Exemple de configuration de migration logicielle DMVPN vers FlexVPN

Contenu

Introduction

Ce document décrit comment effectuer une migration *logicielle* où DMVPN (Dynamic Multipoint VPN) et FlexVPN fonctionnent simultanément sur un périphérique sans avoir besoin de contournement et fournit un exemple de configuration.

> **Note**: Ce document développe les concepts décrits dans la migration FlexVPN : Déplacement de DMVPN vers FlexVPN sur les mêmes périphériques et migration FlexVPN : Déplacement de DMVPN vers FlexVPN sur un autre article Hub Cisco. Ces deux documents décrivent des migrations *difficiles*, qui provoquent des perturbations du trafic pendant la migration. Les limitations de ces articles sont dues à une défaillance du logiciel Cisco IOS®

qui est maintenant corrigée.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseaux RPV multipoint dynamique (DMVPN)
- FlexVPN

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Integrated Service Router (ISR) versions 15.3(3)M ou ultérieures
- Routeur à services agrégés (ASR1K) de la gamme Cisco 1000, versions 3.10 ou ultérieures

> **Note**: Tous les logiciels et matériels ne prennent pas en charge Internet Key Exchange Version 2 (IKEv2). Référez-vous à Navigateur de fonctionnalités Cisco pour plus d'informations.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

L'un des avantages de la nouvelle plate-forme et du nouveau logiciel Cisco IOS est la possibilité d'utiliser la cryptographie nouvelle génération. Un exemple est l'utilisation de la norme AES (Advanced Encryption Standard) en mode Galois/Counter (GCM) pour le chiffrement dans IPsec, comme discuté dans la RFC 4106. AES GCM permet des vitesses de cryptage beaucoup plus rapides sur certains matériels.

> **Note**: Pour plus d'informations sur l'utilisation et la migration vers la cryptographie de nouvelle génération, reportez-vous à l'article Next Generation Encryption Cisco.

Configuration

Cet exemple de configuration se concentre sur une migration d'une configuration DMVPN de phase 3 vers un FlexVPN, car les deux conceptions fonctionnent de la même manière.

DMVPN Phase 2	DMVPN Phase 3	FlexVPN

Transport	GRE sur IPsec	GRE sur IPsec	GRE sur IPsec, V
Utilisation NHRP	Enregistrement et résolution	Enregistrement et résolution	Résolution
Saut suivant de Spoke	Autres rayons ou concentrateur	Résumé du concentrateur	Résumé du concentrateur
Commutation de raccourcis NHRP	Non	Oui	Oui (facultatif)
Redirection NHRP	Non	Oui	Oui
IKE et IPsec	IPsec facultatif, IKEv1 standard	IPsec facultatif, IKEv1 standard	IPsec, IKEv2

Diagrammes du réseau

Cette section fournit des diagrammes de réseau de transport et de superposition.

Schéma du réseau de transport

Le réseau de transport utilisé dans cet exemple comprend un seul concentrateur avec deux rayons connectés. Tous les périphériques sont connectés via un réseau qui simule Internet.

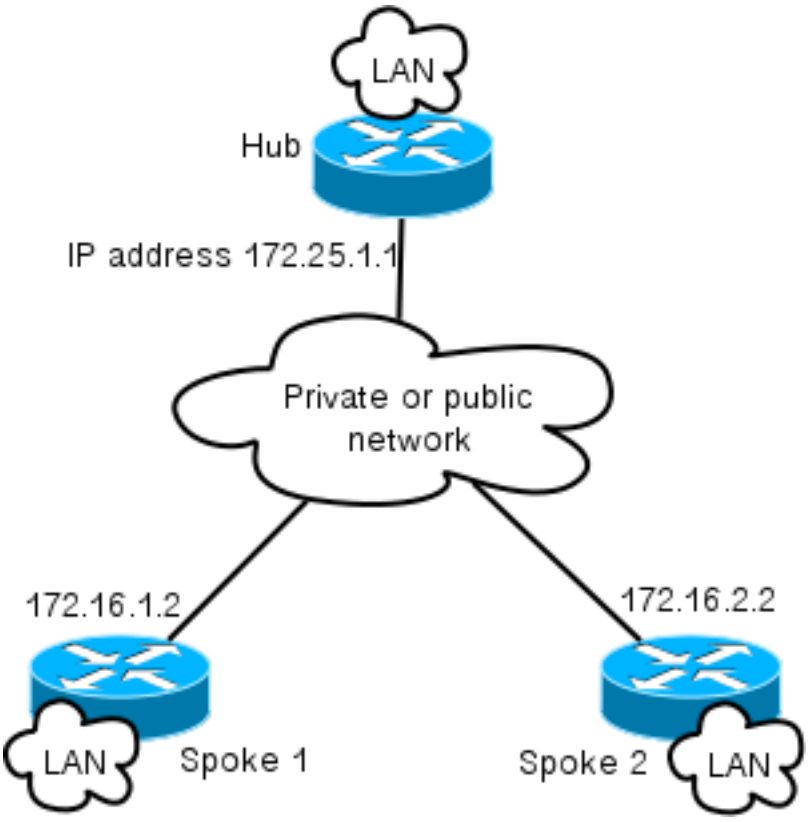
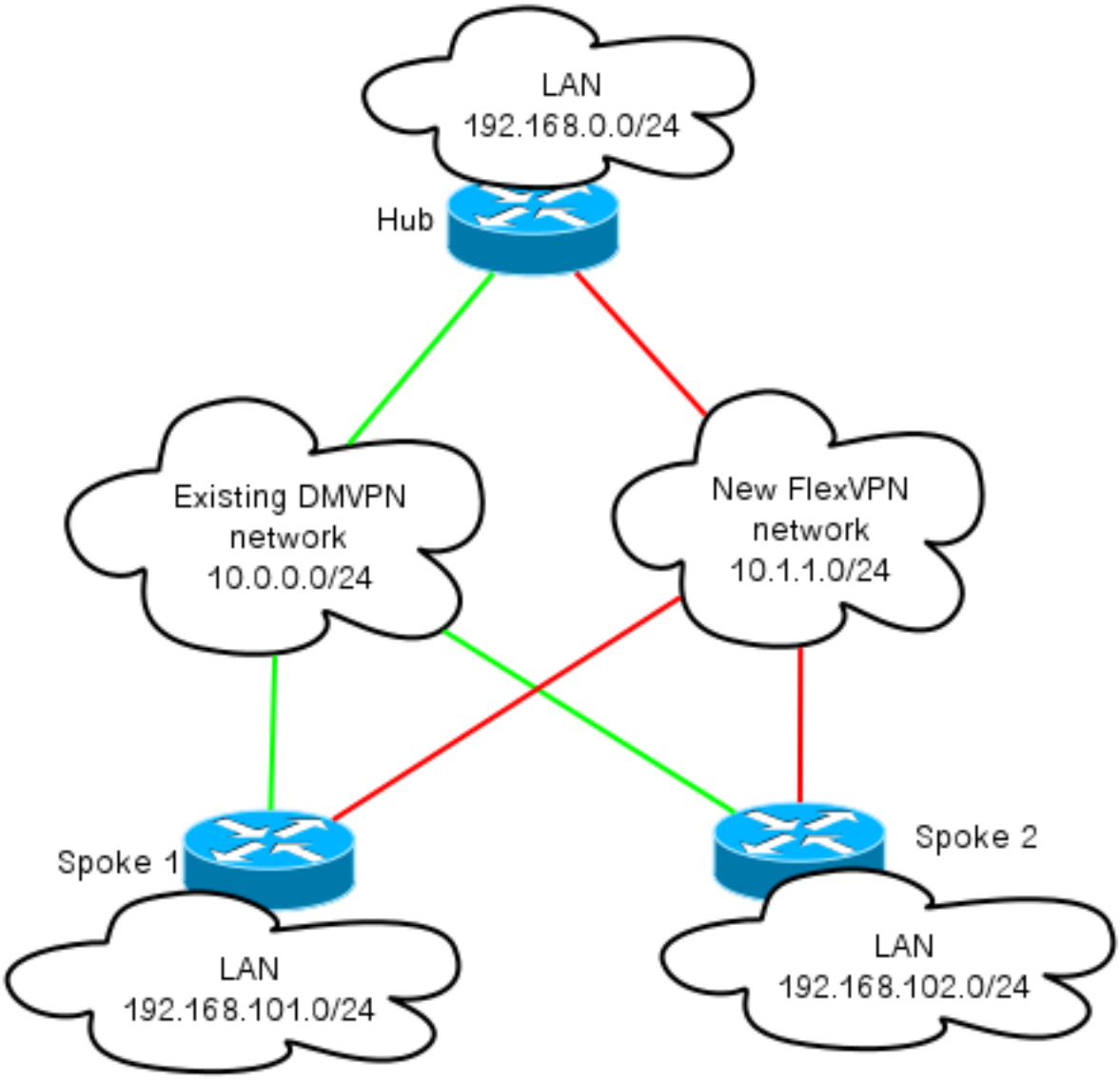


Diagramme de réseau superposé

Le réseau de superposition utilisé dans cet exemple comprend un seul concentrateur avec deux rayons connectés. N'oubliez pas que DMVPN et FlexVPN sont actifs simultanément, mais qu'ils utilisent des espaces d'adresses IP différents.



Configurations

Cette configuration migre le déploiement le plus répandu de DMVPN Phase 3 via le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) vers FlexVPN avec le protocole BGP (Border Gateway Protocol). Cisco recommande l'utilisation du protocole BGP avec FlexVPN, car il permet aux déploiements d'évoluer plus efficacement.

> **Note**: Le concentrateur termine les sessions IKEv1 (DMVPN) et IKEv2 (FlexVPN) sur la même adresse IP. Cela n'est possible qu'avec les versions récentes de Cisco IOS.

Configuration du rayon

Il s'agit d'une configuration très basique, avec deux exceptions notables qui permettent l'interopérabilité à la fois de IKEv1 et IKEv2, ainsi que deux cadres qui utilisent GRE (Generic Routing Encapsulation) sur IPsec pour le transport afin de coexister.

> **Note**: Les modifications pertinentes apportées à la configuration ISAKMP (Internet Security Association and Key Management Protocol) et IKEv2 sont mises en évidence en gras.

```
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
```

La version 15.3 de Cisco IOS vous permet de lier les profils IKEv2 et ISAKMP dans une configuration *de protection de tunnel*. En plus de certaines modifications internes du code, IKEv1 et IKEv2 peuvent fonctionner simultanément sur le même périphérique.

En raison de la manière dont Cisco IOS sélectionne les profils (IKEv1 ou IKEv2) dans les versions antérieures à 15.3, il a suscité certaines mises en garde, telles que les situations où IKEv1 est initié à IKEv2 par l'intermédiaire de l'homologue. La séparation d'IKE est désormais basée sur le niveau de profil et non sur le niveau d'interface, ce qui est réalisé via la nouvelle interface de ligne de commande.

Une autre mise à niveau de la nouvelle version de Cisco IOS est l'ajout de la *clé de tunnel*. Cela est nécessaire car DMVPN et FlexVPN utilisent la même interface source et la même adresse IP de destination. Une fois ce paramètre en place, le tunnel GRE n'a aucun moyen de savoir quelle interface de tunnel est utilisée pour décapsuler le trafic. La clé de tunnel vous permet de différencier **tunnel0** et **tunnel1** avec l'ajout d'une petite surcharge (4 octets). Une clé différente peut être configurée sur les deux interfaces, mais vous n'avez généralement besoin de différencier qu'un seul tunnel.

> **Note**: L'option de protection de tunnel partagé n'est pas requise lorsque DMVPN et FlexVPN partagent la même interface.

Ainsi, la configuration du protocole de routage en étoile est de base. EIGRP et BGP fonctionnent séparément. Le protocole EIGRP annonce uniquement sur l'interface de tunnel afin d'éviter d'appairer sur les tunnels de rayon à rayon, ce qui limite l'évolutivité. BGP maintient une relation uniquement avec le routeur concentrateur (**10.1.1.1**) afin d'annoncer le réseau local (**192.168.101.0/24**).

```
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
```

Configuration du concentrateur

Vous devez apporter des modifications similaires à celles décrites dans la section **Configuration satellite**.

> **Note**: Les modifications pertinentes apportées à la configuration ISAKMP et IKEV2 sont mises en évidence en gras.

```
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
```

Sur le côté concentrateur, la liaison entre le profil IKE et le profil IPsec se produit au niveau du profil, contrairement à la configuration en étoile, où ceci est effectué via la commande **de protection de tunnel**. Les deux approches sont des méthodes viables pour compléter cette liaison.

Il est important de noter que les ID réseau NHRP (Next Hop Resolution Protocol) sont différents pour DMVPN et FlexVPN dans le cloud. Dans la plupart des cas, il n'est pas souhaitable que le PNDH crée un domaine unique sur les deux cadres.

La clé de tunnel différencie les tunnels DMVPN et FlexVPN au niveau GRE afin d'atteindre le même objectif que celui mentionné dans la section **Configuration satellite**.

La configuration de routage sur le concentrateur est assez basique. Le périphérique concentrateur entretient deux relations avec un rayon donné, l'une utilisant le protocole EIGRP et l'autre utilisant le protocole BGP. La configuration BGP utilise la plage d'écoute afin d'éviter une configuration longue en étoile.

Les adresses récapitulatives sont introduites deux fois. La configuration EIGRP envoie un résumé avec l'utilisation de la configuration **tunnel0** (adresse de résumé IP EIGRP 100), et le BGP introduit un résumé avec l'utilisation de l'adresse d'agrégation. Les résumés sont nécessaires pour s'assurer que la redirection NHRP a lieu et pour simplifier les mises à jour de routage. Vous pouvez envoyer une redirection NHRP (tout comme une redirection ICMP (Internet Control Message Protocol)) qui indique s'il existe un meilleur saut pour une destination donnée, ce qui permet d'établir un tunnel de rayon à rayon. Ces résumés sont également utilisés afin de minimiser la quantité de mises à jour de routage envoyées entre le concentrateur et chaque rayon, ce qui permet aux configurations de mieux évoluer.

```
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
```

Vérification

La vérification de cet exemple de configuration est divisée en plusieurs sections.

Vérifications avant la migration

Puisque DMVPN/EIGRP et FlexVPN/BGP fonctionnent simultanément, vous devez vérifier que le rayon maintient une relation sur IPsec avec IKEv1 et IKEv2, et que les préfixes appropriés sont

appris sur EIGRP et BGP.

Dans cet exemple, **Spoke1** montre que deux sessions sont maintenues avec le routeur concentrateur ; l'un utilise IKEv1/**Tunnel0** et l'autre utilise IKEv2/**Tunnel1**.

> **Note**: Deux associations de sécurité IPsec (SA) (une entrante et une sortante) sont gérées pour chacun des tunnels.

```
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
```

Lorsque vous vérifiez les protocoles de routage, vous devez vérifier qu'un voisinage est formé et que les préfixes corrects sont appréhendés. Ceci est d'abord vérifié avec le protocole EIGRP. Vérifiez que le concentrateur est visible en tant que voisin et que l'adresse **192.168.0.0/16** (le résumé) est apprise à partir du concentrateur :

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

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
```

Ensuite, vérifiez le BGP :

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

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 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
```

Le résultat montre que l'adresse IP FlexVPN du concentrateur (**10.1.1.1**) est un voisin par lequel le rayon reçoit un préfixe (**192.168.0.0/16**). En outre, le BGP informe l'administrateur qu'une défaillance de la base d'informations de routage (RIB) s'est produite pour le préfixe **192.168.0.0/16**. Cet échec se produit car il existe déjà une meilleure route pour ce préfixe dans la table de routage. Cette route provient du protocole EIGRP et peut être confirmée si vous vérifiez la table de routage.

```
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:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
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
```

Migration

La section précédente a vérifié que les protocoles IPsec et de routage sont configurés et fonctionnent comme prévu. L'une des méthodes les plus simples pour migrer de DMVPN vers FlexVPN sur le même périphérique est de modifier la distance administrative (AD). Dans cet exemple, le BGP interne (iBGP) a une AD de **200** et le protocole EIGRP a une AD de **90**.

Pour que le trafic circule correctement dans FlexVPN, le BGP doit avoir une meilleure distance administrative. Dans cet exemple, la distance administrative EIGRP est remplacée par **230** et **240** pour les routes internes et externes, respectivement. Cela rend la BGP AD (de **200**) plus préférable pour le préfixe **192.168.0.0/16**.

Une autre méthode utilisée pour atteindre cet objectif est de diminuer la distance administrative BGP. Cependant, le protocole qui s'exécute après la migration a des valeurs non par défaut, qui peuvent affecter d'autres parties du déploiement.

Dans cet exemple, la commande **debug ip routing** est utilisée afin de vérifier le fonctionnement sur le rayon.

> **Note**: Si les informations de cette section sont utilisées sur un réseau de production, évitez l'utilisation des commandes debug et utilisez les commandes show répertoriées dans la section suivante. En outre, le processus EIGRP en étoile doit rétablir la contiguïté avec le

concentrateur.

```
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
```

Il y a trois actions importantes à remarquer dans ce résultat :

- Le rayon remarque que la distance administrative a changé et désactive la contiguïté.
- Dans la table de routage, le préfixe EIGRP est retiré et le protocole BGP est introduit.
- La contiguïté au concentrateur sur le protocole EIGRP revient en ligne.

Lorsque vous modifiez la distance administrative sur un périphérique, elle affecte uniquement le chemin du périphérique vers les autres réseaux ; elle n'affecte pas la façon dont les autres routeurs effectuent le routage. Par exemple, une fois que la distance EIGRP est augmentée sur Spoke1 (et qu'il utilise FlexVPN sur le cloud pour acheminer le trafic), le concentrateur conserve les AD configurées (par défaut). Cela signifie qu'il utilise DMVPN afin de router le trafic vers Spoke1.

Dans certains scénarios, cela peut causer des problèmes, par exemple lorsque les pare-feu s'attendent à recevoir du trafic de retour sur la même interface. Par conséquent, vous devez modifier la distance administrative sur tous les rayons avant de la modifier sur le concentrateur. Le trafic est entièrement migré par FlexVPN seulement une fois que ceci est terminé.

Migration EIGRP vers EIGRP

Une migration de DMVPN vers FlexVPN qui exécute uniquement le protocole EIGRP n'est pas abordée en détail dans ce document ; cependant, il est mentionné ici pour être complet.

Il est possible d'ajouter DMVPN et EIGRP à la même instance de routage du système autonome EIGRP. Une fois cette option en place, la contiguïté de routage est établie sur les deux types de nuages. Cela peut entraîner un équilibrage de charge, ce qui n'est généralement pas recommandé.

Afin de s'assurer que FlexVPN ou DMVPN est sélectionné, un administrateur peut attribuer différentes valeurs de **délai** par interface. Cependant, il est important de se rappeler qu'aucune modification n'est possible sur les interfaces de modèle virtuel alors que les interfaces d'accès

virtuel correspondantes sont présentes.

Contrôles post-migration

Tout comme le processus utilisé dans la section **Vérification préalable à la migration**, IPsec et le protocole de routage doivent être vérifiés.

Tout d'abord, vérifiez 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
```

Comme précédemment, deux sessions sont visibles, chacune ayant deux SA IPsec actives.

Sur le rayon, la route agrégée (**192.168.0.0/16**) pointe du concentrateur et est apprise sur 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:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

De même, le réseau local en étoile préfixé sur le concentrateur doit être connu via le protocole EIGRP. Dans cet exemple, le sous-réseau du réseau local **Spoke2** est coché :

```
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:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
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
```

Dans le résultat, le chemin de transfert est mis à jour correctement et pointe vers une interface d'accès virtuel.

Considérations supplémentaires

Cette section décrit certaines zones d'importance supplémentaires qui sont pertinentes pour cet exemple de configuration.

Tunnels Spoke-to-Spoke existants

Avec une migration du protocole EIGRP vers le protocole BGP, les tunnels de rayon à rayon ne sont pas affectés, car la commutation de raccourcis est toujours opérationnelle. La commutation par raccourci sur le rayon insère une route NHRP plus spécifique avec une distance administrative de 250.

Voici un exemple d'une telle route :

```
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:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

Communication entre les rayons migrés et non migrés

Si un rayon qui se trouve déjà sur un FlexVPN/BGP veut communiquer avec un périphérique pour lequel le processus de migration n'a pas commencé, le trafic passe toujours par le concentrateur.

Il s'agit du processus qui se produit :

1. Le rayon effectue une recherche de route pour la destination, qui pointe via une route récapitulative annoncée par le concentrateur.
2. Le paquet est envoyé vers le concentrateur.
3. Le concentrateur reçoit le paquet et effectue une recherche de route pour la destination, qui pointe vers une autre interface qui fait partie d'un domaine NHRP différent.

   Note: L'ID réseau NHRP dans la configuration précédente du concentrateur est différent pour FlexVPN et DMVPN.

Même si les ID réseau NHRP sont unifiés, un problème peut se produire lorsque le rayon migré achemine les objets sur le réseau FlexVPN. Ceci inclut la directive utilisée pour configurer la commutation de raccourcis. Le rayon non migré tente d'exécuter des objets sur le réseau DMVPN, avec un objectif spécifique pour effectuer la commutation de raccourcis.

Dépannage

Cette section décrit les deux catégories généralement utilisées pour résoudre les problèmes de migration.

Problèmes liés aux tentatives d'établissement de tunnels

Suivez ces étapes si la négociation IKE échoue :

1. Vérifiez l'état actuel à l'aide des commandes suivantes :

   show crypto isakmp sa - Cette commande indique la quantité, la source et la destination d'une session IKEv1.**show crypto ipsec sa** - Cette commande révèle l'activité des SA IPsec.**Note**: Contrairement à IKEv1, dans cette sortie, la valeur du groupe Diffie-Hellman (DH) de Perfect Forward Secrecy (PFS) apparaît comme **PFS (Y/N) : N, groupe DH : aucun** lors de la première négociation de tunnel ; toutefois, après une nouvelle clé, les valeurs correctes apparaissent. Ce n'est pas un bogue, même si le comportement est décrit dans CSCug67056. La différence entre IKEv1 et IKEv2 est que dans ce dernier cas, les SA enfant sont créées dans le cadre de l'échange **AUTH**. Le groupe DH qui est configuré sous la carte de chiffrement est utilisé uniquement lors d'une nouvelle clé. Pour cette raison, vous voyez **PFS (O/N) : N, groupe DH : aucun jusqu'à la première clé.** Avec IKEv1, vous voyez un comportement différent car la création de l'association de sécurité enfant se produit pendant le mode rapide, et le message **CREATE_CHILD_SA** contient des dispositions pour le transfert de la charge utile Key Exchange qui spécifie les paramètres DH afin de dériver un nouveau secret partagé.**show crypto ikev2 sa** - Cette commande fournit une sortie similaire à ISAKMP mais est spécifique à IKEv2.**show crypto session** - Cette commande fournit la sortie récapitulative des sessions cryptographiques sur ce périphérique.**show crypto socket** - Cette commande affiche l'état des sockets de chiffrement.**show crypto map** - Cette commande affiche le mappage des profils IKE et IPsec aux interfaces.**show ip nhrp** - Cette commande fournit les informations NHRP du périphérique. Ceci est utile pour les connexions de rayon à rayon dans les configurations FlexVPN, et pour les liaisons de rayon à rayon et de rayon à concentrateur dans les configurations DMVPN.
2. Utilisez ces commandes afin de déboguer l'établissement du tunnel :

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

Problèmes de propagation de route

Voici quelques commandes utiles que vous pouvez utiliser pour dépanner le protocole EIGRP et la topologie :

- **show bgp summary** - Utilisez cette commande afin de vérifier les voisins connectés et leur état.
- **show ip eigrp neighbor** - Utilisez cette commande afin d'afficher les voisins qui sont connectés via EIGRP.
- **show bgp** - Utilisez cette commande afin de vérifier les préfixes appris sur le BGP.
- **show ip eigrp topology** - Utilisez cette commande afin d'afficher les préfixes appris via EIGRP.

Il est important de savoir qu'un préfixe appris est différent d'un préfixe installé dans la table de routage. Pour plus d'informations à ce sujet, reportez-vous à l'article Sélection de route dans les routeurs Cisco ou à l'annuaire de presse Routing TCP/IP Cisco.

Caveats connus

Il existe une limitation similaire à la gestion de tunnel GRE sur l'ASR1K. Ceci est suivi sous l'ID de bogue Cisco CSCue00443. À ce stade, la limitation a une correction planifiée dans le logiciel Cisco IOS XE Version 3.12.

Surveillez ce bogue si vous désirez une notification une fois que la correction sera disponible.