Exemple de configuration d'un satellite FlexVPN dans une conception de concentrateur redondant avec un bloc de client FlexVPN

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.

Informations générales

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 les connexions aux deux concentrateurs sont actives	• Spoke maintient une session aux de concentrateurs en même temps, ce consomme des ressources sur les c 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 - bas la détection DPD (Dead Peer Detec ou (éventuellement) le suivi des obj • Tout le trafic est contraint de se dép vers un concentrateur à la fois

Ce document décrit la deuxième approche.

Configuration

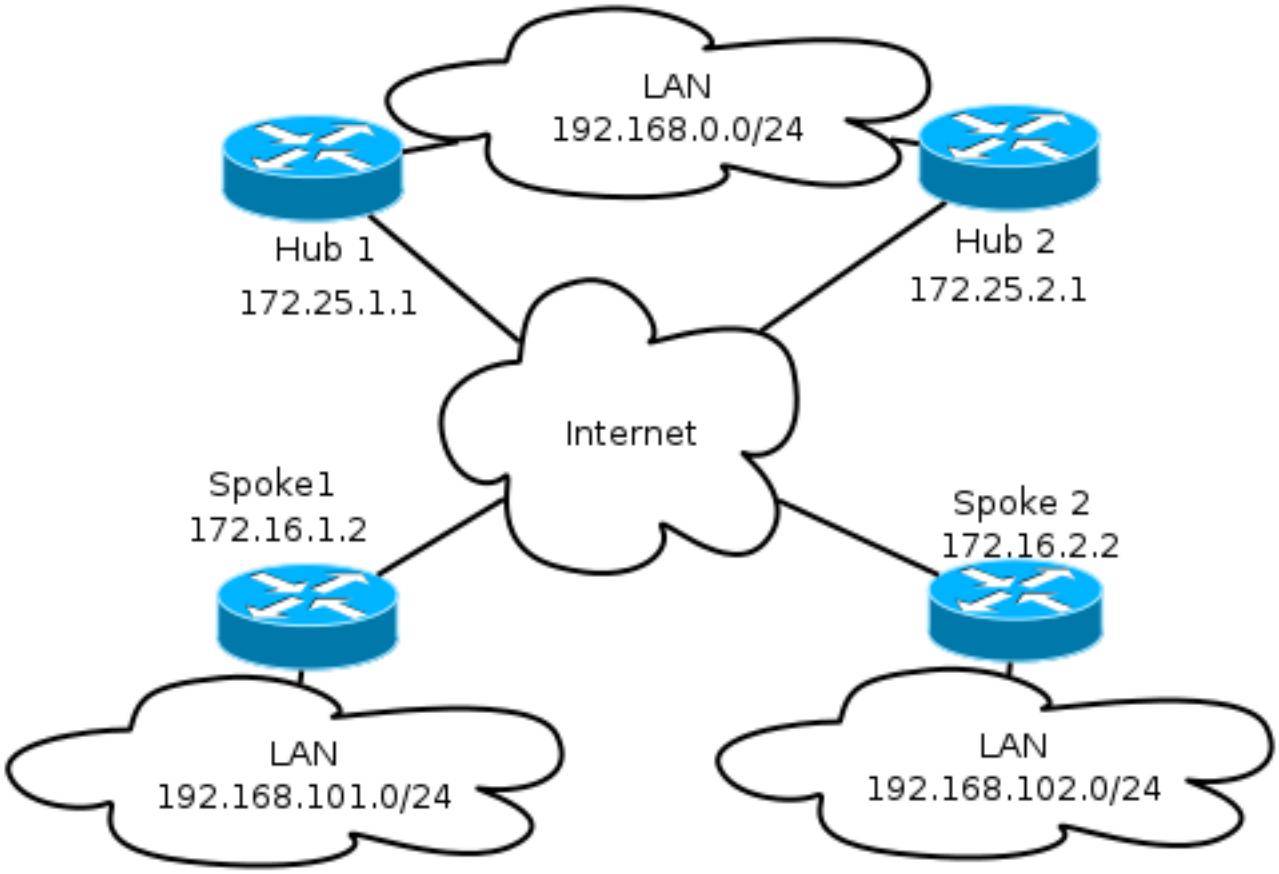
Note: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagrammes du réseau

Ces diagrammes présentent à la fois les diagrammes de topologie de transport et de superposition.

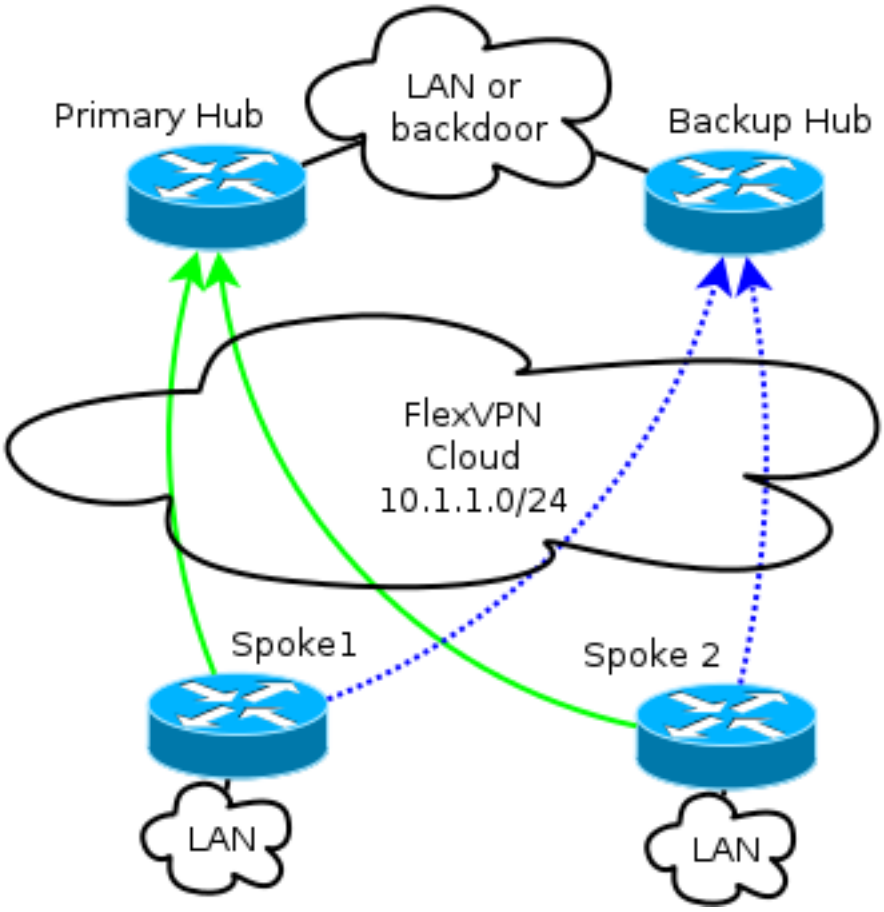
Réseau de transport

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



Réseau superposé

Ce schéma illustre le réseau superposé avec une connectivité logique qui montre comment le basculement doit fonctionner. En fonctionnement normal, les satellites 1 et 2 entretiennent une relation avec un seul concentrateur.



Note: Dans le schéma, les lignes vertes solides indiquent la connexion et la direction des sessions IKEv2/Flex principales d'Internet Key Exchange et les lignes bleues en pointillés indiquent la connexion de secours en cas d'échec de la session IKE (Internet Key Exchange) vers le concentrateur principal.

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.

Configuration de base de Spoke et de Hub

La configuration de base du concentrateur et du rayon est basée sur les documents de migration de DMVPN (Dynamic Multipoint VPN) à FlexVPN. Cette configuration est décrite dans la migration FlexVPN : Déplacement de DMVPN vers FlexVPN sur le même article.

Ajustement de la configuration du rayon

Configuration du satellite - Bloc de configuration du client

La configuration de satellite doit être étendue par le bloc de configuration du client.

Dans la configuration de base, plusieurs homologues sont spécifiés. L'homologue ayant la

préférence la plus élevée (nombre le plus faible) est considéré avant les autres.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

La configuration du tunnel doit changer afin de permettre le choix dynamique de la destination du tunnel, en fonction du bloc de configuration du client FlexVPN.

```
interface Tunnel1
 tunnel destination dynamic
```

Il est essentiel de se rappeler que le bloc de configuration du client FlexVPN est lié à une interface et non à IKEv2 ou au profil de sécurité du protocole Internet (IPsec).

Le bloc de configuration du client fournit plusieurs options afin d'ajuster le temps de basculement et les opérations, qui incluent l'utilisation des objets de suivi, la sauvegarde par numérotation et les fonctionnalités de groupes de sauvegarde.

Avec la configuration de base, le rayon s'appuie sur des DPD afin de détecter si un rayon ne répond pas, et déclenche une modification une fois que l'homologue est déclaré mort. L'option d'utilisation de DPD n'est pas rapide, en raison du fonctionnement des DPD. Un administrateur peut souhaiter améliorer la configuration avec le suivi des objets ou des améliorations similaires.

Pour plus d'informations, reportez-vous au chapitre **FlexVPN Client Configuration** du guide de configuration de Cisco IOS, qui est lié à la section **Informations connexes** à la fin de ce document.

Configuration en étoile complète - Référence

```
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 ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

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

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN 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
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Configuration du concentrateur

Bien que la majorité de la configuration du concentrateur reste identique, plusieurs aspects doivent être abordés. La plupart d'entre elles concernent une situation dans laquelle un ou plusieurs rayons sont connectés à un concentrateur, tandis que d'autres restent liés à un autre concentrateur.

Adresses satellite

Puisque les rayons obtiennent des adresses IP des concentrateurs, il est généralement souhaitable que les concentrateurs attribuent des adresses de sous-réseaux différents ou d'une partie différente d'un sous-réseau.

Exemple :

Concentrateur1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

Concentrateur 2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

Cela évite la création de chevauchement, même si les adresses ne sont pas routées en dehors du cloud FlexVPN, ce qui pourrait nuire au dépannage.

Adresse de superposition du concentrateur

Les deux concentrateurs peuvent conserver la même adresse IP sur une interface de modèle virtuel ; cependant, cela peut avoir un impact sur le dépannage dans certains cas. Ce choix de conception facilite le déploiement et la planification, car le rayon ne doit avoir qu'une seule adresse homologue pour le protocole BGP (Border Gateway Protocol).

Dans certains cas, elle peut ne pas être souhaitée ou nécessaire.

Routage

Il est nécessaire que les concentrateurs échangent des informations sur les rayons connectés.

Les concentrateurs doivent pouvoir échanger les routes spécifiques des périphériques qu'ils ont connectés et fournir un résumé aux rayons.

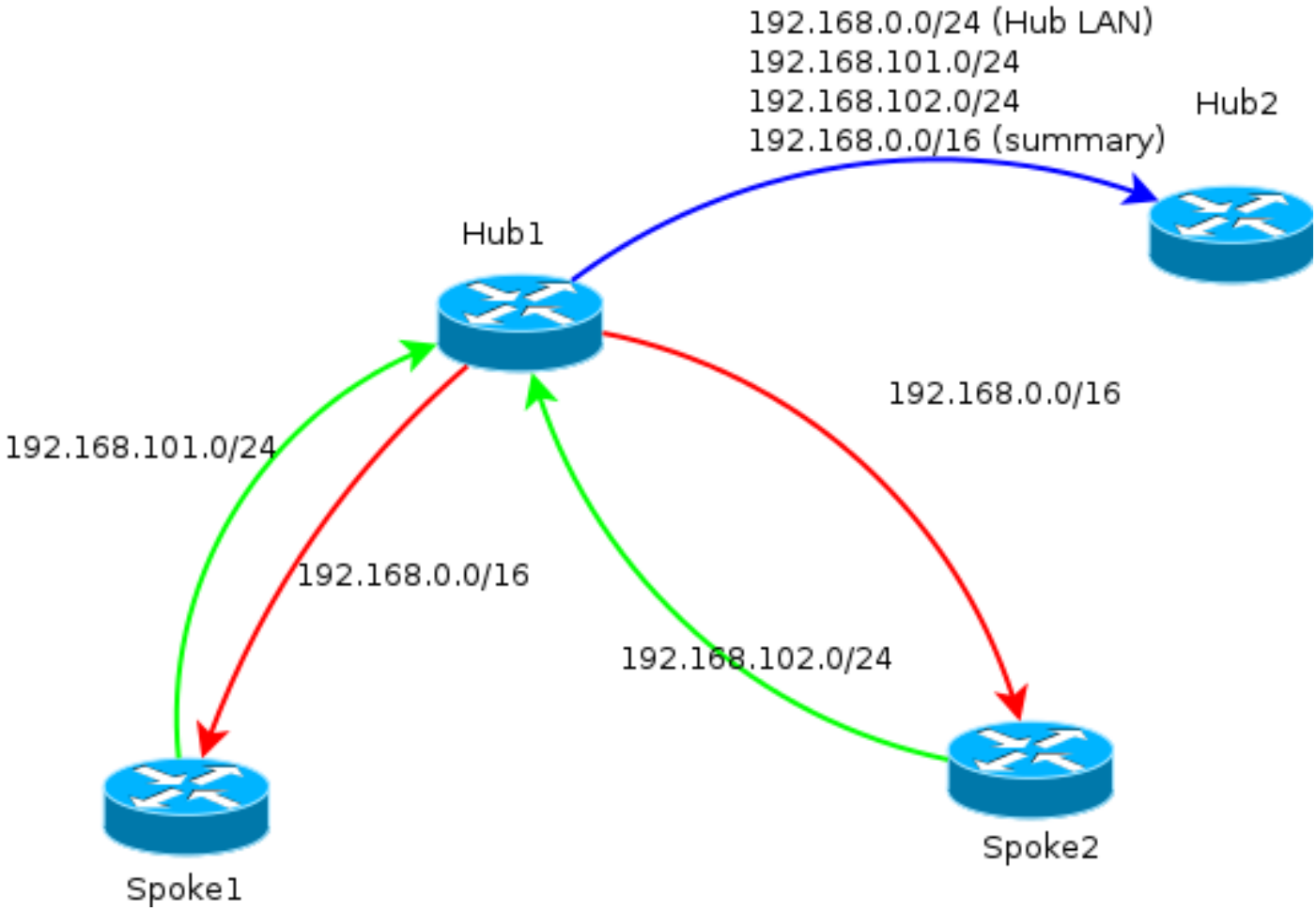
Puisque Cisco vous recommande d'utiliser iBGP avec FlexVPN et DMVPN, seul le protocole de routage est affiché.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
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

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

Cette configuration permet :

- Écouteur dynamique à partir des adresses attribuées aux rayons
- Réseau publicitaire de 192.168.0.0/24
- Annonce de la route récapitulative de 192.168.0.0/16 à tous les rayons. La configuration d'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.
- Transfert de préfixes spécifiques vers l'autre concentrateur
- Client de réflecteur de route pour s'assurer que les concentrateurs échangent les informations acquises par les rayons entre eux

Ce diagramme représente l'échange de préfixe dans BGP dans cette configuration, du point de vue de l'un des concentrateurs.



Note: Dans ce 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.

Récapitulatif des réseaux utilisés

Dans certains scénarios, les résumés peuvent ne pas être applicables ou souhaitées. Soyez prudent lorsque vous spécifiez l'adresse IP de destination dans les préfixes, car iBGP ne remplace pas le saut suivant par défaut.

Les résumés sont recommandés dans les réseaux qui changent fréquemment d'état. Par exemple, les connexions Internet instables peuvent nécessiter des résumés afin de : évitez la suppression et l'ajout de préfixes, limitez le nombre de mises à jour et autorisez la plupart des configurations à évoluer correctement.

Tunnels satellite à satellite

Dans le scénario et la configuration mentionnés dans la section précédente, les rayons des différents concentrateurs ne peuvent pas établir de tunnels de rayon à rayon direct. Le trafic entre les rayons connectés à différents concentrateurs passe par les périphériques centraux.

Il y a une solution facile à cela. Cependant, il nécessite que le protocole NHRP (Next Hop

Resolution Protocol) avec le même ID réseau soit activé entre les concentrateurs. Cela peut être réalisé, par exemple, si vous créez un tunnel GRE (Generic Routing Encapsulation) point à point entre les concentrateurs. Ensuite, IPsec n'est pas requis.

Vérification

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

La commande **show crypto ikev2 sa** vous informe de l'emplacement de connexion du rayon.

La commande **show crypto ikev2 client flexvpn** permet à un administrateur de comprendre l'état actuel du fonctionnement du client FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

Un basculement réussi avec la configuration **show logging** consigne cette sortie sur le périphérique en étoile :

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

Dans cette sortie, le rayon se déconnecte du **concentrateur 172.25.1.1**, le bloc de configuration client Flex_Client détecte une défaillance et force une connexion à **172.25.2.1** où un tunnel s'active, et un rayon se voit attribuer une adresse IP **10.1.1.17**.

Dépannage

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Note: Référez-vous aux informations importantes sur les commandes de débogage avant

d'utiliser les commandes de débogage.

Voici les commandes de débogage appropriées :

- **debug crypto ikev2**
- **debug radius**

Informations connexes

- Guide de configuration FlexVPN et Internet Key Exchange version 2, Cisco IOS version 15 M&T
- Support et documentation techniques - Cisco Systems