Migration de DurMove de DMVPN vers FlexVPN sur un autre concentrateur

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Procédure de migration
Migration Dure Entre Deux Concentrateurs Différents
Approche personnalisée
Topologie du réseau
Topologie du réseau de transport
Topologie de réseau de superposition
Configuration
Configuration DMVPN
Configuration DMVPN satellite
Configuration DMVPN du concentrateur
Configuration FlexVPN
Configuration de Spoke FlexVPN
Configuration du concentrateur FlexVPN
Migration du trafic
Migrer vers BGP en tant que protocole de routage de superposition [recommandé]
Configuration BGP satellite
Configuration du concentrateur BGP
Migration du trafic vers BGP/FlexVPN
Migrer vers de nouveaux tunnels avec EIGRP
Configuration de satellite mise à jour
Configuration du concentrateur FlexVPN mise à jour
Concentrateur DMVPN - Configuration BGP mise à jour
Concentrateur FlexVPN - Configuration BGP mise à jour
Migration du trafic vers FlexVPN
Étapes de vérification
Considérations supplémentaires
Tunnels Spoke-to-Spoke qui existent déjà
Effacer les entrées NHRP
Caveats connus
Informations connexes

Introduction

Ce document fournit des informations sur la migration d'un réseau DMVPN (Dynamic Multipoint VPN) qui existe actuellement vers FlexVPN sur différents concentrateurs. Les configurations des deux cadres coexistent sur les périphériques. Dans ce document, seul le scénario le plus courant est présenté : DMVPN avec l'utilisation de la clé pré-partagée pour l'authentification et EIGRP (Enhanced Interior Gateway Routing Protocol) comme protocole de routage. Dans ce document, la migration vers le protocole BGP (Border Gateway Protocol), qui est le protocole de routage recommandé, et le protocole EIGRP moins souhaitable est démontré.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseaux RPV multipoint dynamique (DMVPN)
- FlexVPN

Components Used

> **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.

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

- Routeur à services intégrés Cisco (ISR) version 15.2(4)M1 ou ultérieure
- Routeur de services d'agrégation Cisco série 1000 (ASR1K) 3.6.2 version 15.2(2)S2 ou ultérieure

L'un des avantages d'une plate-forme et d'un logiciel plus récents est la possibilité d'utiliser la cryptographie de nouvelle génération, telle que la norme AES (Advanced Encryption Standard) Galois/Counter Mode (GCM) pour le cryptage dans IPsec (Internet Protocol Security), comme indiqué dans la demande de commentaires (RFC) 4106. AES GCM vous permet d'atteindre une vitesse de cryptage beaucoup plus rapide sur certains matériels. Afin de voir les recommandations de Cisco sur l'utilisation et la migration vers la cryptographie de nouvelle génération, référez-vous à l'article de chiffrement de nouvelle génération.

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.

Procédure de migration

Actuellement, la méthode recommandée pour migrer de DMVPN vers FlexVPN est que les deux cadres ne fonctionnent pas simultanément. Cette limitation doit être supprimée en raison des nouvelles fonctionnalités de migration qui seront introduites dans la version ASR 3.10, suivie sous plusieurs demandes d'amélioration côté Cisco, qui incluent l'ID de bogue Cisco CSCuc08066. Ces fonctionnalités devraient être disponibles fin juin 2013.

Une migration où les deux cadres coexistent et fonctionnent simultanément sur les mêmes périphériques est appelée **migration logicielle**, ce qui indique l'impact minimal et le basculement fluide d'un cadre à l'autre. Une migration dans laquelle les configurations des deux cadres coexistent, mais ne fonctionnent pas en même temps, est appelée **migration dure**. Cela indique qu'un basculement d'un cadre à un autre signifie un manque de communication sur le VPN, même si cela est minime.

Migration Dure Entre Deux Concentrateurs Différents

Dans ce document, la migration du concentrateur DMVPN actuellement utilisé vers un nouveau concentrateur FlexVPN est abordée. Cette migration permet l'intercommunication entre les rayons déjà migrés vers FlexVPN et ceux qui fonctionnent encore sur DMVPN et peuvent être effectués en plusieurs phases, sur chaque rayon séparément.

Si les informations de routage sont correctement renseignées, la communication entre les rayons migrés et non migrés doit rester possible. Cependant, une latence supplémentaire peut être observée car les rayons migrés et non migrés ne construisent pas de tunnels de rayon à rayon entre eux. Dans le même temps, les rayons migrés devraient être en mesure d'établir des tunnels de rayon à rayon directs entre eux. Il en va de même pour les rayons non migrés.

Jusqu'à ce que cette nouvelle fonctionnalité de migration soit disponible, complétez ces étapes afin d'effectuer des migrations avec un concentrateur différent de DMVPN et FlexVPN :

1. Vérifiez la connectivité sur DMVPN.
2. Ajoutez la configuration FlexVPN et arrêtez le tunnel qui appartient à la nouvelle configuration.
3. (Pendant une fenêtre de maintenance) Sur chaque rayon, un par un, arrêtez le tunnel DMVPN.
4. Sur le même rayon que l'étape 3, désactivez les interfaces de tunnel FlexVPN.
5. vérification de la connectivité de satellite à concentrateur
6. Vérifiez la connectivité de rayon à rayon dans FlexVPN.
7. Vérifiez la connectivité de satellite à satellite avec DMVPN à partir de FlexVPN.
8. Répétez les étapes 3 à 7 pour chaque rayon séparément.
9. Si vous rencontrez des problèmes avec les vérifications décrites aux étapes 5, 6 ou 7, arrêtez l'interface FlexVPN et désactivez les interfaces DMVPN afin de revenir à DMVPN.
10. Vérifiez la communication de rayon à concentrateur sur le DMVPN sauvegardé.
11. Vérifiez la communication de rayon à rayon sur le DMVPN sauvegardé.

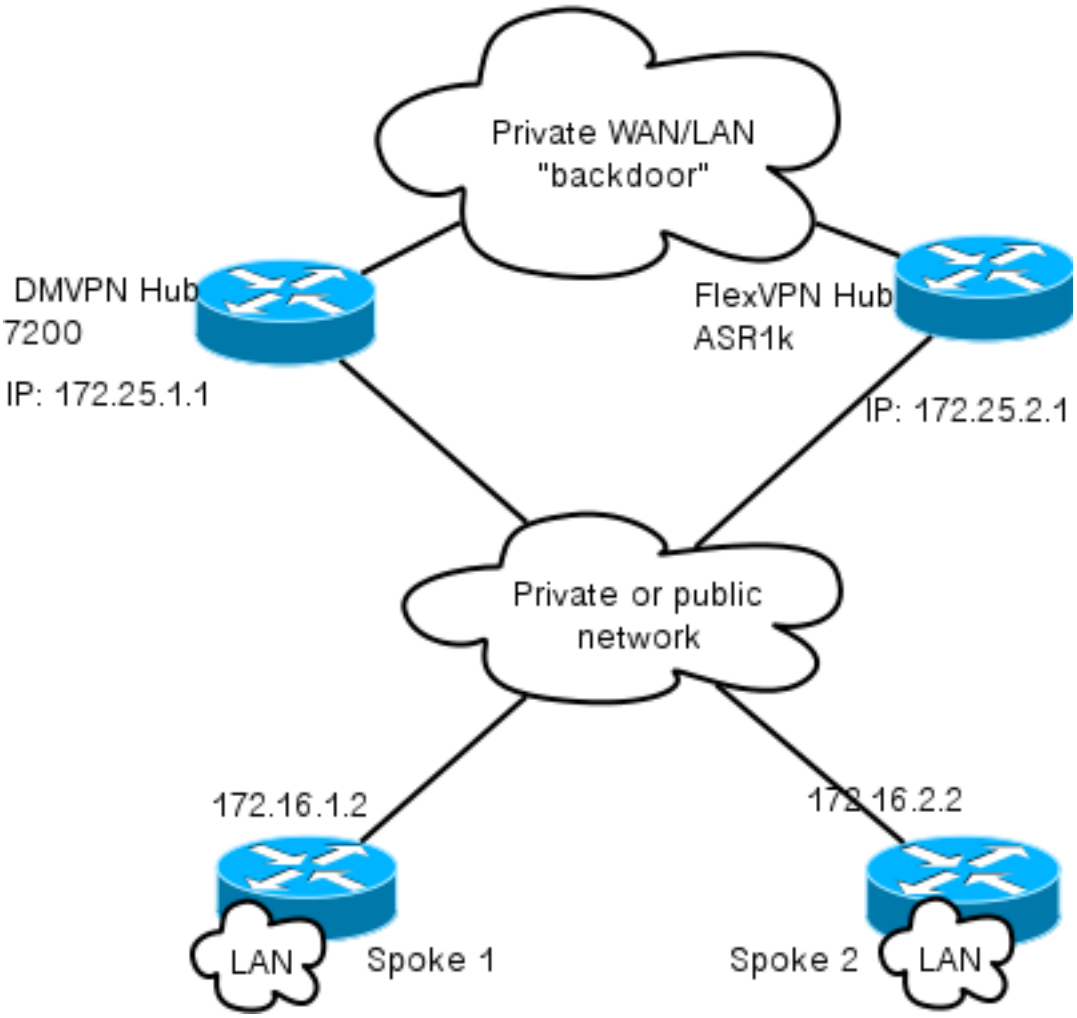
Approche personnalisée

Si l'approche précédente n'est peut-être pas la meilleure solution pour vous en raison de la complexité de votre réseau ou de votre routage, commencez une discussion avec votre représentant Cisco avant de migrer. La meilleure personne avec laquelle discuter d'un processus de migration personnalisé est votre ingénieur système ou votre ingénieur des services avancés.

Topologie du réseau

Topologie du réseau de transport

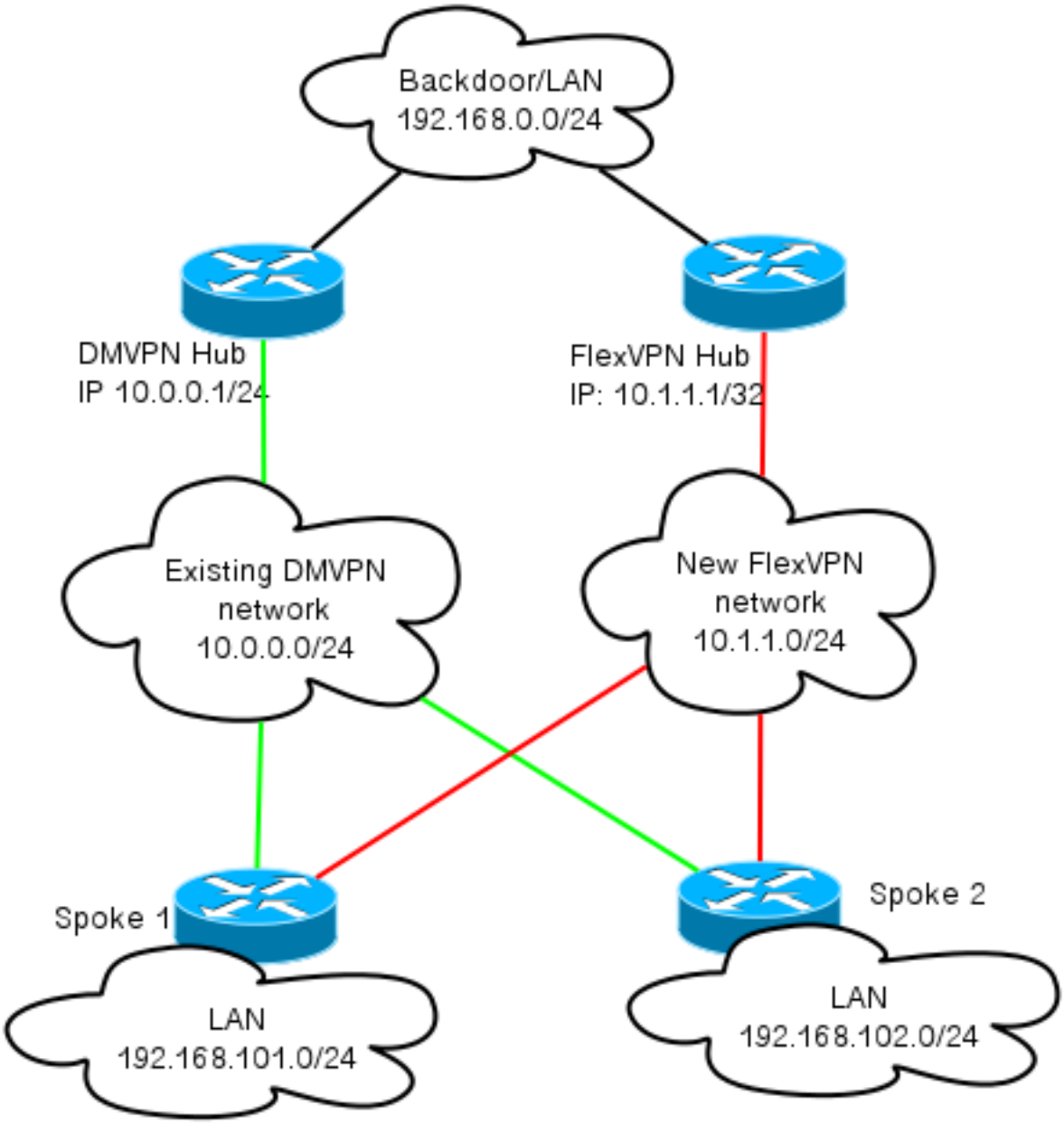
Ce schéma présente la topologie de connexion type des hôtes sur Internet. L'adresse IP du concentrateur **loopback0** (**172.25.1.1**) est utilisée afin de mettre fin à la session IPsec DMVPN. L'adresse IP du nouveau concentrateur (**172.25.2.1**) est utilisée pour FlexVPN.



Notez la liaison entre les deux concentrateurs. Cette liaison est essentielle pour permettre la connectivité entre les clouds FlexVPN et DMVPN pendant la migration. Il permet aux rayons déjà migrés vers FlexVPN de communiquer avec les réseaux DMVPN et vice versa.

Topologie de réseau de superposition

Ce schéma de topologie présente deux nuages distincts utilisés pour la superposition : DMVPN (connexions vertes) et FlexVPN (connexions rouges). Les préfixes LAN sont affichés pour les sites correspondants. Le sous-réseau **10.1.1.0/24** ne représente pas un sous-réseau réel en termes d'adressage d'interface, mais représente une partie de l'espace IP dédié au cloud FlexVPN. La raison d'être de ce problème est traitée plus loin dans la section **Configuration FlexVPN**.



Configuration

Cette section décrit les configurations DMVPN et FlexVPN.

Configuration DMVPN

Cette section décrit la configuration de base du concentrateur et du rayon DMVPN.

La clé prépartagée (PSK) est utilisée pour l'authentification IKEv1. Une fois IPsec établi, l'enregistrement NHRP (Next Hop Resolution Protocol) de rayon à concentrateur est effectué afin que le concentrateur puisse apprendre l'adressage NBMA (Nonbroadcast Multiaccess) des rayons de manière dynamique.

Lorsque NHRP effectue l'enregistrement sur le rayon et le concentrateur, la contiguïté de routage peut s'établir et les routes peuvent être échangées. Dans cet exemple, le protocole EIGRP est utilisé comme protocole de routage de base pour le réseau de superposition.

Configuration DMVPN satellite

Vous trouverez ici un exemple de configuration de base de DMVPN avec authentification PSK et 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 DMVPN du concentrateur

Dans la configuration du concentrateur, le tunnel provient de **loopback0** avec l'adresse IP **172.25.1.1**. Le reste est un déploiement standard d'un concentrateur DMVPN avec 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 FlexVPN

FlexVPN repose sur les mêmes technologies fondamentales :

- **IPSEC :** Contrairement à la valeur par défaut dans DMVPN, IKEv2 est utilisé à la place d'IKEv1 afin de négocier les associations de sécurité (SA) IPsec. IKEv2 offre des améliorations par rapport à IKEv1, telles que la résilience et le nombre de messages nécessaires pour établir un canal de données protégé.

- **GRE:** Contrairement au DMVPN, les interfaces point à point statiques et dynamiques sont utilisées, et pas seulement une interface GRE multipoint statique. Cette configuration permet une plus grande flexibilité, en particulier pour le comportement par rayon/par concentrateur.

- **NHRP** : Dans FlexVPN, NHRP est principalement utilisé pour établir une communication de rayon à rayon. Les rayons ne s'inscrivent pas au concentrateur.

- **Routage** : Comme les rayons n'effectuent pas d'enregistrement NHRP vers le concentrateur, vous devez utiliser d'autres mécanismes pour vous assurer que le concentrateur et les rayons peuvent communiquer bidirectionnellement. Des protocoles de routage dynamique similaires à DMVPN peuvent être utilisés. Cependant, FlexVPN vous permet d'utiliser IPsec afin d'introduire des informations de routage. La valeur par défaut est d'introduire en tant que route **/32** pour l'adresse IP de l'autre côté du tunnel, ce qui permet une communication directe de rayon à concentrateur.

Dans une migration dure de DMVPN vers FlexVPN, les deux cadres ne fonctionnent pas simultanément sur les mêmes périphériques. Il est toutefois recommandé de les séparer.

Séparez-les sur plusieurs niveaux :

- NHRP : utilisez un ID réseau NHRP différent (recommandé).
- Routage : utilisez des processus de routage distincts (recommandé).
- Routage et transfert virtuels (VRF) : la séparation VRF permet une plus grande flexibilité, mais n'est pas abordée ici (facultatif).

Configuration de Spoke FlexVPN

Une des différences de configuration en étoile dans FlexVPN par rapport au DMVPN est que vous avez potentiellement deux interfaces. Il existe un tunnel requis pour la communication entre les rayons et les concentrateurs et un tunnel facultatif pour les tunnels entre les rayons. Si vous choisissez de ne pas avoir de tunnellisation dynamique de rayon à rayon et préférez que tout passe par le périphérique concentrateur, vous pouvez supprimer l'interface de modèle virtuel et supprimer la commutation de raccourcis NHRP de l'interface de tunnel.

Notez que l'interface de tunnel statique reçoit une adresse IP basée sur la négociation. Cela permet au concentrateur de fournir l'adresse IP de l'interface de tunnel au rayon de manière dynamique sans avoir à créer d'adressage statique dans le cloud 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 définie afin d'utiliser l'adresse IP. Ainsi, l'instruction de correspondance correspondante sur l'homologue doit également correspondre en fonction de l'adresse. Si la condition requise doit correspondre en fonction du nom distinctif (DN) dans le certificat, la correspondance doit être effectuée à l'aide d'une carte de certificat.

Cisco vous recommande d'utiliser AES GCM avec du 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
```

Public Key Infrastructure (PKI) est la méthode recommandée pour effectuer une authentification à grande échelle dans IKEv2. Cependant, vous pouvez toujours utiliser PSK tant que vous connaissez 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 du concentrateur FlexVPN

En règle générale, un concentrateur ne termine que les tunnels de rayon à concentrateur dynamiques. C'est pourquoi vous ne trouvez pas d'interface de tunnel statique pour FlexVPN dans la configuration du concentrateur. À la place, une interface de modèle virtuel est utilisée.

> **Note**: Du côté concentrateur, vous devez indiquer les adresses de pool à attribuer aux rayons.

Les adresses de ce pool sont ajoutées ultérieurement dans la table de routage en tant que routes **/32** pour chaque rayon.

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

crypto ikev2 authorization policy default
pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn hub.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
```

Cisco vous recommande d'utiliser AES GCM avec du matériel qui le prend en charge.

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

> **Note**: Dans cette configuration, l'opération AES GCM a été commentée.

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

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
interface Loopback100
ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip nhrp network-id 2
ip nhrp redirect
tunnel path-mtu-discovery
tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Avec l'authentification dans IKEv2, le même principe s'applique au concentrateur que sur le rayon. Pour des raisons d'évolutivité et de flexibilité, utilisez des certificats. Cependant, vous pouvez réutiliser la même configuration pour PSK que sur le rayon.

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

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

Connexion BGP entre concentrateurs

Assurez-vous que les concentrateurs savent où se trouvent les préfixes spécifiques. Cela devient de plus en plus important car certains rayons ont été transférés vers FlexVPN alors que d'autres rayons restent sur DMVPN.

Voici la connexion BGP inter-concentrateur basée sur la configuration du concentrateur DMVPN :

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

Migration du trafic

Migrer vers BGP en tant que protocole de routage de superposition [recommandé]

Le protocole BGP est un protocole de routage basé sur l'échange de monodiffusion. En raison de ses caractéristiques, il s'agit du meilleur protocole d'évolutivité dans les réseaux DMVPN.

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

Configuration BGP satellite

La migration des rayons se compose de deux parties. Tout d'abord, activez BGP en tant que routage dynamique :

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

Une fois que le voisin BGP est activé (voir la section suivante) et que de nouveaux préfixes sur BGP sont appris, vous pouvez faire passer le trafic du cloud DMVPN actuel à un nouveau cloud FlexVPN.

Configuration du concentrateur BGP

Concentrateur FlexVPN - Configuration BGP complète

Sur le concentrateur, afin d'éviter de conserver séparément la configuration de voisinage pour chaque rayon, configurez des écouteurs dynamiques. Dans cette configuration, BGP n'initie pas de nouvelles connexions, mais accepte les connexions à partir du pool d'adresses IP fourni. Dans ce cas, ce pool est **10.1.1.0/24**, qui correspond à toutes les adresses du nouveau cloud FlexVPN.

Deux points à noter :

- Le concentrateur FlexVPN annonce des préfixes spécifiques au concentrateur DMVPN ; la carte unsupress est donc utilisée.
- Annoncez le sous-réseau FlexVPN de **10.1.1.0/24** à la table de routage, ou assurez-vous que le concentrateur DMVPN voit le concentrateur FlexVPN comme tronçon suivant.

Ce document montre cette 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
```

Concentrateur DMVPN - Configuration BGP et EIGRP complète

La configuration sur le concentrateur DMVPN est de base, car il reçoit uniquement des préfixes spécifiques du concentrateur FlexVPN et annonce les préfixes qu'il apprend du protocole EIGRP.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

Migration du trafic vers BGP/FlexVPN

Comme indiqué précédemment, vous devez arrêter la fonctionnalité DMVPN et activer FlexVPN pour effectuer la migration.

Cette procédure garantit un impact minimal :

1. Sur chaque rayon, entrez ceci séparément :

   ```
   interface tunnel 0
    shut
   ```

   À ce stade, assurez-vous qu'aucune session IKEv1 n'est établie pour ce discours. Ceci peut être vérifié si vous vérifiez le résultat de la commande **show crypto isakmp sa** et surveillez les messages syslog générés par la commande **crypto logging session**. Une fois que cela a été confirmé, vous pouvez continuer à activer FlexVPN.

2. Sur le même orateur, entrez ceci :

   ```
   interface tunnel 1
     no shut
   ```

Étapes de vérification

Stabilité IPsec

La meilleure façon d'évaluer la stabilité IPsec est de surveiller les sylogs avec la commande de configuration **crypto logging session** activée. Si vous voyez des sessions qui montent et descendent, cela peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que la migration puisse commencer.

Informations BGP renseignées

Si IPsec est stable, assurez-vous que la table BGP est remplie d'entrées provenant des rayons (sur le concentrateur) et d'un résumé provenant du concentrateur (sur les rayons). Dans le cas du protocole BGP, vous pouvez afficher ceci à l'aide des commandes suivantes :

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Voici un exemple d'informations correctes provenant du concentrateur 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
```

Le résultat montre que le concentrateur a appris un préfixe à partir de chacun des rayons et que les deux rayons sont dynamiques et marqués d'un astérisque (*). Il indique également qu'un total de quatre préfixes de la connexion inter-concentrateur est reçu.

Voici un exemple d'informations similaires provenant du discours :

```
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 rayon a reçu deux préfixes du concentrateur. Dans le cas de cette configuration, un préfixe doit être le résumé annoncé sur le concentrateur FlexVPN. L'autre est le réseau DMVPN **10.0.0.0/24** redistribué sur le DMVPN satellite dans BGP.

Migrer vers de nouveaux tunnels avec EIGRP

Le protocole EIGRP est un choix populaire dans les réseaux DMVPN en raison de son déploiement relativement simple et de sa convergence rapide. Cependant, elle évolue moins vite que le protocole BGP et n'offre pas beaucoup de mécanismes avancés qui peuvent être utilisés directement par le protocole BGP. La section suivante décrit l'une des façons de passer à FlexVPN avec un nouveau processus EIGRP.

Configuration de satellite mise à jour

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

```
router eigrp 200
network 10.1.1.0 0.0.0.255
network 192.168.101.0
passive-interface default
```

```
no passive-interface Tunnel1
```

Note: Il est préférable de ne pas établir de contiguïté de protocole de routage sur des tunnels de rayon à rayon. Par conséquent, ne faites que rendre l'interface de **tunnel1** (rayon à concentrateur) non passive.

Configuration du concentrateur FlexVPN mise à jour

De même, pour le concentrateur FlexVPN, préparez le protocole de routage dans le système autonome approprié, correspondant à celui configuré sur les rayons.

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

Deux méthodes sont utilisées pour fournir un résumé vers le satellite.

- Redistribuez une route statique qui pointe vers **null0** (option préférée).

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY

router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

Cette option permet de contrôler le résumé et la redistribution sans modifier la configuration de la technologie de virtualisation (VT) du concentrateur. Ceci est important, car la configuration VT du concentrateur ne peut pas être modifiée si un accès virtuel actif lui est associé.

- Configurez une adresse récapitulative de type DMVPN sur un modèle virtuel.

Cette configuration *n*'est *pas recommandée*, en raison du traitement interne et de la réplication de ce résumé à chaque accès virtuel. Il est présenté ici à titre de référence.

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

Un autre aspect à prendre en compte est l’échange de routage entre concentrateurs. Cela peut être fait si vous redistribuez des instances EIGRP à iBGP.

Concentrateur DMVPN - Configuration BGP mise à jour

La configuration reste de base. Vous devez redistribuer des préfixes spécifiques du protocole EIGRP vers BGP :

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

Concentrateur FlexVPN - Configuration BGP mise à jour

À l'instar du concentrateur DMVPN, dans FlexVPN, vous devez redistribuer les préfixes du nouveau processus EIGRP à BGP :

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

Migration du trafic vers FlexVPN

Vous devez arrêter la fonctionnalité DMVPN et activer FlexVPN sur chaque rayon, un par un, afin d'effectuer la migration. Cette procédure garantit un impact minimal :

1. Sur chaque rayon, entrez ceci séparément :

   ```
   interface tunnel 0
    shut
   ```

   À ce stade, assurez-vous qu'aucune session IKEv1 n'est établie sur ce rayon. Ceci peut être vérifié si vous vérifiez le résultat de la commande **show crypto isakmp sa** et surveillez les messages syslog générés par la commande **crypto logging session**. Une fois que cela a été confirmé, vous pouvez continuer à activer FlexVPN.
2. Sur le même orateur, entrez ceci :

   ```
   interface tunnel 1
     no shut
   ```

Étapes de vérification

Stabilité IPsec

Comme dans le cas de BGP, vous devez évaluer si IPsec est stable. La meilleure façon de le faire est de surveiller les sylogs avec la commande de configuration **crypto logging session** activée. Si vous voyez des sessions monter et descendre, cela peut indiquer un problème au niveau IKEv2/FlexVPN qui doit être corrigé avant que la migration puisse commencer.

Informations EIGRP dans la table topologique

Assurez-vous que votre table topologique EIGRP contient des entrées LAN en étoile sur le concentrateur et un résumé sur les rayons. Vous pouvez vérifier si vous entrez cette commande sur les concentrateurs et les rayons :

```
show ip eigrp [AS_NUMBER] topology
```

Voici un exemple de sortie du satellite :

```
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
```

Le résultat montre que le rayon connaît son sous-réseau LAN (en *italique*) et les résumés de ceux-ci (en **gras**).

Voici un exemple de sortie du concentrateur :

```
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)
```

Le résultat montre que le concentrateur connaît les sous-réseaux LAN des rayons (en *italique*), le préfixe de résumé qu'il annonce (en **gras**) et l'adresse IP attribuée à chaque rayon par négociation.

Considérations supplémentaires

Tunnels Spoke-to-Spoke qui existent déjà

Comme un arrêt de l'interface de tunnel DMVPN entraîne la suppression des entrées NHRP, les tunnels de rayon à rayon qui existent déjà seront désactivés.

Effacer les entrées NHRP

Un concentrateur FlexVPN ne dépend pas du processus d'enregistrement NHRP du rayon pour savoir comment router le trafic. Cependant, les tunnels de rayon à rayon dynamique reposent sur des entrées NHRP.

Dans DMVPN, si le protocole NHRP sur le concentrateur est effacé, il peut entraîner des problèmes de connectivité de courte durée. Dans FlexVPN, la suppression de NHRP sur les rayons entraîne la désactivation de la session IPsec FlexVPN, liée aux tunnels de rayon à rayon. La suppression de NHRP sur le concentrateur n'a aucun effet sur la session FlexVPN.

En effet, dans FlexVPN par défaut :

- Les rayons ne s'inscrivent pas aux concentrateurs.
- Les concentrateurs fonctionnent uniquement en tant que redirecteurs NHRP et n'installent pas d'entrées NHRP.
- Les entrées de raccourci NHRP sont installées sur les rayons des tunnels de rayon à rayon et sont dynamiques.

Caveats connus

Le trafic Spoke-to-Spoke peut être affecté par l'ID de bogue Cisco CSCub07382 .

Informations connexes

- Exemple de configuration de migration logicielle DMVPN vers FlexVPN
- Support et documentation techniques - Cisco Systems