# FlexVPN : Exemple de configuration d'IPv6 dans un déploiement Hub and Spoke

## Contenu



## Introduction

Ce document décrit une configuration commune qui utilise un déploiement de concentrateur et de satellite Cisco IOS® FlexVPN dans un environnement IPv6. Il développe les concepts abordés dans FlexVPN : Configuration de base de LAN à LAN IPv6.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS FlexVPN
- Protocoles de routage

### Components Used

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

- Routeurs à services intégrés Cisco de 2e génération (ISR G2)
- Logiciel Cisco IOS Version 15.3 (ou Version 15.4T pour tunnels de rayon à rayon dynamique avec IPv6)

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

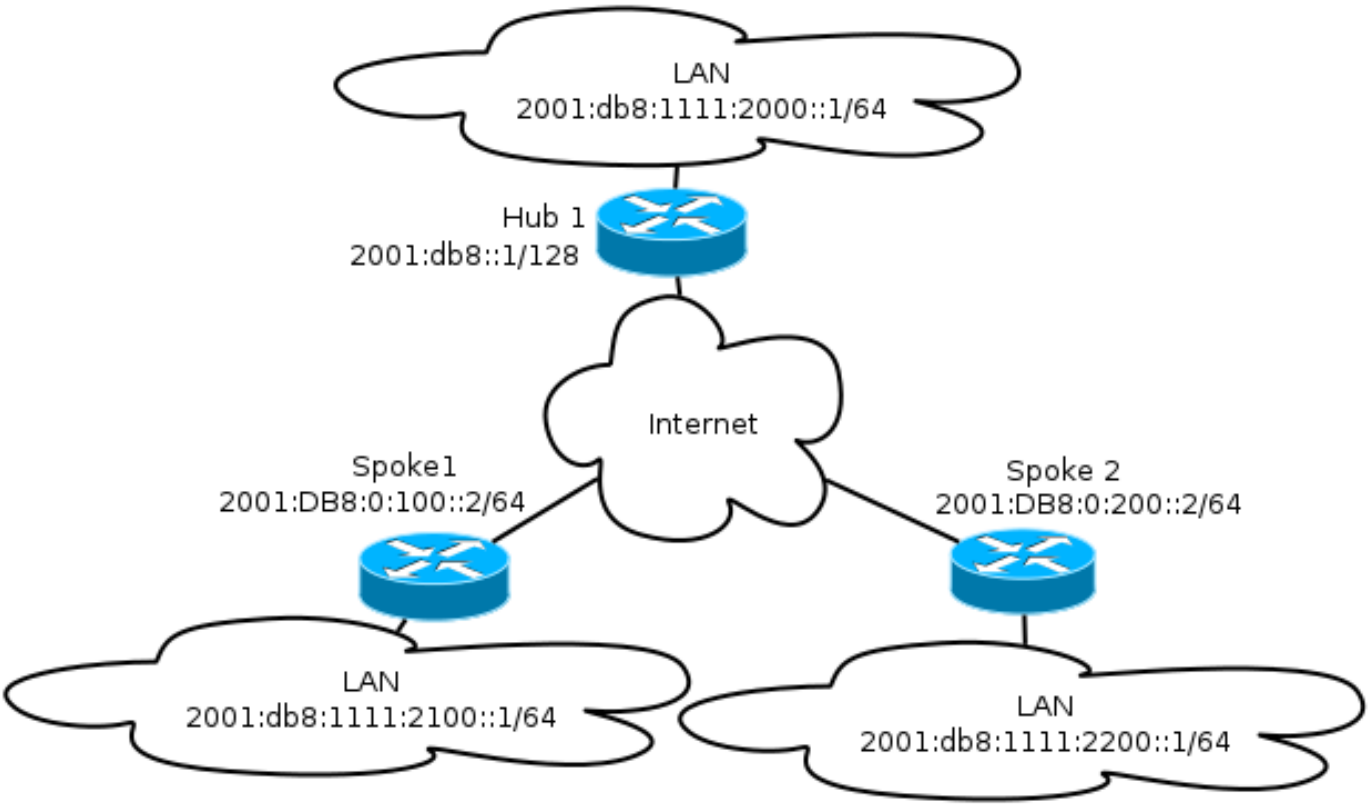
> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Bien que cet exemple de configuration et ce schéma de réseau utilisent IPv6 comme réseau de transport, l'encapsulation de routage générique (GRE) est généralement utilisée dans les déploiements FlexVPN. L'utilisation de GRE au lieu d'IPsec permet aux administrateurs d'exécuter IPv4 ou IPv6 ou les deux sur les mêmes tunnels, quel que soit le réseau de transport.

## Diagramme du réseau

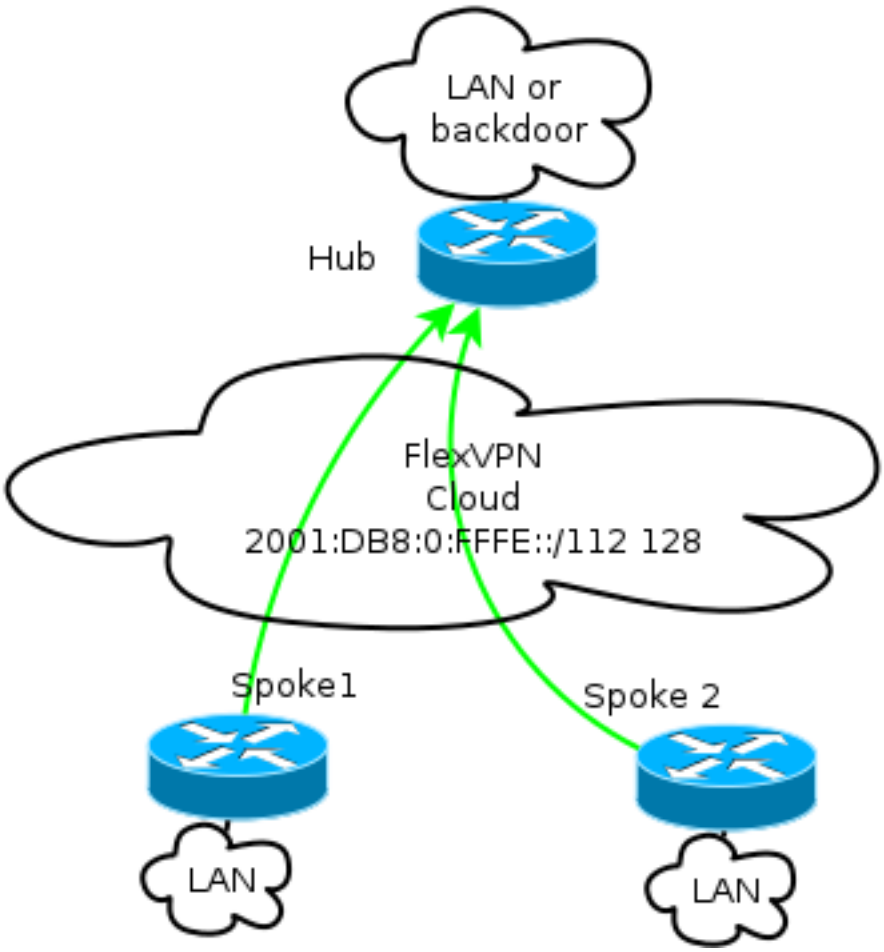
### Réseau de transport

Voici un schéma du réseau de transport utilisé dans cet exemple :



### Réseau superposé

Voici un schéma de la topologie de réseau de superposition de base utilisée dans cet exemple :




Chaque rayon est attribué à partir d'un pool d'adresses /112, mais reçoit une adresse /128. Ainsi, la notation '/112 128' est utilisée dans la configuration du pool IPv6 du concentrateur.

## Configurations

Cette configuration montre une superposition IPv4 et IPv6 qui fonctionne sur un backbone IPv6.

Comparé aux exemples qui utilisent IPv4 comme backbone, notez que vous devez utiliser la commande **tunnel mode** afin de modifier le noeud et de prendre en charge le transport IPv6.

La fonctionnalité de tunnel en étoile sur IPv6 sera introduite dans le logiciel Cisco IOS Version 15.4T, qui n'est pas encore disponible.

### Protocoles de routage

Cisco vous recommande d'utiliser le protocole BGP (Border Gateway Protocol) interne pour l'appairage entre les rayons et les concentrateurs pour les déploiements de grande envergure, car iBGP est le protocole de routage le plus évolutif.

La plage d'écoute BGP (Border Gateway Protocol) ne prend pas en charge la plage IPv6, mais elle simplifie l'utilisation avec un transport IPv4. Bien qu'il soit possible d'utiliser BGP dans un tel environnement, cette configuration illustre un exemple de base, de sorte que le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) a été choisi.

### Configuration du concentrateur

Par rapport aux exemples précédents, cette configuration inclut l'utilisation de nouveaux protocoles de transport.

Pour configurer le concentrateur, l'administrateur doit :

- Activez le routage de monodiffusion.
- Provisionner le routage de transport.
- Provisionnez un nouveau pool d'adresses IPv6 à attribuer dynamiquement. Le pool est 2001:DB8:0:FFFE::/112 ; 16 bits permettent d'adresser 65 535 périphériques.
- Activez IPv6 pour la configuration NHRP (Next Hop Resolution Protocol) afin d'autoriser IPv6 dans la superposition.
- Compte pour l'adressage IPv6 dans le trousseau de clés ainsi que le profil dans la configuration de chiffrement.

Dans cet exemple, le concentrateur annonce un résumé EIGRP à tous les rayons.

Cisco ne recommande pas l'utilisation d'une adresse récapitulative sur l'interface Virtual-Template dans le déploiement FlexVPN ; cependant, dans un VPN multipoint dynamique (DMVPN), ceci n'est pas seulement courant, mais est également considéré comme une pratique recommandée. Voir Migration FlexVPN : Déplacement de DMVPN vers FlexVPN sur les mêmes périphériques : Configuration du concentrateur mise à jour pour plus de détails.

```
ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
 ipv6 pool FlexSpokesv6
pool FlexSpokes
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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
```

```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Loopback100
ipv6 enable
ipv6 eigrp 65001
 ipv6 nhrp network-id 2
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
 distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Template1
 network 10.1.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 redistribute static metric 1500 10 10 1 1500

ipv6 router eigrp 65001
 distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1
 redistribute static metric 1500 10 10 1 1500
```

## Configuration du rayon

Comme dans la configuration du concentrateur, l'administrateur doit provisionner l'adressage IPv6, activer le routage IPv6 et ajouter la configuration NHRP et de chiffrement.

Il est possible d'utiliser le protocole EIGRP et d'autres protocoles de routage pour l'appairage de rayon à rayon. Cependant, dans un scénario type, les protocoles ne sont pas nécessaires et peuvent avoir un impact sur l'évolutivité et la stabilité.

Dans cet exemple, la configuration de routage conserve uniquement la contiguïté EIGRP entre le rayon et le concentrateur, et la seule interface qui n'est pas passive est l'interface Tunnel1 :

```
ipv6 unicast-routing
ipv6 cef
```

```
crypto logging session

crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

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 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel source Ethernet0/0
 tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

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
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Ethernet1/0
ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

Suivez ces recommandations lorsque vous créez des entrées de protocole de routage sur un rayon :

1. Autoriser le protocole de routage à établir une relation via la connexion (dans ce cas,

l'interface Tunnel1) au concentrateur. Il n'est généralement pas souhaitable d'établir une contiguïté de routage entre les rayons, car cela augmente considérablement la complexité dans la plupart des cas.

2. Annoncez les sous-réseaux LAN locaux uniquement et activez le protocole de routage sur une adresse IP attribuée par le concentrateur. Veillez à ne pas annoncer un grand sous-réseau, car il peut avoir un impact sur la communication de rayon à rayon.

Cet exemple reflète les deux recommandations pour le protocole EIGRP sur Spoke1 :

```
router eigrp 65001
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel1

ipv6 router eigrp 65001
 passive-interface default
 no passive-interface Tunnel1
```

# Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

> **Note**: 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 .

## Session Spoke-to-Hub

Une session correctement configurée entre les périphériques en étoile et les périphériques concentrateurs a une session Internet Key Exchange Version 2 (IKEv2) qui est active et un protocole de routage qui peut établir la contiguïté. Dans cet exemple, le protocole de routage est EIGRP. Il existe donc deux commandes EIGRP :

- **show crypto ikev2 sa**
- **show ipv6 eigrp 65001 neighbor**
- **show ip eigrp 65001 neighbor**

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/1945 sec
```

```
Spoke1#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   Link-local address:     Tu1                  14 00:32:29   72  1470  0  10
   FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   10.1.1.1                Tu1                  11 00:21:05   11  1398  0  26
```

Dans IPv4, EIGRP utilise une adresse IP attribuée à l'homologue ; dans l'exemple précédent, il s'agit de l'adresse IP du concentrateur 10.1.1.1.

IPv6 utilise une adresse link-local ; dans cet exemple, le concentrateur est FE80::A8BB:CCFF:FE00:6600. Utilisez la commande **ping** afin de vérifier que le concentrateur est accessible via son adresse IP link-local :

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

## Session Spoke-to-Spoke

Les sessions Spoke-to-Spoke sont abordées dynamiquement à la demande. Utilisez une simple commande **ping** afin de déclencher une session :

```
Spoke1#ping  2001:DB8:1111:2200::100 source e1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2200::100, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1111:2100::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
```

Pour confirmer la connectivité en étoile directe, l'administrateur doit :

- Vérifiez qu'une session dynamique de rayon à rayon déclenche une nouvelle interface d'accès virtuel :

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.
Peer 2001:DB8:0:200::2:500       Id: 2001:DB8:0:200::2
```

- Vérifiez l'état de la session IKEv2 :

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
```

```
 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/3275 sec

Tunnel-id    fvrf/ivrf              Status
2          none/none             READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8:0:200::2/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/665 sec
```

Notez que deux sessions sont disponibles : un rayon à concentrateur et un rayon à rayon.

- Vérifier NHRP :

```
Spoke1#show ipv6 nhrp
2001:DB8:0:FFFE::/128 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
2001:DB8:1111:2200::/64 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
NBMA address: 2001:DB8:0:200::2
```

Le résultat montre que 2001:DB8:111:2200::/64 (le LAN pour Spoke2) est disponible via 2001:DB8:0:FFFE::, qui est l'adresse IPv6 négociée sur l'interface Tunnel1 pour Spoke2. L'interface Tunnel1 est disponible via l'adresse NBMA (nonbroadcast multiaccess) 2001:db8:0:200::2 , qui est l'adresse IPv6 attribuée à Spoke2 de manière statique.

- Vérifiez que le trafic passe par cette interface :

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0)
  remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0)
  current_peer 2001:DB8:0:200::2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196
   #pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195
(...)
```

- Vérifiez le chemin de routage et les paramètres CEF :

```
Spoke1#show ipv6 route
(...)
D   2001:DB8:1111:2200::/64 [90/27161600]
    via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut]
```

```
    via FE80::A8BB:CCFF:FE00:6600, Tunnel1
(...)
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
 nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

# Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Ces commandes de débogage vous aident à résoudre les problèmes :

- FlexVPN/IKEv2 et IPsec : **debug crypto ipsecdebug crypto ikev2 [paquet|interne]**
- NHRP (satellite à satellite) :
  - **debug nhrp pack**
  - **debug nhrp extension**
  - **debug nhrp cache**
  - **debug nhrp route**

Reportez-vous à la liste de commandes principale de Cisco IOS, Toutes les versions pour plus d'informations sur ces commandes.