FlexVPN: Konfigurationsbeispiel für die Bereitstellung von IPv6 in einem Hub-and-Spoke

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Transportnetz](#)
[Overlay-Netzwerk](#)
[Konfigurationen](#)
[Routing-Protokolle](#)
[Hub-Konfiguration](#)
[Spoke-Konfiguration](#)
[Überprüfen](#)
[Spoke-to-Hub-Sitzung](#)
[Spoke-to-Spoke-Sitzung](#)
[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt eine allgemeine Konfiguration, die eine Cisco IOS® FlexVPN Spoke- und Hub-Bereitstellung in einer IPv6-Umgebung verwendet. Sie erweitert die in [FlexVPN: IPv6-Basiskonfiguration für das LAN zu LAN](#) erörterten Konzepte.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco IOS FlexVPN
- Routing-Protokolle

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Integrated Services Router Generation 2 (ISR G2)
- Cisco IOS Software Release 15.3 (oder Release 15.4T für dynamische Spoke-to-Spoke-Tunnel mit IPv6)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

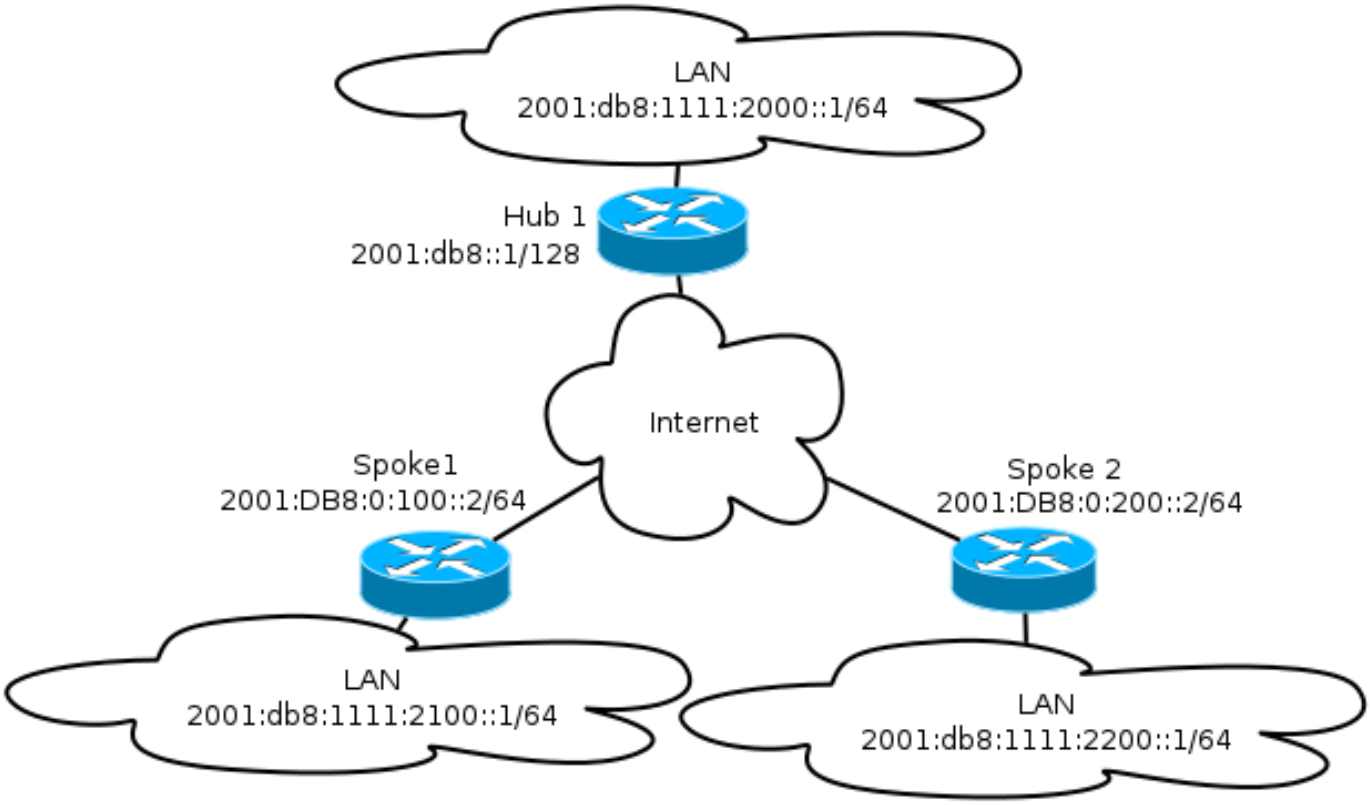
> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Während in diesem Konfigurationsbeispiel und Netzwerkdiagramm IPv6 als Transportnetzwerk verwendet wird, wird Generic Routing Encapsulation (GRE) in der Regel in FlexVPN-Bereitstellungen verwendet. Die Verwendung von GRE anstelle von IPsec ermöglicht es Administratoren, IPv4 oder IPv6 oder beides über dieselben Tunnel auszuführen, unabhängig vom Transportnetzwerk.

Netzwerkdiagramm

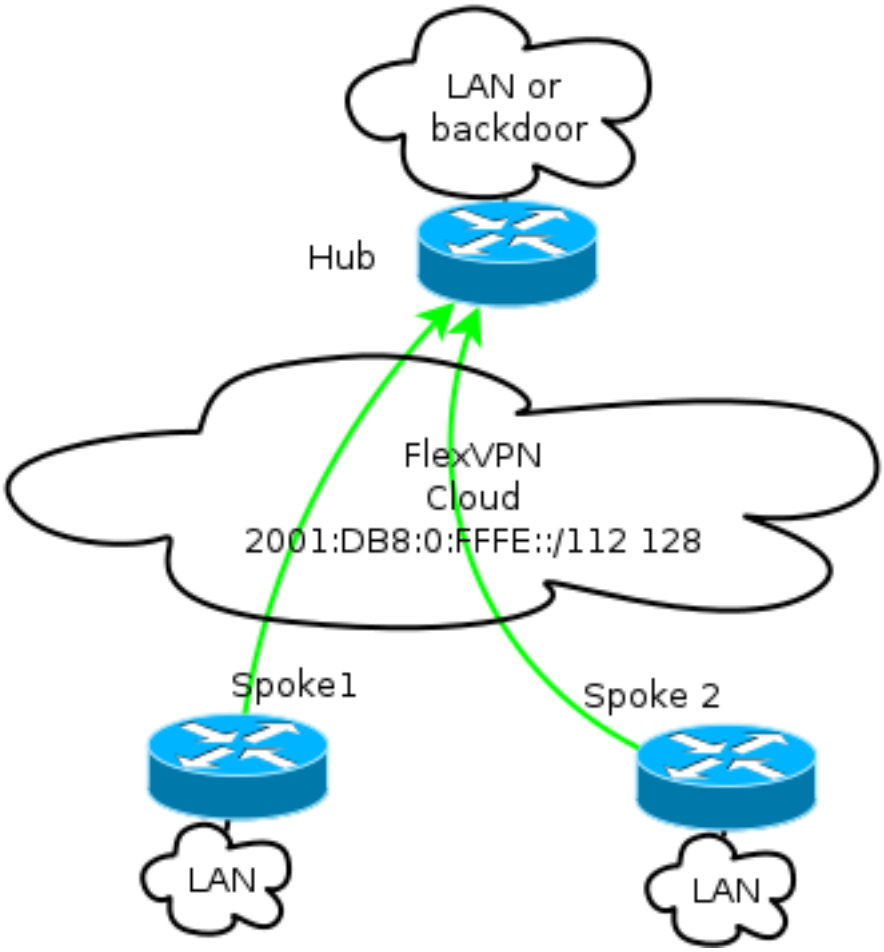
Transportnetz

Dies ist ein Diagramm des in diesem Beispiel verwendeten Transportnetzwerks:



Overlay-Netzwerk

Dies ist ein Diagramm der in diesem Beispiel verwendeten grundlegenden Overlay-Netzwerktopologie:



Jeder Spoke wird aus einem Adresspool von /112 zugewiesen, erhält aber eine /128-Adresse. So wird die Notation '/112 128' in der IPv6-Pool-Konfiguration des Hubs verwendet.

Konfigurationen

Diese Konfiguration zeigt ein IPv4- und IPv6-Overlay, das über einen IPv6-Backbone arbeitet.

Im Vergleich zu Beispielen, die IPv4 als Backbone verwenden, sollten Sie den Befehl **Tunnel-Modus** verwenden, um eine Knotenänderung durchzuführen und IPv6-Transport zu ermöglichen.

Die Spoke-to-Spoke-Tunnelfunktion über IPv6 wird in Version 15.4T der Cisco IOS-Software eingeführt, die noch nicht verfügbar ist.

Routing-Protokolle

Cisco empfiehlt die Verwendung des internen Border Gateway Protocol (iBGP) für das Peering zwischen Spoke- und Hubs bei großen Bereitstellungen, da iBGP das skalierbarste Routing-Protokoll ist.

Der Border Gateway Protocol (BGP)-Listen-Bereich unterstützt zwar den IPv6-Bereich nicht, vereinfacht jedoch die Verwendung bei einem IPv4-Transport. Obwohl BGP in einer solchen Umgebung verwendet werden kann, stellt diese Konfiguration ein einfaches Beispiel dar. Daher wurde das Enhanced Interior Gateway Routing Protocol (EIGRP) gewählt.

Hub-Konfiguration

Im Vergleich zu älteren Beispielen umfasst diese Konfiguration die Verwendung neuer Transportprotokolle.

Um den Hub zu konfigurieren, muss der Administrator:

- Aktivieren Sie Unicast-Routing.
- Bereitstellung von Transportrouting.
- Bereitstellung eines neuen Pools mit dynamisch zuzuweisenden IPv6-Adressen. Der Pool ist 2001:DB8:0:FFFE::/112; 16 Bit ermöglichen die Adressierung von 65.535 Geräten.
- Aktivieren Sie IPv6 für die NHRP-Konfiguration (Next Hop Resolution Protocol), um IPv6 im Overlay zu ermöglichen.
- Konto für IPv6-Adressierung im Keyring sowie im Profil in der Verschlüsselungskonfiguration.

In diesem Beispiel gibt der Hub allen Stationen eine EIGRP-Zusammenfassung bekannt.

Cisco rät von der Verwendung einer zusammengefassten Adresse auf der Virtual-Template-Schnittstelle in der FlexVPN-Bereitstellung ab. In einem Dynamic Multipoint VPN (DMVPN) ist dies jedoch nicht nur üblich, sondern gilt auch als Best Practice. Siehe FlexVPN-Migration: Hard Move from DMVPN to FlexVPN on same Devices: Aktualisierte Hub-Konfiguration für Details.

```
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
```

Spoke-Konfiguration

Wie bei der Hub-Konfiguration muss der Administrator IPv6-Adressierung bereitstellen, IPv6-Routing aktivieren und NHRP- und Krypto-Konfiguration hinzufügen.

EIGRP und andere Routing-Protokolle können für Spoke-to-Spoke-Peering verwendet werden. In einem typischen Szenario sind die Protokolle jedoch nicht erforderlich und können sich auf Skalierbarkeit und Stabilität auswirken.

In diesem Beispiel behält die Routing-Konfiguration nur die EIGRP-Adjacency zwischen dem Spoke- und dem Hub bei. Die einzige nicht passive Schnittstelle ist die Tunnel1-Schnittstelle:

```
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
```

Befolgen Sie diese Empfehlungen, wenn Sie Routing-Protokolleinträge in einem Spoke-System erstellen:

1. Lassen Sie zu, dass das Routing-Protokoll eine Beziehung über die Verbindung (in diesem Fall die Tunnel1-Schnittstelle) zum Hub herstellt. Generell ist es nicht wünschenswert, eine Routing-Adjacency zwischen Spokes einzurichten, da dies in den meisten Fällen die Komplexität erheblich erhöht.

2. Geben Sie nur lokale LAN-Subnetze an, und aktivieren Sie das Routing-Protokoll für eine vom Hub zugewiesene IP-Adresse. Achten Sie darauf, kein großes Subnetz anzukündigen, da dies die Spoke-to-Spoke-Kommunikation beeinträchtigen könnte.

Dieses Beispiel enthält beide Empfehlungen für EIGRP auf 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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

> **Hinweis**: Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Spoke-to-Hub-Sitzung

Eine ordnungsgemäß konfigurierte Sitzung zwischen Spoke- und Hub-Geräten verfügt über eine

IKEv2-Sitzung (Internet Key Exchange Version 2), die aktiviert ist, und über ein Routing-Protokoll, das eine Adjacency erstellen kann. In diesem Beispiel ist das Routing-Protokoll EIGRP. Es gibt also zwei EIGRP-Befehle:

- 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
```

In IPv4 verwendet EIGRP eine zugewiesene IP-Adresse für Peer. Im vorherigen Beispiel ist dies die Hub-IP-Adresse 10.1.1.1.

IPv6 verwendet eine lokale Adresse. in diesem Beispiel lautet der Hub FE80::A8BB:CCFF:FE00:6600. Verwenden Sie den Befehl **ping**, um zu überprüfen, ob der Hub über die lokale Link-IP erreicht werden kann:

```
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
```

Spoke-to-Spoke-Sitzung

Spoke-to-Spoke-Sitzungen werden bei Bedarf dynamisch aktiviert. Verwenden Sie einen einfachen **Ping-**Befehl, um eine Sitzung zu 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
```

Um die direkte Spoke-to-Spoke-Verbindung zu bestätigen, muss der Administrator:

- Überprüfen Sie, ob eine dynamische Spoke-to-Spoke-Sitzung eine neue Virtual-Access-Schnittstelle auslöst:

```
%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
```

- Überprüfen Sie den Status der IKEv2-Sitzung:

```
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
```

  Beachten Sie, dass zwei Sitzungen verfügbar sind: ein "Spoke-to-Hub" und ein "Spoke-to-Spoke".

- NHRP überprüfen:

```
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
```

  Die Ausgabe zeigt, dass 2001:DB8:111:2200::/64 (das LAN für Spoke2) ab 2001 verfügbar ist:DB8:0:FFFE::, die ausgehandelte IPv6-Adresse auf der Tunnel1-Schnittstelle für Spoke2. Die Tunnel1-Schnittstelle ist über die NBMA-Adresse 2001:db8:0:200:2 verfügbar, die der Spoke2 statisch zugewiesenen IPv6-Adresse entspricht.

- Überprüfen Sie, ob der Datenverkehr über diese Schnittstelle weitergeleitet wird:

```
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
(...)
```

- Überprüfen Sie den Routing-Pfad und die CEF-Einstellungen:

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

> **Hinweis**: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug**-Befehlen finden Sie unter Wichtige Informationen.

Diese Debugbefehle helfen Ihnen bei der Behebung von Problemen:

- FlexVPN/IKEv2 und IPsec: **debuggen crypto ipsecdebug crypto ikev2 [paket|internal]**
- NHRP (Spoke-to-Spoke):
  - **Debug-Paket**
  - **Debug Nhrp-Erweiterung**
  - **Debug-Nhrp-Cache**
  - **Debug-Nhrp-Route**

Weitere Informationen zu diesen Befehlen finden Sie in der Cisco IOS Master Command List, All Releases (Cisco IOS Master-Befehlsliste, Alle Versionen).