Transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur un hub différent

Contenu

Introduction

Ce document fournit des informations au sujet de la façon migrer d'un réseau de VPN multipoint dynamique (DMVPN) qui existe actuellement à FlexVPN sur différents périphériques de hub. Les configuations pour les deux cadres coexistent sur les périphériques. Dans ce document, seulement le scénario le plus commun est affiché - DMVPN avec l'utilisation de la clé pré-partagée pour l'authentification et du Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) comme protocole de routage. Dans ce document, le transfert au Protocole BGP (Border Gateway Protocol), qui est le protocole de routage recommandé, et l'EIGRP moins-desirable est expliqué.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- DMVPN
- FlexVPN

Composants utilisés

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

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

- Version 15.2(4)M1 ou plus récentes du routeur de service intégré de Cisco (ISR)
- La gamme 1000 de routeur de services d'agrégation de Cisco (ASR1K) 3.6.2 libère 15.2(2)S2 ou plus nouveau

On les avantages d'une plus nouveaux plate-forme et logiciel est la capacité d'utiliser le chiffrement de nouvelle génération, tel que le Norme AES (Advanced Encryption Standard) Galois/mode de compteur (GCM) pour le cryptage dans l'IPSec (IPsec), comme évoqué dans le Request For Comments (RFC) 4106. AES GCM te permet pour atteindre une vitesse beaucoup plus rapide de cryptage sur du matériel. Afin de voir des recommandations de Cisco concernant l'utilisation de et le transfert au chiffrement de nouvelle génération, référez-vous à l'article de cryptage de nouvelle génération.

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.

Procédure de migration

Actuellement, la méthode recommandée à migrer de DMVPN vers FlexVPN est pour que les deux cadres ne fonctionnent pas en même temps. Cette limite est programmée pour devoir retiré de nouvelles caractéristiques de transfert être introduite dans la release ASR 3.10, dépistée sous les demandes d'amélioration de multilple du côté de Cisco, qui incluent l'ID de bogue Cisco CSCuc08066. Ces caractéristiques devraient être fin juin 2013 disponibles.

Un transfert où les deux cadres coexistent et fonctionnent en même temps sur les mêmes périphériques désigné sous le nom d'un **transfert doux**, qui indique l'incidence minimale et le Basculement sans heurt d'un cadre à l'autre. Un transfert où les configurations pour les deux cadres coexistent, mais ne fonctionnent pas en même temps désigné sous le nom d'un **transfert dur**. Ceci indique qu'un basculement d'un cadre à l'autre signifie un manque de transmission au-dessus du VPN, même si minimal.

Transfert dur entre deux Concentrateurs différents

Dans ce document, le transfert du hub DMVPN qui est actuellement utilisé à un nouveau hub de FlexVPN est discuté. Ce transfert permet l'intercommunication entre les rais migrés déjà vers FlexVPN, et ceux qui fonctionnent sur DMVPN et peuvent toujours être exécutés en plusieurs phases, sur le chaque ont parlé séparément.

Àcondition que les informations de routage soient correctement remplies, la transmission entre les rais migrés et nonmigrated devrait demeurer possible. Cependant, on peut observer la latence supplémentaire parce que migré et les rais nonmigrated ne construisent pas des tunnels de spoke-to-spoke entre l'un l'autre. En même temps, les rais migrés devraient pouvoir établir les tunnels directs de spoke-to-spoke entre eux-mêmes. Le même applique aux rais nonmigrated.

Jusqu'à ce que cette nouvelle caractéristique de transfert soit disponible, terminez-vous ces étapes afin d'exécuter des transferts avec un hub différent de DMVPN et de FlexVPN :

1. Vérifiez la Connectivité au-dessus de DMVPN.
2. Ajoutez la configuration de FlexVPN, et arrêtez le tunnel qui appartient à la nouvelle configuration.
3. (Pendant une fenêtre de maintenance) sur chaque rai, un, arrêtez le tunnel DMVPN.
4. Sur le même rai que dans l'étape 3, unshut les interfaces de tunnel de FlexVPN.
5. Vérifiez la Connectivité de rai-à-hub.
6. Vérifiez la Connectivité de spoke-to-spoke dans FlexVPN.
7. Vérifiez la Connectivité de spoke-to-spoke avec DMVPN de FlexVPN.
8. Répétez les étapes 3 à 7 pour le chaque a parlé séparément.
9. Si vous rencontrez n'importe quels problèmes avec les vérifications décrites dans les étapes 5, 6, ou 7, arrêtez l'interface de FlexVPN, et l'unshut les interfaces DMVPN afin de retourner à DMVPN.
10. Vérifiez la transmission de rai-à-hub au-dessus du DMVPN sauvegardé.
11. Vérifiez la transmission de spoke-to-spoke au-dessus du DMVPN sauvegardé.

Approche faite sur commande

Si l'approche précédente ne pourrait pas être la meilleure solution pour vous dû à vos complexités de réseau ou de routage, commencez une discussion avec votre représentant Cisco avant que vous migriez. La meilleure personne avec laquelle discuter un procédé fait sur commande de transfert est votre ingénieur système ou ingénieur de Services avancés.

Topologie du réseau

Topologie du réseau de transport

Ce diagramme affiche la topologie typique de connexion des hôtes sur l'Internet. L'adresse IP du hub de **loopback0** (**172.25.1.1**) est utilisée afin de terminer la session DMVPN IPsec. L'adresse IP sur le nouveau hub (**172.25.2.1**) est utilisée pour FlexVPN.

Notez le lien entre les deux Concentrateurs. Ce lien est crucial afin de permettre la Connectivité entre le FlexVPN et les nuages DMVPN pendant le transfert. Il permet des rais déjà migrés vers FlexVPN pour communiquer avec des réseaux DMVPN et vice versa.

Topologie du réseau de recouvrement

Ce diagramme de topologie affiche deux nuages distincts utilisés pour le recouvrement : DMVPN (connexions vertes) et FlexVPN (connexions rouges). Des préfixes de RÉSEAU LOCAL sont affichés pour les sites correspondants. Le sous-réseau **10.1.1.0/24** ne représente pas un sous-réseau réel en termes d'interface adressant, mais représente un bloc de l'espace IP dédié au nuage de FlexVPN. Le raisonnement derrière ceci est discuté plus tard dans la section de **configuration de FlexVPN**.

Configuration

Cette section décrit le DMVPN et les configurations de FlexVPN.

Configuration DMVPN

Cette section décrit la configuration de base pour le hub and spoke DMVPN.

La clé pré-partagée (PSK) est utilisée pour l'authentification IKEv1. Une fois qu'IPsec est établi, l'enregistrement de Protocole NHRP (Next Hop Resolution Protocol) du rai-à-hub est exécuté de sorte que le hub puisse apprendre l'adressage à plusieurs accès de Nonbroadcast des rais (NBMA) dynamiquement.

Quand le NHRP exécute l'enregistrement sur le rai et le hub, l'acheminement de l'adjacancy peut établir, et des artères peuvent être permutées. Dans cet exemple, l'EIGRP est utilisé comme protocole de routage de base pour le réseau de substitution.

Configuration du rai DMVPN

Voici que vous pouvez trouver un exemple de configuration de base de DMVPN avec l'authentification PSK et d'EIGRP comme protocole de routage.

```
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
```

Configuration du hub DMVPN

Dans la configuration de hub, le tunnel est originaire de **loopback0** avec une adresse IP de **172.25.1.1**. Le repos est un déploiement standard d'un hub DMVPN avec l'EIGRP comme protocole de routage.

```
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
```

Configuration de FlexVPN

FlexVPN est basé sur ces mêmes Technologies fondamentales :

- **IPsec** : À la différence du par défaut dans DMVPN, IKEv2 est utilisé au lieu d'IKEv1 afin de négocier les associations de sécurité IPSec (SAS). IKEv2 offre des améliorations au-dessus d'IKEv1, tel que la résilience et nombre de messages qui sont nécessaires afin d'établir une voie de transmission de données protégés.

- **GRE** : À la différence de DMVPN, des interfaces point par point statiques et dynamiques sont utilisées, et non seulement une interface statique du multpoint GRE. Cette configuration permet la flexibilité accrue, particulièrement pour le comportement de par-rai/par-hub.

- **NHRP** : Dans FlexVPN, le NHRP est principalement utilisé afin d'établir la transmission de spoke-to-spoke. Les rais ne s'enregistrent pas au hub.

- **Acheminement** : Puisque les rais n'exécutent pas l'enregistrement de NHRP au hub, vous devez compter sur d'autres mécanismes afin de s'assurer que le hub and spoke peut communiquer bidirectionnel. Simliar à DMVPN, des protocoles de routage dynamique peut être utilisé. Cependant, FlexVPN te permet pour employer IPsec afin d'introduire les informations de routage. Le par défaut est d'introduire comme artère de **/32** pour l'adresse IP de l'autre côté du tunnel, qui permet à rai-à-hub la transmission directe.

Dans un transfert dur de DMVPN à FlexVPN, les deux framemworks ne fonctionnent pas en même temps sur les mêmes périphériques. Cependant, il est recommandé pour les maintenir distincts.

Séparez-les à plusieurs niveaux :

- NHRP - Utilisez un (recommandé) différent d'ID de réseau de NHRP.
- Acheminement - (recommandé) distinct de processus de routage d'utilisation.
- Virtual Routing and Forwarding (VRF) - La séparation de VRF laisse a ajouté la flexibilité mais n'est pas discutée ici (facultatif).

Configuration de FlexVPN de rai

Une des différences en configuration en étoile dans FlexVPN par rapport à DMVPN est que vous avez potentiellement deux interfaces. Il y a un tunnel exigé pour la transmission de rai-à-hub et un tunnel facultatif pour des tunnels de spoke-to-spoke. Si vous choisissez de ne pas avoir le Tunnellisation dynamique de spoke-to-spoke et préféreriez que tout passe par le périphérique de hub, vous pouvez retirer l'interface de modèle virtuel, et enlevez la commutation raccourcie par NHRP de l'interface de tunnel.

Notez que l'interface de tunnel statique reçoit une adresse IP basée sur la négociation. Ceci permet au hub pour fournir l'adresse IP d'interface de tunnel au rai dynamiquement sans nécessité de créer l'adressage statique dans le nuage de FlexVPN.

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

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

> **Note**: Par défaut, l'identité locale est placée afin d'utiliser l'adresse IP. Ainsi la déclaration correspondante de correspondance sur le pair doit s'assortir basé sur l'adresse aussi bien. Si la condition requise est d'apparier basé sur le nom unique (DN) dans le certifcate, alors la correspondance doit être faite avec l'utilisation d'une carte de certificat.

Cisco recommande que vous utilisiez AES GCM avec le matériel qui le prend en charge.

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

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

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

interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
```

```
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

L'Infrastructure à clés publiques (PKI) est la méthode recommandée pour exécuter l'authentification de large échelle dans IKEv2. Cependant, vous pouvez encore utiliser PSK tant que vous vous rendez compte de ses limites.

Voici un exemple de configuration qui utilise **Cisco** comme 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
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Configuration de hub de FlexVPN

Typiquement, un hub termine seulement les tunnels dynamiques de rai-à-hub. C'est pourquoi vous ne trouvez pas une interface de tunnel statique pour FlexVPN dans la configuration de hub. Au lieu de cela, une interface de modèle virtuel est utilisée.

> **Note**: Du côté concentrateur, vous devez indiquer les adresses de groupe à assigner aux rais.

Des adresses de ce groupe sont ajoutées plus tard dans la table de routage comme artères de **/32** pour chaque rai.

```
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
```

Cisco recommande que vous utilisiez AES GCM avec le matériel qui le prend en charge.

```
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
```

Note: Dans cette configuration, l'exécution AES GCM a été commentée.

```
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
```

Avec l'authentification dans IKEv2, le même principe s'applique sur le hub comme sur le rai. Pour l'évolutivité et la flexibilité, Certificats d'utilisation. Cependant, vous pouvez réutiliser la même configuration pour PSK que sur le rai.

Note: IKEv2 offre la flexibilité en termes d'authentification. Un côté peut authentifier avec PSK tandis que l'autre côté utilise la signature de Rivest-Shamir-Adleman (RSA-SIG).

Si la condition requise est d'utiliser des clés pré-partagées pour l'authentification, alors les modifications de configuration sont semblables à ceux décrites pour le routeur en étoile ici.

Connexion BGP d'Inter-hub

Assurez-vous que les Concentrateurs savent où les préfixes particuliers se trouvent. Ceci devient de plus en plus important parce que quelques rais ont été migrés vers FlexVPN tandis que quelques autres rais restent sur DMVPN.

Voici la connexion BGP d'inter-hub basée sur la configuration de hub DMVPN :

```
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
```

Transfert du trafic

Migrez vers le BGP comme protocole de routage de recouvrement [recommandé]

Le BGP est un protocole de routage qui est basé sur l'échange d'unicast. En raison de ses caractéristiques, c'est le meilleur protocole d'évolution dans des réseaux DMVPN.

Dans cet exemple, BGP interne (iBGP) est utilisé.

Configuration BGP de rai

Le transfert de rai se compose de deux parts. D'abord, BGP d'enable comme routage dynamique :

```
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
```

Après que le voisin BGP monte (voient la section suivante) et de nouveaux préfixes au-dessus de BGP sont appris, vous pouvez balancer le trafic du nuage du courant DMVPN à un nouveau nuage de FlexVPN.

Configuration BGP de hub

Hub de FlexVPN - Pleine configuration BGP

Sur le hub, afin d'éviter de garder la configuration de proximité pour le chaque a parlé séparément, configurent les auditeurs dynamiques. Dans cette installation, le BGP n'initie pas de nouvelles connexions, mais reçoit des connexions du groupe fourni d'adresses IP. Dans ce cas, ledit groupe a **10.1.1.0/24 ans**, qui est toutes les adresses dans le nouveau nuage de FlexVPN.

Deux points à noter :

- Le hub de FlexVPN annonce des préfixes spécifiques au hub DMVPN ; ainsi la carte d'unsupress est utilisée.
- Annoncez le sous-réseau de FlexVPN de **10.1.1.0/24 à la** table de routage, ou assurez-vous

que le hub DMVPN voit le hub de FlexVPN comme prochain saut.

Ce document affiche la dernière approche.

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

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

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

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

Hub DMVPN - Pleine configuration BGP et EIGRP

La configuration sur le hub DMVPN est de base, parce qu'elle reçoit seulement des préfixes spécifiques du hub de FlexVPN et annonce des préfixes qu'il apprend de l'EIGRP.

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

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

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

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

Migrez le trafic vers BGP/FlexVPN

Comme discuté avant, vous devez arrêter la fonctionnalité DMVPN et apporter FlexVPN afin d'exécuter le transfert.

Cette procédure garantit l'incidence minimale :

1. Sur chaque rai, séparément, entrez dans ceci :

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

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

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

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

En ce moment, assurez-vous qu'il n'y a aucune session IKEv1 établie à ce rai. Ceci peut être vérifié si vous vérifiez la sortie des messages de Syslog de commande et de moniteur de **show crypto isakmp sa** générés par la commande de **session de crypto logging**. Une fois que ceci est confirmé, vous pouvez poursuivre pour apporter FlexVPN.

2. Sur le même rai, entrez dans ceci :

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

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

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

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

Étapes de vérification

Stabilité d'IPsec

La meilleure manière d'évaluer la stabilité d'IPsec est de surveiller des sylogs avec la commande enabled de configuration de **session de crypto logging**. Si vous voyez les sessions qui vont en haut et en bas, ceci peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que le transfert puisse commencer.

Les informations BGP remplies

Si IPsec est stable, assurez-vous que la table BGP est remplie avec des entrées des rais (sur le hub) et de résumé du hub (sur les rais). Dans le cas du BGP, ceci peut être visualisé avec ces commandes :

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

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

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

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

Voici un exemple des informations correctes du hub de FlexVPN :

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

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

La sortie prouve que le hub a appris un préfixe de chacun des rais, et les deux rais sont dynamiques et marqués avec un signe d'astérisque (*). Il prouve également qu'un total de quatre préfixes de la connexion d'inter-hub est reçus.

Voici un exemple des informations semblables du rai :

```
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
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Le rai a reçu deux préfixes du hub. Dans le cas de cette installation, un préfixe devrait être le résumé annoncé sur le hub de FlexVPN. L'autre est réseau DMVPN **10.0.0.0/24** redistribué sur le rai DMVPN dans le BGP.

Migrez vers de nouveaux tunnels avec l'EIGRP

L'EIGRP est un choix populaire dans des réseaux DMVPN dus à son déploiement et convergence rapide relativement simples. Cependant, il mesure plus mauvais que le BGP, et n'offre pas beaucoup de mécanismes avancés qui peuvent être utilisés par BGP directement hors de la case. La section suivante décrit une des manières de se déplacer à FlexVPN avec un nouveau

processus EIGRP.

Configuration en étoile mise à jour

Un nouveau système autonome (AS) est ajouté avec un processus distinct EIGRP :

```
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
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

> **Note**: Il est le meilleur de ne pas établir la contiguïté de protocole de routage au-dessus des tunnels de spoke-to-spoke. Par conséquent, rendez seulement l'interface de **tunnel1** (rai-à-hub) non passive.

Configuration mise à jour de hub de FlexVPN

De même, pour le hub de FlexVPN, préparez le protocole de routage dans l'appopriate COMME, en appariant un configuré sur les rais.

```
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
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Il y a deux méthodes qui sont utilisées afin de fournir le dos de résumé vers le rai.

- Redistribuez une artère statique qui indique **null0** (option préférée).

  ```
  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
  10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
  ```

  Cette option permet le contrôle du résumé et la redistribution sans modifications à la configuration de la technologie de la virtualisation du hub (VT). C'est important, parce que la configuration VT du hub ne peut pas être modifiée s'il y a d'accès virtuel actif associé avec lui.

- Installez une adresse récapitulative de style DMVPN sur un modèle virtuel.

  Cette configuration *n'est pas recommandée*, en raison du traitement interne et de la réplication de ledit résumé à chaque accès virtuel. On lui affiche ici pour la référence.

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

Un autre aspect à expliquer est l'échange de routage d'inter-hub. Ceci peut être fait si vous redistribuez des exemples EIGRP à l'iBGP.

Hub DMVPN - Configuration BGP mise à jour

La configuration demeure de base. Vous devez redistribuer des préfixes spécifiques d'EIGRP au BGP :

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

Hub de FlexVPN - Configuration BGP mise à jour

Semblable au hub DMVPN, dans FlexVPN, vous devez redistribuer des nouveaux les préfixes processus EIGRP au BGP :

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

Migrez le trafic vers FlexVPN

Vous devez arrêter la fonctionnalité DMVPN et apporter FlexVPN sur chaque rai, un par un, afin d'exécuter le transfert. Cette procédure garantit l'incidence minimum :

1. Sur chaque rai, séparément, entrez dans ceci :

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

   En ce moment, assurez-vous qu'il n'y a aucune session IKEv1 établie sur ce rai. Ceci peut être vérifié si vous vérifiez la sortie des messages de Syslog de commande et de moniteur de **show crypto isakmp sa** générés par la commande de **session de crypto logging**. Une fois que ceci est confirmé, vous pouvez poursuivre pour apporter FlexVPN.
2. Sur le même rai, entrez dans ceci :

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

Étapes de vérification

Stabilité d'IPsec

Comme dans le cas du BGP, vous devez évaluer si IPsec est stable. La meilleure manière de

faire ainsi est de surveiller des sylogs avec la commande enabled de configuration de **session de crypto logging**. Si vous voyez des sessions aller en haut et en bas, ceci peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que le transfert puisse commencer.

Les informations EIGRP dans la table de topologie

Assurez-vous que votre table de topologie EIGRP est remplie avec des entrées de RÉSEAU LOCAL de rai sur le hub et le résumé sur les rais. Ceci peut être vérifié si vous sélectionnez cette commande sur les hub et les rais :

show ip eigrp [AS_NUMBER] topology

Voici un exemple de sortie du rai :

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

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

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

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

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

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

La sortie prouve que le rai sait son sous-réseau LAN (en *italique*) et les résumés pour ceux (en **gras**).

Voici un exemple de sortie du hub :

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

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

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

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

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

La sortie prouve que le hub sait les sous-réseaux LAN des rais (en *italique*), le préfixe récapitulatif

qu'il annonce (en **gras**), et l'adresse IP assignée de chaque rai par l'intermédiaire de la négociation.

Considérations supplémentaires

Tunnels de spoke-to-spoke qui existent déjà

Puisqu'un arrêt de l'interface de tunnel DMVPN cause des entrées de NHRP d'être retirées, des tunnels de spoke-to-spoke qui existent déjà seront démolis.

Effacez les entrées de NHRP

Un hub de FlexVPN ne se fonde pas sur la procédure d'enregistrement de NHRP du rai afin de savoir conduire le trafic de retour. Cependant, les tunnels dynamiques de spoke-to-spoke se fondent sur des entrées de NHRP.

Dans DMVPN, si le NHRP sur le hub est effacé, il peut avoir comme conséquence des problèmes de courte durée de Connectivité. Dans FlexVPN, le NHRP effaçant sur les rais entraînera la session de FlexVPN IPsec, liée aux tunnels de spoke-to-spoke, pour être démoli. Effacer le NHRP sur le hub n'exerce aucun effet sur la session de FlexVPN.

C'est parce que, dans FlexVPN par défaut :

- Les rais ne s'enregistrent pas aux Concentrateurs.
- Les Concentrateurs fonctionnent seulement comme redirections de NHRP, et n'installent pas des entrées de NHRP.
- Des entrées raccourcies de NHRP sont installées sur des rais pour des tunnels de spoke-to-spoke et sont dynamiques.

Mises en garde connues

Le trafic de spoke-to-spoke pourrait être affecté par l'ID de bogue Cisco CSCub07382.

Informations connexes

- DMVPN à l'exemple doux de configuration de transfert de FlexVPN
- Support et documentation techniques - Cisco Systems