DMVPN à l'exemple doux de configuration de transfert de FlexVPN

Contenu

Introduction

Ce document décrit comment exécuter un transfert *doux* où le VPN multipoint dynamique (DMVPN) et le FlexVPN travaillent à un périphérique simultanément sans besoin de contournement et fournit un exemple de configuration.

> **Note**: Ce document examine les concepts décrits dans le transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur les mêmes périphériques et transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur différents articles de Cisco d'un hub. Chacun des deux documents décrivent les transferts *durs*, qui font trafiquer une certaine interruption pendant le transfert. Les limites en ces articles sont dues à une insuffisance en logiciel de

Cisco IOS® qui est maintenant rectifié.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- DMVPN
- FlexVPN

Composants utilisés

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

- Versions 15.3(3)M ou ultérieures du routeur de service intégré de Cisco (ISR)
- La gamme Cisco 1000 a agrégé des versions 3.10 du routeur de service (ASR1K) ou plus tard

> **Note**: Non toute la version 2 (IKEv2) de logiciel et d'échange de clés Internet (IKE) de supports matériels. Référez-vous au navigateur de caractéristique de Cisco pour information.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Un des avantages de la plate-forme Cisco IOS et du logiciel plus nouveaux est la capacité d'utiliser le chiffrement de nouvelle génération. Un exemple est l'utilisation du Norme AES (Advanced Encryption Standard) en mode de Galois/compteur (GCM) pour le cryptage dans IPsec, comme évoqué dans RFC 4106. AES GCM laisse des vitesses beaucoup plus rapides de cryptage sur du matériel.

> **Note**: Pour des informations supplémentaires sur l'utilisation de et le transfert au chiffrement de nouvelle génération, référez-vous à l'article de Cisco de cryptage de nouvelle génération.

Configurez

Cet exemple de configuration se concentre sur un transfert d'une configuration de Phase 3

DMVPN à un FlexVPN, parce que les deux conceptions fonctionnent pareillement.

	Phase 2 DMVPN	Phase 3 DMVPN	FlexVPN
Transport	GRE au-dessus d'IPsec	GRE au-dessus d'IPsec	GRE au-dessus d'IP VTI
Utilisation de NHRP	Enregistrement et résolution	Enregistrement et résolution	Résolution
Prochain saut de rai	Les autres rais ou hub	Résumé de hub	Résumé de hub
Commutation raccourcie de NHRP	Non	Oui	Oui (facultatif)
Redirection de NHRP	Non	Oui	Oui
IKE et IPsec	IPsec facultatif, IKEv1 typique	IPsec facultatif, IKEv1 typique	IPsec, IKEv2

Diagrammes du réseau

Cette section fournit des schémas de réseau de transport et de recouvrement.

Schéma de réseau de transport

Le réseau de transport utilisé dans cet exemple inclut un hub simple avec deux rais connectés. Tous les périphériques sont connectés par un réseau qui simule l'Internet.

Schéma de réseau de recouvrement

Le réseau de substitution utilisé dans cet exemple inclut un hub simple avec deux rais connectés. Souvenez-vous que DMVPN et FlexVPN sont en activité simultanément, mais ils utilisent les différents espaces des adresses IP.

Configurations

Cette configuration migre le déploiement le plus populaire du Phase 3 DMVPN par l'intermédiaire du Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) vers FlexVPN avec le Protocole BGP (Border Gateway Protocol). Cisco recommande l'utilisation du BGP avec FlexVPN, parce qu'il permet à des déploiements de mesurer mieux.

> **Note**: Le hub termine les sessions IKEv1 (DMVPN) et IKEv2 (FlexVPN) sur la même adresse IP. C'est possible seulement avec les releases récentes de Cisco IOS.

Configuration du rayon

C'est très une configuration de base, à deux exceptions notables qui permettent l'interopérabilité d'IKEv1 et d'IKEv2, aussi bien que deux cadres qui emploient l'Encapsulation de routage générique (GRE) au-dessus d'IPsec pour le transport afin de coexister.

Note: Les modifications appropriées au Protocole ISAKMP (Internet Security Association and Key Management Protocol) et la configuration IKEv2 sont mises en valeur 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 Cisco IOS version 15.3 te permet pour attacher IKEv2 et profils d'ISAKMP ensemble dans une configuration de *tunnel protection*. Avec quelques modifications internes au code, ceci permet à IKEv1 et à IKEv2 pour traiter le même périphérique simultanément.

En raison de la manière le Cisco IOS sélectionne les profils (IKEv1 ou IKEv2) dans des releases plus tôt que 15.3, il ont mené à quelques mises en garde, telles que des situations où IKEv1 est initié à IKEv2 par le pair. La séparation de l'IKE est maintenant basée sur niveau du profil, non niveau de l'interface, qui est réalisé par l'intermédiaire du nouveau CLI.

Une autre mise à jour dans la nouvelle release de Cisco IOS est l'ajout du *tunnel key*. C'est nécessaire parce que les DMVPN et FlexVPN utilisent la même interface de source et la même adresse IP de destination. Avec ceci en place, il n'y a aucune manière pour que le tunnel GRE connaisse quelle interface de tunnel est utilisée afin de désencapsuler le trafic. Le tunnel key te permet pour différencier tunnel0 et tunnel1 en plus d'un petit (temps système d'octet 4). Une clé différente peut être configurée sur les deux interfaces, mais vous devez en général seulement différencier un tunnel.

> Note: L'option partagée de tunnel protection n'est pas exigée quand DMVPN et FlexVPN partagent la même interface.

Ainsi, la configuration de protocole de routage de rai est de base. L'EIGRP et le BGP fonctionnent séparément. L'EIGRP annonce seulement au-dessus de l'interface de tunnel afin d'éviter de scruter au-dessus des tunnels de spoke-to-spoke, qui limite l'évolutivité. Le BGP met à jour des relations seulement avec le routeur concentrateur (10.1.1.1) afin d'annoncer le réseau local (192.168.101.0/24).

```
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
```

Configuration du concentrateur

Vous devez apporter les modifications semblables sur la configuration de côté concentrateur en tant que ceux décrites dans la section de **configuration en étoile**.

> **Note**: Les changements appropriés à l'ISAKMP et à la configuration IKEV2 sont mis en valeur de gras.

```
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


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
```

Du côté concentrateur, l'attache entre le profil d'IKE et le profil IPSec se produit au niveau du profil, à la différence de la configuration en étoile, où ceci est terminé par l'intermédiaire de la commande de **tunnel protection**. Les deux approches sont des méthodes viables pour se terminer cette attache.

Il est important de noter que les id de réseau de Protocole NHRP (Next Hop Resolution Protocol) sont différents pour DMVPN et FlexVPN dans le nuage. Dans la plupart des cas, il est indésirable

quand le NHRP crée un domaine simple au-dessus des deux cadres.

Le tunnel key différencie DMVPN et tunnels de FlexVPN au niveau GRE afin d'atteindre le même but qui est mentionné dans la section de **configuration en étoile**.

La configuration de routage sur le hub est assez fondamentale. Le périphérique de hub met à jour deux relations avec des n'importe quels rai, qui utilisent l'EIGRP et donnés qui utilise le BGP. La configuration BGP emploie l'écouter-plage afin d'éviter un prolongé, configuration de par-rai.

Les adresses récapitulatives sont introduites deux fois. La configuration EIGRP envoie un résumé avec l'utilisation de la configuration **tunnel0** (ip summary-address eigrp 100), et le BGP introduit un résumé avec l'utilisation de l'aggregate-address. Les résumés sont exigés afin de s'assurer que la redirection de NHRP se produit, et afin de simplifier les mises à jour de routage. Vous pouvez envoyer un NHRP réorientez (tout comme un Protocole ICMP (Internet Control Message Protocol) réorientez) qui indique si un meilleur saut existe pour une destination donnée, qui permet un tunnel de spoke-to-spoke à établir. Ces résumés sont également utilisés afin de réduire la quantité de mises à jour de routage qui sont envoyées entre le hub et chaque rai, qui permet à des installations pour mesurer mieux.

```
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
```

Vérifiez

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

Contrôles de prémigration

Puisque DMVPN/EIGRP et FlexVPN/BGP fonctionnent simultanément, vous devez vérifier que le rai met à jour des relations au-dessus d'IPsec avec IKEv1 et IKEv2, et que les préfixes appropriés sont appris au-dessus de l'EIGRP et du BGP.

Dans cet exemple, **Spoke1** prouve que deux sessions sont mises à jour avec le routeur concentrateur ; on utilise IKEv1/Tunnel0 et on utilise IKEv2/Tunnel1.

> **Note**: Deux associations de sécurité IPSec (SAS) (une d'arrivée et une sortante) sont mises à jour 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
```

Quand vous vérifiez les protocoles de routage, vous devez vérifier qu'une proximité est formée, et que les préfixes corrects sont appris. Ceci est d'abord vérifié avec l'EIGRP. Vérifiez que le hub est visible en tant que voisin, et que l'adresse 192.168.0.0/16 (le résumé) est apprise du hub :

```
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
```

La sortie prouve que l'adresse IP de FlexVPN de hub (10.1.1.1) est un voisin par lequel le rai reçoit un préfixe (192.168.0.0/16). Supplémentaire, le BGP informe l'administrateur qu'une panne de Routing Information Base (NERVURE) s'est produite pour le préfixe 192.168.0.0/16. Cette panne se produit parce qu'il y a une meilleure artère pour ce préfixe qui existe déjà dans la table de routage. Cette artère est lancée par 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
```

Transfert

La section précédente a vérifié que l'IPsec et les protocoles de routage sont configurés et travail comme prévus. Un des moyens les plus simples de migrer de DMVPN vers FlexVPN sur le même périphérique est de changer la distance administrative (AD). Dans cet exemple, le BGP interne (iBGP) a un AD de 200, et l'EIGRP a un AD de 90.

Pour que le trafic traverse le FlexVPN correctement, le BGP doit avoir un meilleur AD. Dans cet exemple, l'AD EIGRP est changé à 230 et à 240 pour des routes internes et externes, respectivement. Ceci rend l'AD BGP (de 200) plus préférable pour le préfixe 192.168.0.0/16.

Une autre méthode qui est utilisée afin de réaliser ceci est de diminuer l'AD BGP. Cependant, le protocole qui fonctionne après que le transfert ait les valeurs autres que par défaut, qui peuvent affecter d'autres parties du déploiement.

Dans cet exemple, la commande de Routage IP de débogage est utilisée afin de vérifier l'exécution sur le rai.

> Note: Si les informations dans cette section sont utilisées sur un réseau de production, évitez l'utilisation des commandes de débogage, et comptez sur les commandes show répertoriées dans la section suivante. En outre, le processus du rai EIGRP doit rétablir la contiguïté avec le hub.

```
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

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
```

Il y a trois importantes actions de noter dans cette sortie :

- Le rai note que l'AD a changé, et désactive la contiguïté.
- Dans la table de routage, le préfixe EIGRP retied, et le BGP est introduit.
- La contiguïté au hub au-dessus de l'EIGRP revient en ligne.

Quand vous changez l'AD sur un périphérique, il affecte seulement le chemin du périphérique aux autres réseaux ; il n'affecte pas comment d'autres Routeurs exécutent le routage. Par exemple, après que la distance EIGRP soit augmentée là-dessus **Spoke1** (et emploie FlexVPN sur le nuage afin de conduire le trafic), le hub met à jour les annonces (par défaut) configurées. Ceci signifie qu'il emploie DMVPN afin de conduire le trafic de nouveau à **Spoke1**.

Dans certains scénarios, ceci peut poser des problèmes, comme quand les Pare-feu s'attendent au trafic de retour sur la même interface. Par conséquent, vous devriez changer l'AD sur tous les rais avant que vous le changiez sur le hub. Le trafic est entièrement migré par FlexVPN seulement une fois que c'est complet.

Transfert EIGRP-à-EIGRP

Un transfert de DMVPN à FlexVPN qui exécute seulement l'EIGRP n'est pas en profondeur discuté dans ce document ; cependant, on lui mentionne ici pour l'exhaustivité.

Il est possible d'ajouter DMVPN et EIGRP au même (AS) de système d'EIGRP autonome conduisant l'exemple. Avec ceci en place, la contiguïté de routage est établie au-dessus des deux types de nuages. Ceci peut faire produire l'Équilibrage de charge, qui n'est pas typiquement recommandé.

Afin de s'assurer que FlexVPN ou DMVPN est choisi, un administrateur peut assigner différentes valeurs de **retard** par interface. Cependant, il est important de se souvenir qu'aucune modification n'est possible sur les interfaces de modèle virtuel tandis que les interfaces d'accès virtuel correspondantes sont présentes.

Contrôles de post-transfert

Semblable au processus utilisé dans la section de **contrôles de prémigration**, l'IPsec et le protocole de routage doit être vérifié.

D'abord, vérifiez l'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 avant, deux sessions sont vues, qui ont deux l'active IPsec SAS.

Sur le rai, l'artère d'agrégat (**192.168.0.0/16**) se dirige du hub et est apprise au-dessus du 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 de rai qui est préfixé sur le hub doit être connu par l'intermédiaire de l'EIGRP. Dans cet exemple, le sous-réseau LAN **Spoke2** est vérifié :

```
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 la sortie, le chemin de transfert est mis à jour correctement et précise d'une interface d'accès virtuel.

Considérations supplémentaires

Cette section décrit quelques zones supplémentaires d'importance qui sont appropriées à cet exemple de configuration.

Tunnels existants de spoke-to-spoke

Avec un transfert d'EIGRP au BGP, les tunnels de spoke-to-spoke ne sont pas affectés, parce que la raccourci-commutation est encore en fonction. la Raccourci-commutation sur le rai insère une artère plus spécifique de NHRP avec un AD de 250.

Voici un exemple d'une telle artère :

```
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
```

Transmission entre les rais migrés et Non-migrés

Si un rai qui est déjà sur un FlexVPN/BGP veut communiquer avec un périphérique pour lequel le procédé de transfert n'a pas commencé, le trafic circule toujours sur le hub.

C'est le processus qui se produit :

1. Le rai effectue une recherche de route pour la destination, qui se dirige par une route récapitulative qui est annoncée par le hub.
2. Le paquet est envoyé vers le hub.
3. Le hub reçoit le paquet et effectue une recherche de route pour la destination, qui précise d'une autre interface qui fait partie d'un domaine différent de NHRP.

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

Même si les id de réseau de NHRP sont unifiés, un problème pourrait se poser où le rai migré conduit des objets au-dessus du réseau de FlexVPN. Ceci inclut la directive utilisée afin de configurer la commutation raccourcie. Les tentatives non-migrées de rai d'exécuter des objets au-dessus du réseau DMVPN, avec un but spécifique pour exécuter la commutation raccourcie.

Dépannez

Cette section décrit le toubleshoot typiquement utilisé de deux catégories le transfert.

Problèmes avec des tentatives d'établir des tunnels

Terminez-vous ces étapes si la négociation d'IKE échoue :

1. Vérifiez l'état actuel avec ces commandes :

   show crypto isakmp sa - Cette commande indique la quantité, la source, et la destination de session IKEv1.**l'exposition crypto** cette commande d'**ipsec SA** indique l'activité d'IPsec SAS.**Note**: À la différence de dans IKEv1, en cela sorti la valeur de groupe de Protocole DH (Diffie-Hellman) de perfect forward secrecy (PFS) apparaît comme **PFS (Y/N) : N, groupe CAD : aucun** pendant la première négociation de tunnel ; cependant, après qu'un rekey se produise, les valeurs correctes apparaissent. Ce n'est pas une bogue, quoique le comportement soit décrit dans CSCug67056. La différence entre IKEv1 et IKEv2 est celle dans ce dernier, l'enfant que SAS sont créées car une partie de l'échange **AUTHENTIQUE**. Le groupe CAD qui est configuré sous le crypto map est utilisé seulement pendant un rekey. Pour cette raison, vous voyez le **PFS (Y/N) : N, groupe CAD : aucun** jusqu'au premier rekey. Avec IKEv1, vous voyez un comportement différent parce que la création d'enfant SA se produit pendant le mode rapide, et le message **CREATE_CHILD_SA** prévoit le transfert de la charge utile de Key Exchange qui spécifie les paramètres CAD afin de dériver un nouveau secret partagé.**affichez cryptos ikev2 SA** - Cette commande fournit la sortie semblable à l'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 montre le statut de crypto-sockets.**crypto map d'exposition** - Cette commande montre le mappage de l'IKE et des profils IPSecs aux interfaces.**show ip nhrp** - Cette commande fournit les informations de NHRP du périphérique. C'est utile pour le spoke-to-spoke dans des installations de FlexVPN, et pour des attaches de spoke-to-spoke et de rai-à-hub dans des installations DMVPN.
2. Employez ces commandes afin de mettre au point l'établissement de tunnel :

   debug crypto ikev2debug crypto isakmpdebug crypto ipseckmi de **debug crypto**

Problèmes avec la propagation d'artère

Voici quelques commandes utiles que vous pouvez employer afin de dépanner l'EIGRP et la topologie :

- **show bgp summary** - Employez cette commande afin de vérifier les voisins connectés et leurs états.
- **voisin de show ip eigrp** - Employez cette commande afin d'afficher les voisins qui sont connectés par l'intermédiaire de l'EIGRP.
- **show bgp** - Employez cette commande afin de vérifier les préfixes appris au-dessus du BGP.
- **show ip eigrp topology** - Employez cette commande afin d'afficher les préfixes appris par l'intermédiaire de l'EIGRP.

Il est important de savoir qu'un préfixe instruit est différent qu'un préfixe qui est installé dans la table de routage. Pour plus d'informations sur ceci, mettez en référence la sélection de routes en article de Cisco de Routeurs de Cisco, ou le TCP/IP de acheminement Cisco appuient sur l'ouvrage.

Mises en garde connues

Une limite qui met en parallèle la manipulation de tunnel GRE existe sur l'ASR1K. Ceci est dépisté sous l'ID de bogue Cisco CSCue00443. À ce moment, la limite a une difficulté programmée dans la version 3.12 de Logiciel Cisco IOS XE version 2.

Surveillez cette bogue si vous désirez une notification une fois que la difficulté devient disponible.