FlexVPN : IPv6 dans un exemple de configuration de déploiement de hub and spoke

Contenu

Introduction

Ce document décrit une configuration commune qui utilise un Cisco IOS® FlexVPN a parlé et déploiement de hub dans un environnement d'IPv6. Il examine les concepts discutés dans FlexVPN : RÉSEAU LOCAL de base d'IPv6 à la configuration LAN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS FlexVPN
- Protocoles de routage

Composants utilisés

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

- Génération 2 (ISR G2) d'Integrated Services Router de Cisco
- Version du logiciel Cisco IOS 15.3 (ou version 15.4T pour les tunnels dynamiques de spoke-to-spoke avec l'IPv6)

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.

Configurez

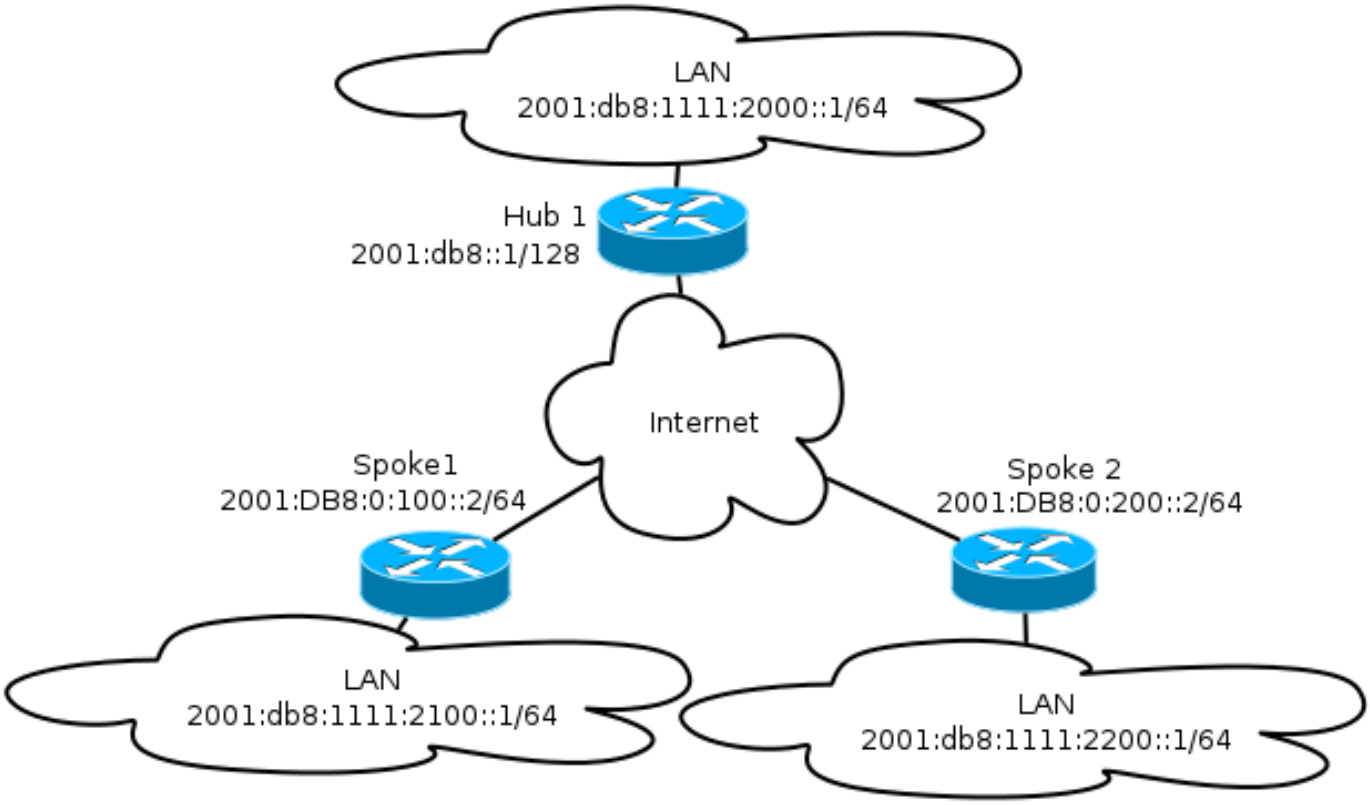
> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Tandis que ces exemple et schéma de réseau de configuration utilisent l'IPv6 comme réseau de transport, l'Encapsulation de routage générique (GRE) est typiquement utilisé dans des déploiements de FlexVPN. L'utilisation de GRE au lieu d'IPsec permet à des administrateurs pour exécuter l'ipv4 ou l'IPv6 ou chacun des deux au-dessus des mêmes tunnels, indépendamment du réseau de transport.

Diagramme du réseau

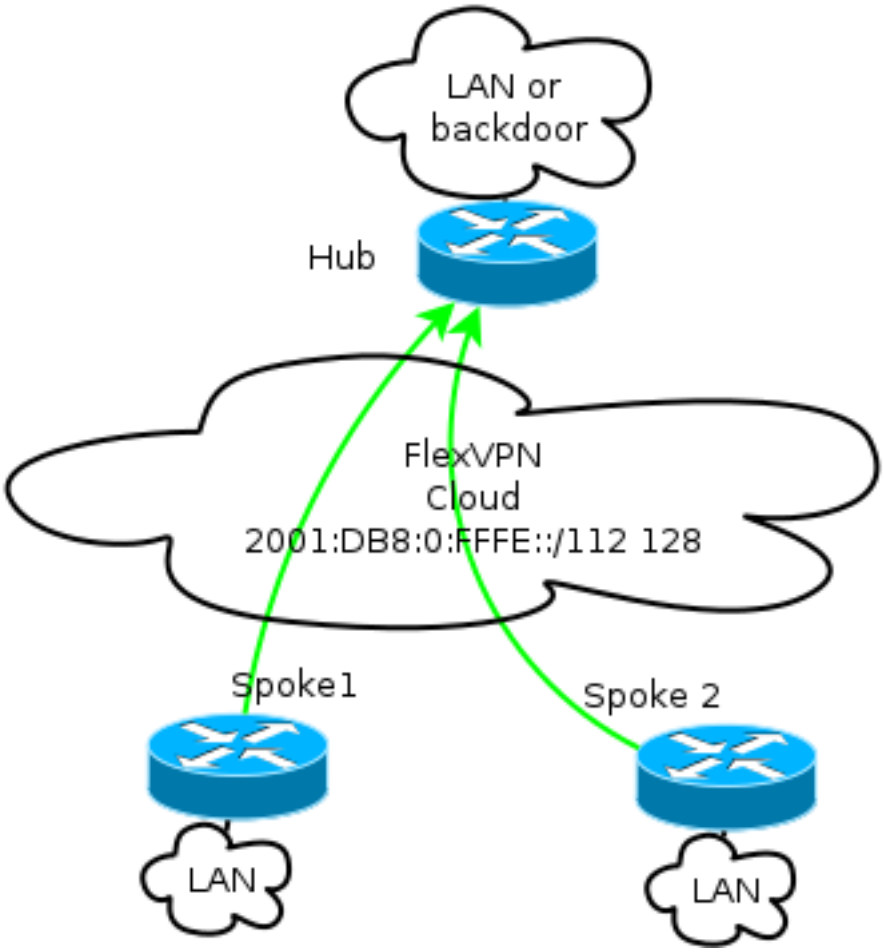
Réseau de transport

C'est un diagramme du réseau de transport utilisé dans cet exemple :



Réseau de substitution

C'est un diagramme de la topologie du réseau de base de recouvrement utilisée dans cet exemple :



Chaque rai est assigné d'un groupe d'adresses de /112, mais reçoit une adresse de /128. Ainsi, la notation '/112 128' est utilisée dans la configuration de groupe d'IPv6 du hub.

Configurations

Cette configuration affiche un ipv4 et l'IPv6 recouverts qui fonctionne au-dessus d'un circuit principal d'IPv6.

Une fois comparé aux exemples qui utilisent l'ipv4 comme circuit principal, notez que vous devriez utiliser la modification de noeud de commande de **tunnel mode** et faciliter le transport d'IPv6.

La caractéristique de tunnel de spoke-to-spoke au-dessus de l'IPv6 sera introduite dans la version du logiciel Cisco IOS 15.4T, qui n'est pas encore disponible.

Protocoles de routage

Cisco recommande que vous utilisiez l'Internal Border Gateway Protocol (iBGP) pour scruter entre le rai et les Concentrateurs pour de grands déploiements parce que l'iBGP est le protocole de routage le plus extensible.

Le Protocole BGP (Border Gateway Protocol) écoutent plage ne prend en charge pas la chaîne d'IPv6, mais elle simplifie l'utilisation avec un transport d'ipv4. Bien qu'il soit faisable d'utiliser le BGP dans un tel environnement, cette configuration illustre un exemple de base, ainsi le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) a été choisi.

Configuration du concentrateur

Comparé à des exemples plus anciens, cette configuration inclut l'utilisation de nouveaux protocoles de transport.

Afin de configurer le hub, l'administrateur a besoin :

- Routage d'unicast d'enable.
- Routage de transport de disposition.
- Provision un nouveau groupe d'adresses d'IPv6 à assigner dynamiquement. Le groupe est 2001:DB8:0:FFFE::/112 ; 16 bits tient compte pour que 65,535 périphériques soient adressés.
- Permettez à l'IPv6 pour la configuration de Protocole NHRP (Next Hop Resolution Protocol) afin de permettre l'IPv6 dans le recouvrement.
- Expliquez l'IPv6 adressant dans le keyring aussi bien que le profil dans la crypto configuration.

Dans cet exemple, le hub annonce un résumé EIGRP à tous les rais.

Cisco ne recommande pas l'utilisation d'une adresse récapitulative sur l'interface de modèle virtuel dans le déploiement de FlexVPN ; cependant, dans un VPN multipoint dynamique (DMVPN), c'est non seulement commun mais est également considéré une pratique recommandée. Voir le transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur les mêmes périphériques : Configuration mise à jour de hub pour des 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 de hub, l'administrateur doit provision l'IPv6 adressant, l'IPv6 d'enable conduisant, et ajoute le NHRP et la crypto configuration.

Il est faisable d'utiliser l'EIGRP et d'autres protocoles de routage pour scruter de spoke-to-spoke. Cependant, dans un scénario typique, les protocoles ne sont pas nécessaires et pourraient affecter l'évolutivité et la stabilité.

Dans cet exemple, la configuration de routage garde seulement la contiguïté EIGRP entre le rai et le hub, 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 quand vous créez des entrées de protocole de routage sur un rai :

1. Permettez au protocole de routage pour établir des relations par l'intermédiaire de la connexion (dans ce cas, l'interface Tunnel1) au hub. Il n'est généralement pas desirable d'établir la contiguïté de routage entre les rais parce que ceci augmente de manière significative la complexité dans la plupart des cas.

2. Annoncez les sous-réseaux de réseau local seulement, et activez le protocole de routage relatif à une adresse IP assignée par le hub. Faites attention à ne pas annoncer un grand sous-réseau parce qu'il pourrait affecter la transmission de spoke-to-spoke.

Cet exemple reflète les deux recommandations pour l'EIGRP sur Spoke1 :

```
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
```

Vérifiez

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

> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Session de Rai-à-hub

Une session correctement configurée entre le rai et les périphériques de hub a une session de la version 2 d'échange de clés Internet (IKE) (IKEv2) qui est en hausse et a un protocole de routage qui peut établir la contiguïté. Dans cet exemple, le protocole de routage est EIGRP, tellement là sont deux commandes EIGRP :

- affichez cryptos ikev2 SA
- voisin du show ipv6 eigrp 65001
- voisin du show ip eigrp 65001

```
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 l'ipv4, l'EIGRP emploie une adresse IP assignée pour scruter ; dans l'exemple précédent, c'est l'adresse IP de hub de 10.1.1.1.

L'IPv6 utilise une adresse locale à la liaison ; dans cet exemple, le hub est FE80::A8BB:CCFF:FE00:6600. Employez la **commande ping** afin de vérifier que le hub peut être accédé par son IP de lien-gens du pays :

```
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 de spoke-to-spoke

Des sessions de spoke-to-spoke sont apportées dynamiquement sur demande. Employez une **commande ping** simple afin de déclencher une session :

```
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
```

Pour confirmer la Connectivité directe de spoke-to-spoke, l'administrateur a besoin :

- Vérifiez qu'une session dynamique de spoke-to-spoke 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 secNotez que deux sessions sont disponibles : un rai-à-hub et un spoke-to-spoke.
```

- Vérifiez le 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::2La sortie prouve que 2001:DB8:1111:2200::/64 (le RÉSEAU LOCAL pour Spoke2) est disponible par l'intermédiaire de 2001:DB8:0:FFFE : : , qui est l'ipv6 addres négocié sur l'interface Tunnel1 pour Spoke2. L'interface Tunnel1 est disponible par l'intermédiaire de l'adresse à plusieurs accès de nonbroadcast (NBMA) de 2001:db8:0:200::2, qui est l'ipv6 addres assigné à Spoke2 statiquement.
```

- Vérifiez que le trafic passe par l'intermédiaire de 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 configurations de 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
```

Dépannez

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

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

Aide de ces commandes de débogage vous dépannez des questions :

- FlexVPN/IKEv2 et IPsec : **debug crypto ipsecdebug crypto ikev2 [paquet|interne]**
- NHRP (spoke-to-spoke) :
  - **paquet de debug nhrp**
  - **debug nhrp extension**
  - **cache de debug nhrp**
  - **artère de debug nhrp**

Référez-vous à la liste de commandes principale de Cisco IOS, toutes les releases pour plus d'informations sur ces commandes.