Exemple de configuration de FlexVPN Spoke dans une conception de concentrateur redondant avec une approche double cloud

Contenu

Introduction

Ce document décrit comment configurer un rayon dans un réseau FlexVPN avec l'utilisation du bloc de configuration du client FlexVPN dans un scénario où plusieurs concentrateurs sont disponibles.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- Protocoles de routage Cisco

Components Used

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

- Routeur à services intégrés (ISR) de la gamme Cisco G2
- Cisco IOS® Version 15.2M

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.

Configuration

Pour des raisons de redondance, un rayon peut avoir besoin de se connecter à plusieurs concentrateurs. La redondance côté satellite permet un fonctionnement continu sans point de défaillance unique côté concentrateur.

Les deux conceptions de concentrateurs redondants FlexVPN les plus courantes qui utilisent la configuration en étoile sont les suivantes :

- **Double approche cloud**, où un rayon a deux tunnels distincts actifs aux deux concentrateurs en tout temps.
- **Approche de basculement**, où un rayon a un tunnel actif avec un concentrateur à un moment donné.

Les deux approches présentent un ensemble unique de avantages et de inconvénients.

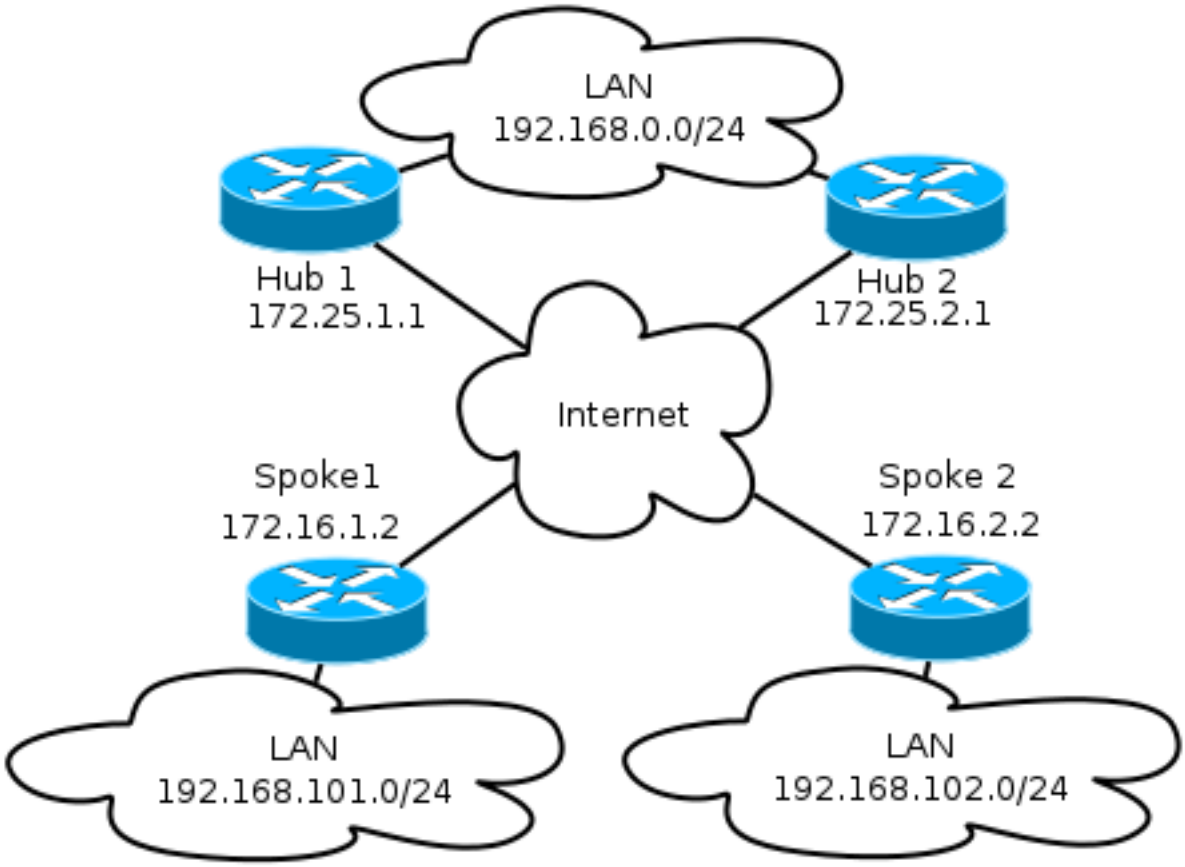
Approche	Avantages	Cons
Double cloud	• Récupération plus rapide en cas de panne, en fonction des compteurs de protocole de routage • Plus de possibilités de distribution du trafic entre les concentrateurs, car la connexion aux deux concentrateurs est active	• Spoke maintient une session aux deu concentrateurs en même temps, ce c consomme des ressources sur les de concentrateurs
Basculement	• Configuration facile - intégré à FlexVPN • Ne s'appuie pas sur le protocole de routage en cas de défaillance	• Délai de récupération plus lent - basé la détection DPD (Dead Peer Detecti ou (éventuellement) le suivi des obje • Tout le trafic est contraint de se dépla vers un seul concentrateur à la fois.

Ce document décrit la première approche. L'approche de cette configuration est similaire à la configuration double cloud DMVPN (Dynamic Multipoint VPN). La configuration de base du concentrateur et du rayon est basée sur les documents de migration de DMVPN à FlexVPN. Reportez-vous à la migration FlexVPN : Article Hard Move from DMVPN to FlexVPN on Same Devices on Same Devices pour une description de cette configuration.

Diagramme du réseau

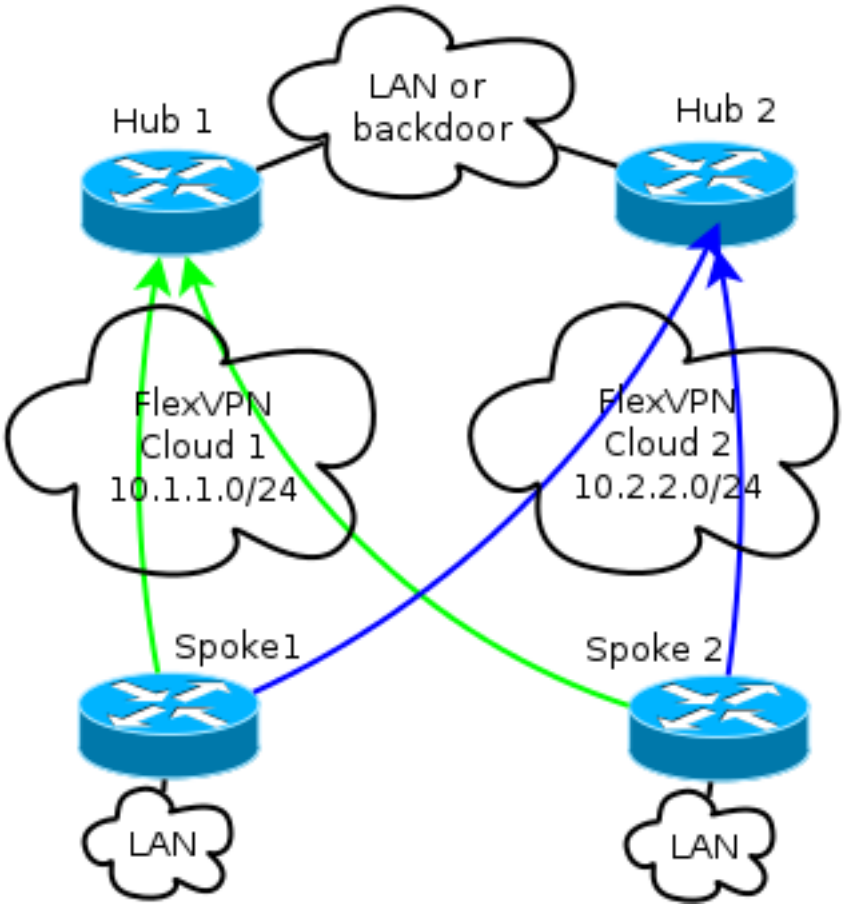
Réseau de transport

Ce schéma illustre le réseau de transport de base généralement utilisé dans les réseaux FlexVPN.



Réseau superposé

Le schéma illustre le réseau superposé avec une connectivité logique qui montre comment le basculement doit fonctionner. Pendant le fonctionnement normal, Spoke 1 et Spoke 2 entretiennent une relation avec les deux concentrateurs. En cas de défaillance, le protocole de routage bascule d’un concentrateur à un autre.



Note: Dans le schéma, les lignes vertes indiquent la connexion et la direction des sessions Internet Key Exchange Version 2 (IKEv2)/Flex vers le concentrateur 1, et les lignes bleues indiquent la connexion au concentrateur 2.

Les deux concentrateurs conservent un adressage IP distinct dans les nuages superposés. L'adressage **/24** représente le pool d'adresses alloué pour ce nuage, et non l'adressage d'interface réel. En effet, le concentrateur FlexVPN alloue généralement une adresse IP dynamique pour l'interface en étoile et repose sur des routes insérées dynamiquement via des commandes de route dans le bloc d'autorisation FlexVPN.

Configurations des rayons

Configuration de l'interface du tunnel en étoile

La configuration type utilisée dans cet exemple est simplement deux interfaces de tunnel avec deux adresses de destination distinctes.

```
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
tunnel source Ethernet0/0
```

```
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
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 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Pour permettre aux tunnels de rayon à rayon de se former correctement, un modèle virtuel (VT) est nécessaire.

```
interface Virtual-Template1 type tunnel
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 path-mtu-discovery
tunnel protection ipsec profile default
```

Le rayon utilise une interface non numérotée qui indique l'interface LAN dans le VRF (Virtual Routing and Forwarding), qui est globale dans ce cas. Cependant, il peut être préférable de référencer une interface de bouclage. En effet, les interfaces de bouclage restent en ligne dans presque toutes les conditions.

Configuration du protocole BGP (Spoke Border Gateway Protocol)

Puisque Cisco recommande iBGP comme protocole de routage à utiliser dans le réseau de superposition, ce document mentionne uniquement cette configuration.

> **Note**: Les rayons doivent conserver l'accessibilité BGP aux deux concentrateurs.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

Dans cette configuration, FlexVPN n'a pas de concept de concentrateur principal ou secondaire. L’administrateur décide si le protocole de routage préfère un concentrateur à un autre ou, dans certains cas, effectue l’équilibrage de charge.

Considérations relatives au basculement et à la convergence des rayons

Afin de minimiser le temps nécessaire à un rayon pour détecter une défaillance, utilisez ces deux méthodes typiques.

- Raccourcissez les temporisateurs BGP. Le temps d'attente par défaut entraîne le basculement.
- Configurez le basculement BGP, qui est abordé dans cet article, Prise en charge BGP pour la désactivation de session d'appairage rapide.
- N'utilisez pas la détection de transfert bidirectionnel (BFD), car elle n'est pas recommandée dans la plupart des déploiements FlexVPN.

Tunnels Spoke-to-Spoke et basculement

Les tunnels de rayon à rayon utilisent la commutation de raccourcis NHRP (Next Hop Resolution Protocol). Cisco IOS indique que ces raccourcis sont des routes NHRP, par exemple :

```
Spoke1#show ip route nhrp
(...)

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Ces routes n'expirent pas lorsque la connexion BGP expire ; au lieu de cela, ils sont conservés pendant la durée de conservation du NHRP, qui est de deux heures par défaut. Cela signifie que les tunnels de rayon à rayon actifs restent en fonctionnement même en cas de défaillance.

Configurations du concentrateur

Pools locaux

Comme indiqué dans la section **Schéma du réseau**, les deux concentrateurs conservent un adressage IP distinct.

Concentrateur1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Concentrateur 2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

Configuration du concentrateur BGP

La configuration BGP du concentrateur reste similaire aux exemples précédents.

Ce résultat provient du concentrateur 1 avec l'adresse IP LAN **192.168.0.1**.

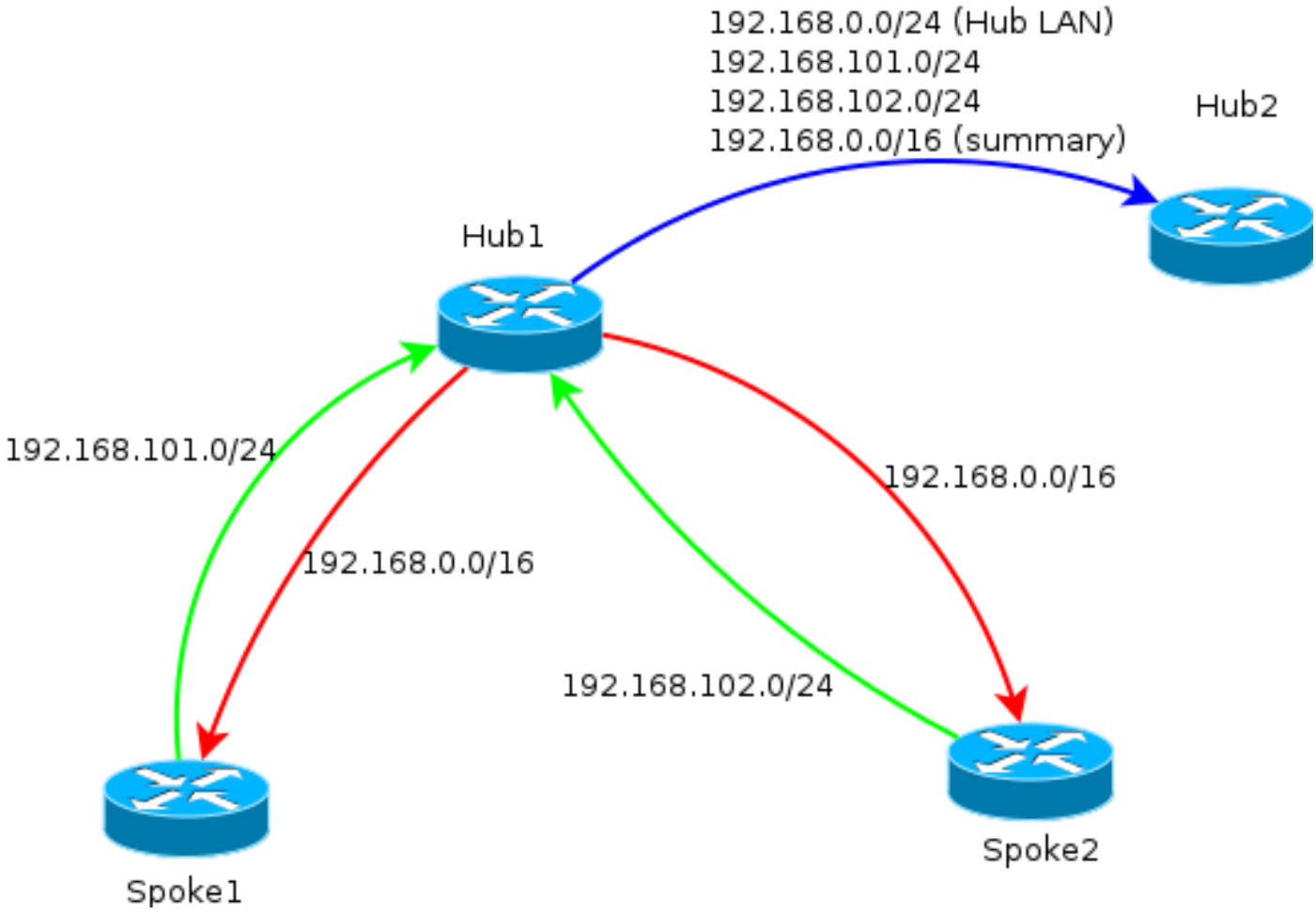
```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
```

```
neighbor Spokes fall-over
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

En substance, voici ce qui est fait :

- Le pool d'adresses FlexVPN local se trouve dans la plage d'écoute BGP.
- Le réseau local est 192.168.0.0/24.
- Un résumé n'est annoncé que pour les rayons. La configuration de l'adresse agrégée crée une route statique pour ce préfixe via l'interface null0, qui est une route de rejet utilisée afin d'empêcher les boucles de routage.
- Tous les préfixes spécifiques sont annoncés à l'autre concentrateur. Comme il s'agit également d'une connexion iBGP, il nécessite une configuration de réflecteur de route.

Ce diagramme représente l'échange de préfixes BGP entre les rayons et les concentrateurs dans un cloud FlexVPN.



Note: Dans le diagramme, la ligne verte représente les informations fournies par les rayons au concentrateur, la ligne rouge représente les informations fournies par chaque concentrateur aux rayons (un résumé uniquement) et la ligne bleue représente les préfixes échangés entre les concentrateurs.

Vérification

Puisque chaque rayon conserve son association avec les deux concentrateurs, deux sessions IKEv2 sont vues avec la commande **show crypto ikev2 sa**.

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

Pour afficher les informations du protocole de routage, entrez les commandes suivantes :

show bgp ipv4 unicast

show bgp summary

Sur les rayons, vous devez voir que le préfixe de résumé est reçu des concentrateurs et que les connexions aux deux concentrateurs sont actives.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, 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
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

Dépannage

Il y a deux principaux blocs à dépanner :

- IKE (Internet Key Exchange)
- Sécurité du protocole Internet (IPsec)

Voici les commandes show appropriées :

```
show crypto ipsec sa

show crypto ikev2 sa
```

Voici les commandes de débogage appropriées :

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Voici le protocole de routage approprié :

```
show bgp ipv4 unicast (or show ip bgp)

show bgp summary
```