.106, 00:00:42 ago, via Virtual-Access1 ,10.1.1.106 *
  Route metric is 1, traffic share count is 1
```

الاتصال بين الفروع المرحلة وغير المرحلة

إذا كان الشخص الذي تم تكليفه بالفعل على FlexVPN/BGP يريد الاتصال بجهاز لم تبدأ عملية الترحيل من أجله، فإن حركة مرور البيانات تتدفق دائما عبر الصرة.

هذه هي العملية التي تحدث:

1. يجري المحادثة بحث المسار عن الوجهة، والذي يشير من خلال مسار ملخص يتم الإعلان عنه بواسطة الموزع.
2. أرسلت الربط نحو الصرة.
3. يستلم الصرة الربط وينفذ بحث طريق للغاية، أي يشير إلى آخر قارن أن يكون جزء من مختلف NHRP مجال.

ملاحظة: يختلف معرف شبكة NHRP في تكوين الموزع السابق لكل من FlexVPN و DMVPN.
حتى إذا كانت معرفات شبكة NHRP موحدة، فقد تحدث مشكلة في الحالات التي يقوم فيها الشخص الذي تم ترحيله بتوجيه الكائنات عبر شبكة FlexVPN. يتضمن هذا التوجيه المستخدم لتكوين تبديل الاختصار. يحاول الشخص الذي لم يتم ترحيله تشغيل الكائنات عبر شبكة DMVPN، بهدف محدد لإجراء تبديل مختصر.

استكشاف الأخطاء وإصلاحها

يصف هذا القسم الفئتين المستخدمتين بشكل نموذجي من أجل التعامل مع عملية الترحيل.

مشاكل مع محاولات إنشاء أنفاق

أكمل الخطوات التالية إذا فشل تفاوض IKE:

1. دققت الحالة حالي مع هذا أمر:

show crypto isakmp sa - يعرض هذا الأمر المبلغ والمصدر والوجهة لجلسة IKEv1.**show crypto ipSec**-IKEv1 يكشف هذا الأمر عن نشاط IPsec SAs.**ملاحظة**: على عكس ما هو الحال في IKEv1، في هذا الإخراج تظهر قيمة مجموعة السرية التامة لإعادة التوجيه Diffie-Hellman (DH) (PFS) على أنها **PFS (Y/N): N، مجموعة DH: none** أثناء تفاوض النفق الأول، ومع ذلك، بعد حدوث مفتاح، تظهر القيم الصحيحة. هذا ليس خطأ، على الرغم من وصف السلوك في CSCug67056. الفرق بين IKEv1 و IKEv2 هو أنه في الحالة الأخيرة، يتم إنشاء شبكات SA التابعة كجزء من تبادل **المصادقة**. يتم إستخدام مجموعة DH التي تم تكوينها ضمن خريطة التشفير فقط أثناء أحد المفاتيح. لهذا السبب، ترى **PFS (Y/N): N، مجموعة DH: لا شيء** حتى المفتاح الأول. مع IKEv1، سترى سلوكا مختلفا لأن إنشاء SA التابع يحدث أثناء الوضع السريع، ولرسالة **CREATE_CHILD_SA** أحكام لنقل حمولة تبادل المفاتيح التي تحدد معلمات DH لاستخراج سر مشترك جديد.**show crypto ikev2 sa** - يوفر هذا الأمر مخرجات مماثلة ل ISAKMP ولكنها خاصة ب IKEv2.**show crypto session** - يوفر هذا الأمر إخراج الملخص لجلسات عمل التشفير على هذا الجهاز.**show crypto socket** - يعرض هذا الأمر حالة مآخذ التشفير.**show crypto map** - يعرض هذا الأمر تعيين توصيفات IKE و IPsec للواجهات.**show ip nhrp** - يوفر هذا الأمر معلومات NHRP من الجهاز. وهذا مفيد للتحاور عبر المواقع التي تعمل بتقنية FlexVPN، وللحلقات التي يتم التحدث بها أو التحدث إليها عبر المحور في مواقع DMVPN.
2. استعملت هذا أمر in order to صححت النفق إنشاء:

debug crypto ikev2debug crypto isakmpdebug crypto ipSecdebug crypto kmi

مشاكل نشر المسار

هنا بعض الأوامر المفيدة التي يمكنك إستخدامها لاستكشاف أخطاء EIGRP والمخطط وإصلاحها:

- **show bgp summary** - أستخدم هذا الأمر للتحقق من الجيران المتصلين وحالاتهم.
- **show ip eigrp neighbor** - أستخدم هذا الأمر لعرض الجيران المتصلين عبر EIGRP.
- **show bgp** - أستخدم هذا الأمر للتحقق من البادئات التي تم التعرف عليها عبر BGP.
- **show ip eigrp topology** - أستخدم هذا الأمر لعرض البادئات التي تم التعرف عليها عبر EIGRP.

من المهم معرفة أن البادئة المتعلمة تختلف عن البادئة التي يتم تثبيتها في جدول التوجيه. لمزيد من المعلومات حول

هذا الأمر، راجع تحديد المسار في مقالة Cisco Routers Cisco، أو كتاب المطبعة للتوجيه TCP/IP من Cisco.

المحاذير المعروفة

يوجد قيد يتوافق مع معالجة نفق GRE على ASR1K. يتم تعقب هذا ضمن معرف تصحيح الأخطاء من Cisco CSCue00443. في هذا الوقت، يحتوي التحديد على إصلاح مجدول في البرنامج Cisco IOS XE Software، الإصدار 3.12.

مراقبة هذا الخطأ إذا كنت تريد إخطارا بمجرد أن يصبح الإصلاح متاحا.

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).