# FlexVPN: IPv6 in het configuratievoorbeeld van een hub en een dergelijke implementatie

## Inhoud



## Inleiding

Dit document beschrijft een gezamenlijke configuratie die een door Cisco IOS: FlexVPN gemaakte en een hub toepassing in een IPv6-omgeving gebruikt. Het programma breidt zich uit op de concepten die in FlexVPN worden besproken: IPv6 basis-LAN-configuratie.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS FlexVPN-module
- Routing protocollen

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco generatie 2 geïntegreerde services routers (ISR G2)
- Cisco IOS-softwarerelease 15.3 (of release 15.4T voor dynamische gesproken tunnels met IPv6)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Configureren

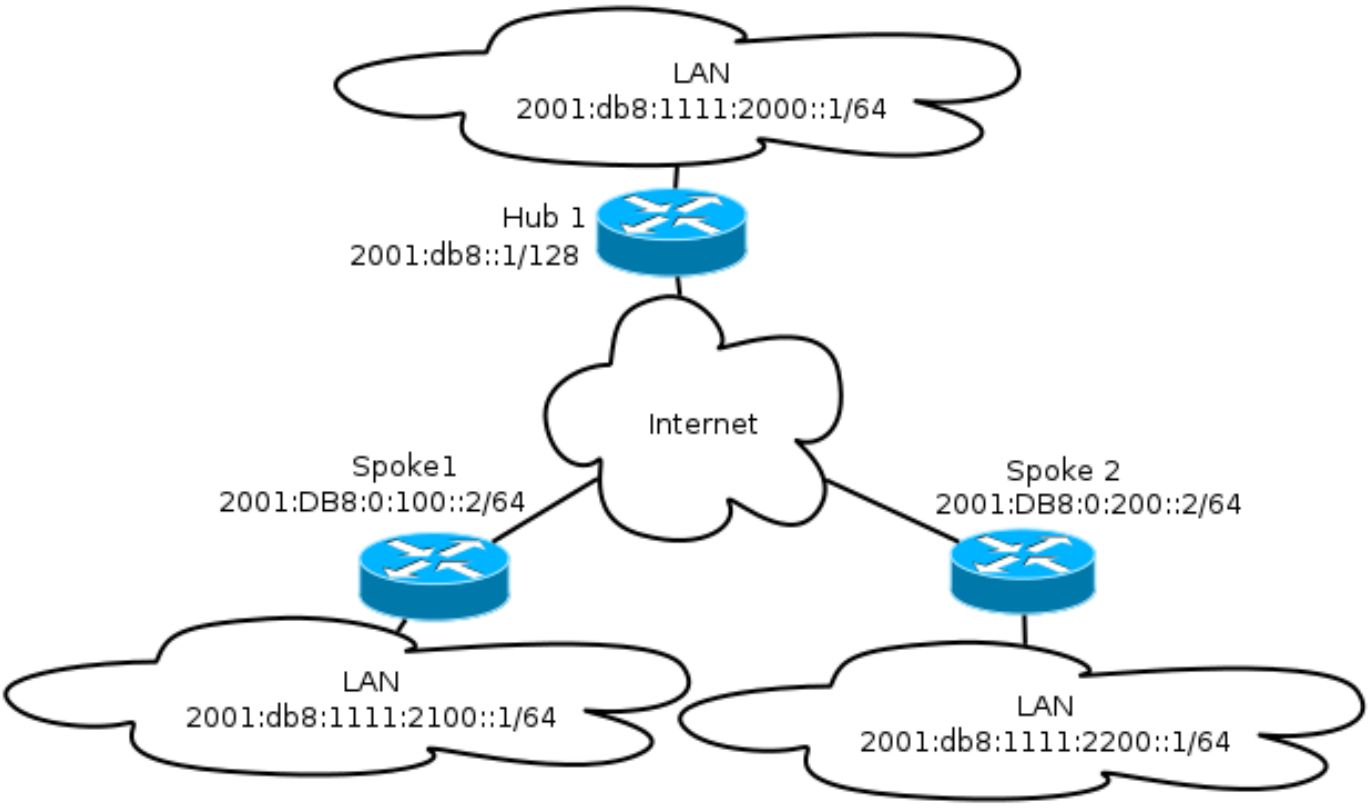
> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Terwijl dit configuratievoorbeeld en netwerkdiagram IPv6 als het transportnetwerk gebruiken, wordt de Generic Routing Encapsulation (GRE) normaal gebruikt in FlexVPN-implementaties. Met gebruik van GRE in plaats van IPsec kunnen beheerders IPv4 of IPv6 of beide via dezelfde tunnels uitvoeren, ongeacht het transportnetwerk.

## Netwerkdiagram

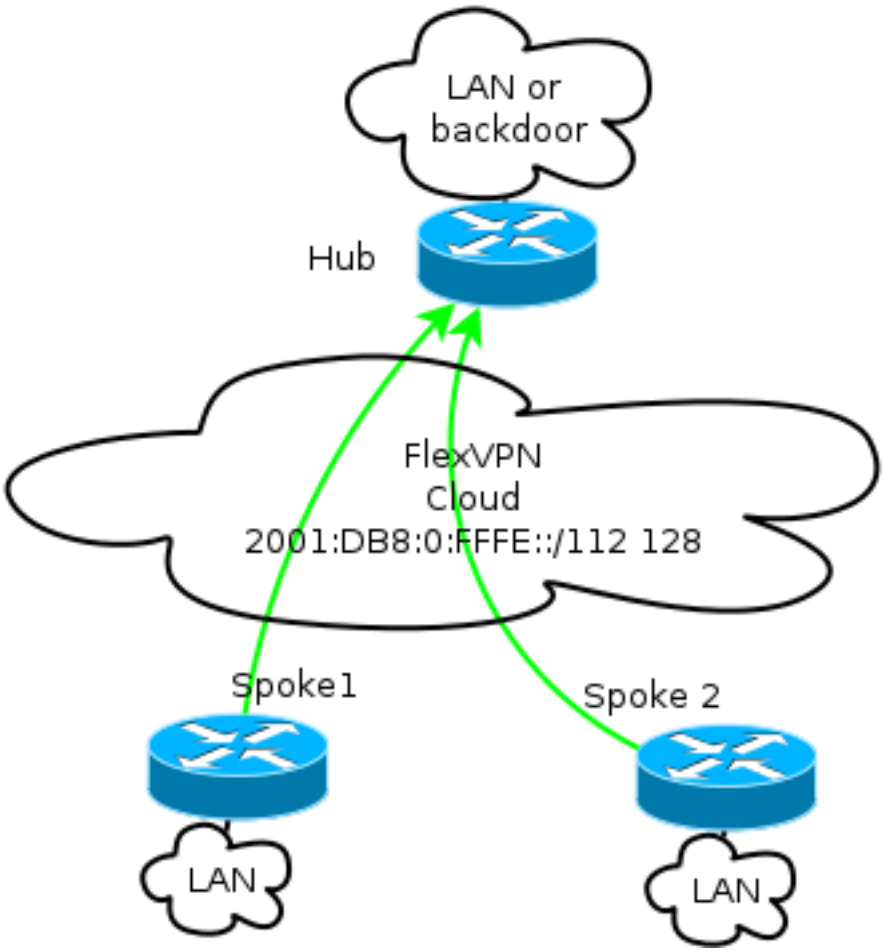
### transportnetwerk

Dit is een schema van het in dit voorbeeld gebruikte vervoersnet:



### Overlay-netwerk

Dit is een diagram van de basale overlay netwerktopologie die in dit voorbeeld wordt gebruikt:




Elke toespraak is toegewezen van een pool van adressen van /112, maar ontvangt een /128 adres. Aldus wordt de notatie '/112 128' gebruikt in IPv6 poolconfiguratie van de hub.

## Configuraties

Deze configuratie toont een IPv4- en IPv6-overlay die over een IPv6-backbone werkt.

In vergelijking met voorbeelden die IPv4 als backbone gebruiken, merk op dat u de opdracht **tunnelmodus** moet gebruiken om een verandering van knooppunt aan te brengen en IPv6-transport aan te passen.

De toespraak-aan-spits tunnelfunctie via IPv6 zal worden geïntroduceerd in Cisco IOS softwarerelease 15.4T, die nog niet beschikbaar is.

### Routing protocollen

Cisco raadt u aan om het Protocol van de Gateway (iBGP) intern te gebruiken voor het uitvoeren tussen gesproken en knooppunten voor grote implementaties omdat iBGP het meest schaalbare routingprotocol is.

Het BGP-bereik (Border Gateway Protocol) ondersteunt IPv6-bereik niet, maar het vereenvoudigt het gebruik met een IPv4-transport. Hoewel het haalbaar is om BGP in zulk een milieu te gebruiken, illustreert deze configuratie een basisvoorbeeld, zodat het Enhanced Interior Gateway Routing Protocol (DHCP) werd gekozen.

### Hub-configuratie

Vergeleken met oudere voorbeelden omvat deze configuratie het gebruik van nieuwe vervoersprotocollen.

Om de hub te configureren moet de beheerder:

- Eenvoudige routing inschakelen.
- Vervoersrouting.
- Verstrek een nieuwe pool van IPv6 adressen die dynamisch moet worden toegewezen. Het zwembad is 2001:DB8:0:FFFE::/112; 16 bits maken het mogelijk 65.535 apparaten aan te pakken .
- IPv6 inschakelen voor de NHRP-configuratie (Next Hop Resolutie Protocol) om IPv6 in de lay-out toe te staan.
- Account voor IPv6-adressering in de sleutelring en het profiel in de cryptoconfiguratie.

In dit voorbeeld, adverteert de hub een samenvatting Ecu aan alle woordjes.

Cisco adviseert geen gebruik van een overzichtsadres op de Virtual-Sjablooninterface in FlexVPN-implementatie; in een Dynamic Multipoint VPN (DMVPN) is dit echter niet alleen gebruikelijk, maar wordt dit ook als een goede praktijk beschouwd. Zie FlexVPN-migratie: Harde beweging van DMVPN naar FlexVPN op dezelfde apparaten: Bijgewerkt hubconfiguratie voor meer informatie.

```
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
```

## Spoelconfiguratie

Zoals in de hubconfiguratie moet de beheerder IPv6-adressering aanbieden, IPv6-routing mogelijk maken en NHRP en crypto-configuratie toevoegen.

Het is uitvoerbaar om wanneer u EHRM en andere routingprotocollen gebruikt voor spits-aan-spaak. In een typisch scenario zijn de protocollen echter niet nodig en kunnen ze gevolgen hebben voor schaalbaarheid en stabiliteit.

In dit voorbeeld, houdt de routerconfiguratie slechts nabijheid Ecu tussen het gesproken en de hub, en de enige interface die niet passief is de 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
```

Volg deze aanbevelingen wanneer u routeringsprotocollen op een gesproken gebied maakt:

1. Toestaan het routeringsprotocol om een relatie via de verbinding (in dit geval de interface Tunnel1) naar de hub in te stellen. Het is over het algemeen niet wenselijk om het routeren van nabijheid tussen woordjes te maken omdat dit de complexiteit in de meeste gevallen

aanzienlijk verhoogt.

2. Kunt u alleen lokale LAN-subformaten aankondigen en het routingprotocol op een IP-adres inschakelen dat door de hub is toegewezen. Wees voorzichtig met het niet adverteren van een groot netwerk omdat het invloed zou kunnen hebben op de communicatie met de persoon.

Dit voorbeeld weerspiegelt beide aanbevelingen voor EHW op 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
```

# Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

> Opmerking: De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

## Sessiebeheer tussen hub

Een goed gevormde sessie tussen gesproken en hub apparaten heeft een Toetsuitwisseling Versie 2 (IKEv2) die omhoog is en een routeringsprotocol heeft dat nabijheid kan maken. In dit voorbeeld, is het routingprotocol wanneer een NIS, zodat er twee opdrachten zijn aan het EHRM:

- **show crypto ikev2 sa**
- **toon ipv6 eigrp 65001 buurman**
- **zie ip eigrp 65001 buurland**

```
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
```

In IPv4 gebruikt DHCP een toegewezen IP adres om te leren; in het vorige voorbeeld, is het het hub IP adres van 10.1.1.1.

IPv6 gebruikt een link-lokaal adres; in dit voorbeeld is de hub FE80 : A8BB:CCFF:FE00:6600. Gebruik de opdracht **ping** om te verifiëren dat de hub door zijn link-lokale IP kan worden bereikt:

```
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
```

## Sessie-to-Spoke

'Spoke-to-sprak' sessies worden op verzoek dynamisch opgevoed. Gebruik een eenvoudig **ping**-opdracht om een sessie te starten:

```
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
```

Om direct een gesprek-aan-sprak connectiviteit te bevestigen, moet de beheerder:

- Controleer dat een dynamische gesproken-aan-gesproken sessie een nieuwe Virtual-Access-interface veroorzaakt:

```
%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
```

- Controleer de IKEv2 sessiestatus:

```
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
```

Merk op dat twee sessies beschikbaar zijn: één sprak met een speld en één sprak met een spaak.

- Controleer 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
```

De output laat zien dat 2001:DB8:111:200::/64 (het LAN voor Spoke2) beschikbaar is via 2001:DB8:0:FFFE:, het IPv6-adres dat via onderhandelingen tot stand is gebracht op de interface Tunnel1 voor Spoke2. De interface Tunnel1 is beschikbaar via de niet-uitzending-multitoegang NBMA)-adres van 2001:db8:0:200::2, het IPv6-adres dat op statische wijze aan Spoke2 is toegewezen.

- Controleer dat er verkeer via die interface verloopt:

```
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
(...)
```

- Controleer het routepad en de CEF-instellingen:

```
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
```

# Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

> Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Deze debug opdrachten helpen u problemen met uw probleemoplossing:

- FlexVPN/IKEv2 en IPsec: **crypto ipsec debugcrypto-encryptie ikev2 [pakje|inwendig]**
- NHRP (sprak-aan-sprak):
  - **debug-invoer**
  - **debug Nhrp-verlenging**
  - **debug Nhrp cache**
  - **terugdebug nhrp route**

Raadpleeg de Cisco IOS Master Opdracht List, Alle releases voor meer informatie over deze opdrachten.