# Konfigurationsbeispiel für die Migration von DMVPN zu FlexVPN Soft

## Inhalt



## Einführung

Dieses Dokument beschreibt die Durchführung einer *Soft*-Migration, bei der sowohl Dynamic Multipoint VPN (DMVPN) als auch FlexVPN ohne Workaround gleichzeitig auf einem Gerät ausgeführt werden können, und enthält ein Konfigurationsbeispiel.

> **Hinweis**: Dieses Dokument behandelt die in der FlexVPN-Migration beschriebenen Konzepte: Umstieg von DMVPN auf FlexVPN auf denselben Geräten und FlexVPN-Migration: Harter Wechsel von DMVPN zu FlexVPN in Cisco Hub-Artikeln. Beide Dokumente beschreiben *harte* Migrationen, die während der Migration zu einer Unterbrechung des Datenverkehrs führen. Die Einschränkungen in diesen Artikeln sind auf einen Mangel an

Cisco IOS® Software zurückzuführen, der jetzt behoben wird.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- DMVPN
- FlexVPN

## Verwendete Komponenten

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

- Cisco Integrated Service Router (ISR) Version 15.3(3)M oder höher
- Cisco Aggregated Service Router (ASR1K) der Serie 1000, Version 3.10 oder höher

**Hinweis**: Nicht alle Software und Hardware unterstützt Internet Key Exchange Version 2 (IKEv2). Weitere Informationen finden Sie im Cisco Feature Navigator.

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.

# Hintergrundinformationen

Einer der Vorteile der neueren Cisco IOS-Plattform und -Software besteht in der Möglichkeit, Kryptografie der nächsten Generation zu verwenden. Ein Beispiel hierfür ist die Verwendung des Advanced Encryption Standard (AES) im Galois/Counter Mode (GCM) für die Verschlüsselung in IPsec, wie in RFC 4106 beschrieben. AES GCM ermöglicht eine wesentlich schnellere Verschlüsselung einiger Hardware.

**Hinweis**: Weitere Informationen zur Verwendung von und Migration zur Verschlüsselung der nächsten Generation finden Sie im Cisco Verschlüsselungsartikel der nächsten Generation.

# Konfigurieren

Dieses Konfigurationsbeispiel konzentriert sich auf die Migration von einer DMVPN Phase 3-Konfiguration zu einem FlexVPN, da beide Designs ähnlich funktionieren.

| DMVPN Phase 2 | DMVPN Phase 3 | FlexVPN |
|---|---|---|

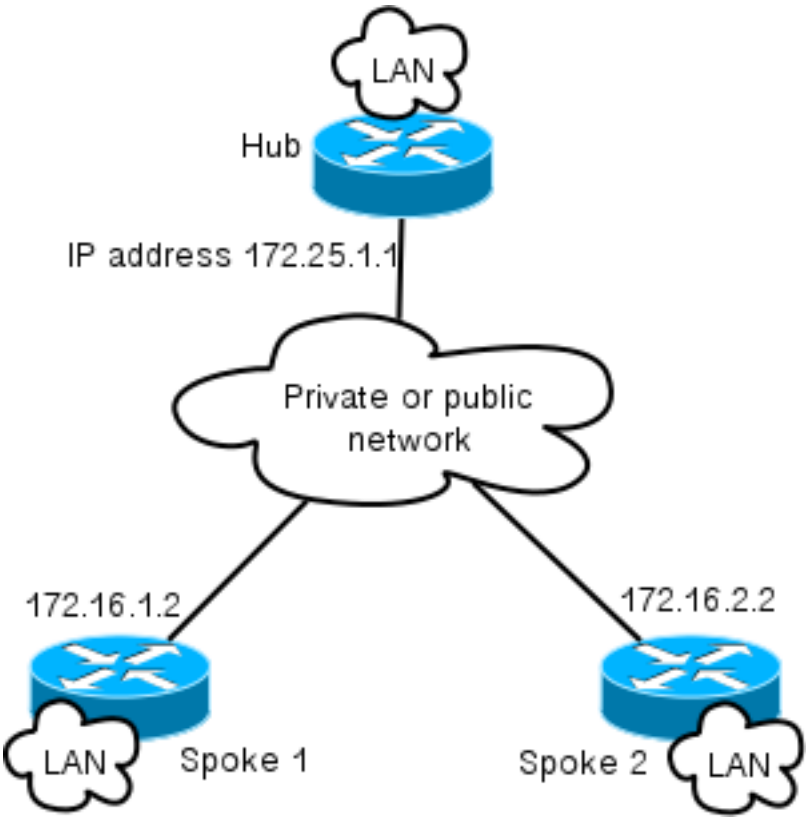
| | | | |
|---|---|---|---|
| **Transport** | GRE über IPsec | GRE über IPsec | GRE über IPsec, VTI |
| **NHRP-Nutzung** | Registrierung und Auflösung | Registrierung und Auflösung | Auflösung |
| **Nächster Hop von Spoke** | Andere Spokes oder Hub | Zusammenfassung aus Hub | Zusammenfassung au Hub |
| **NHRP Shortcut Switching** | Nein | Ja | Ja (optional) |
| **NHRP-Umleitung** | Nein | Ja | Ja |
| **IKE und IPsec** | IPsec optional, IKEv1 typisch | IPsec optional, IKEv1 typisch | IPsec, IKEv2 |

## Netzwerkdiagramme

Dieser Abschnitt enthält sowohl Transport- als auch Overlay-Netzwerkdiagramme.

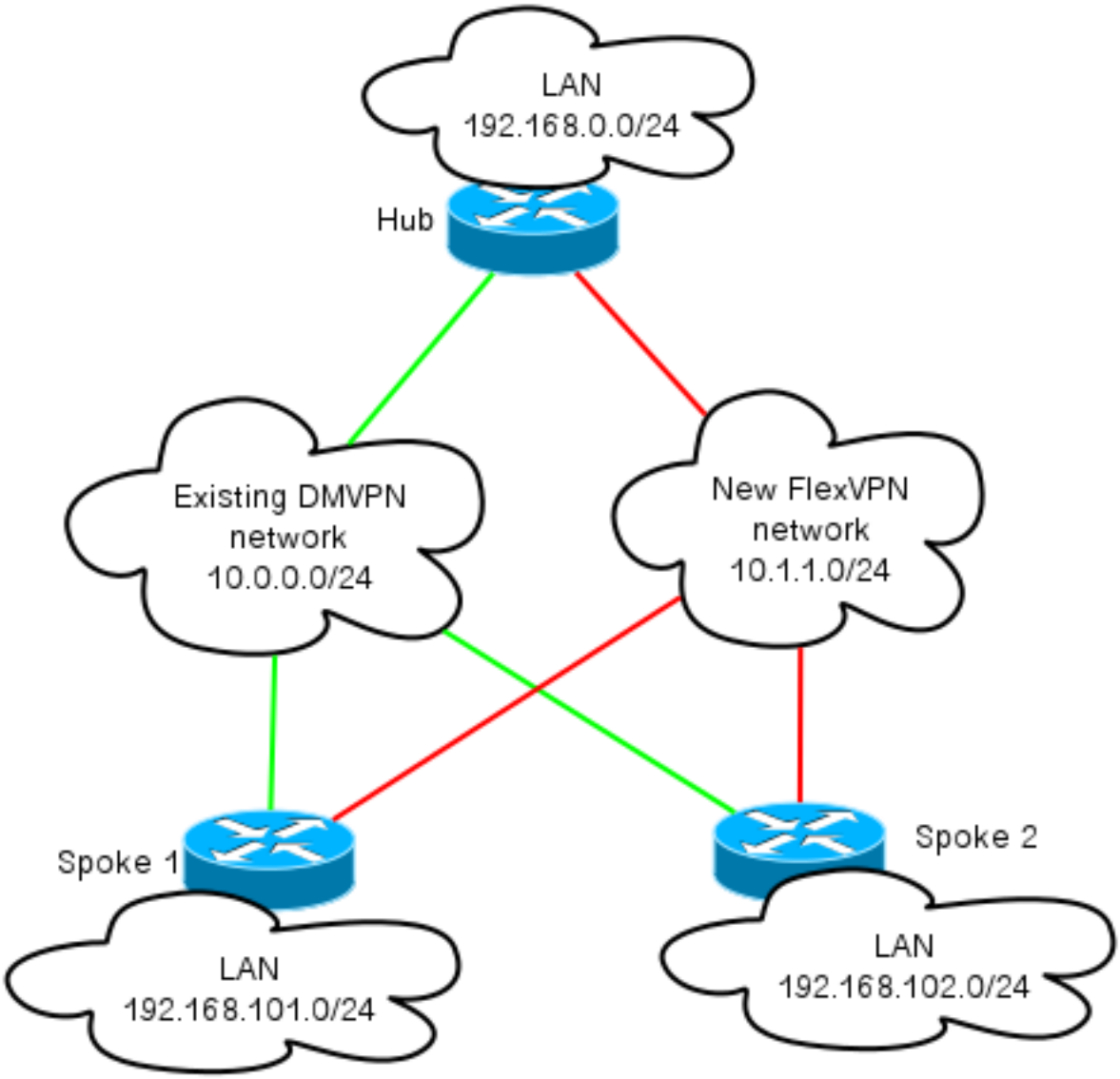
### Transportnetzwerkdiagramm

Das in diesem Beispiel verwendete Transportnetzwerk umfasst einen einzelnen Hub mit zwei verbundenen Spokes. Alle Geräte sind über ein Netzwerk verbunden, das das Internet simuliert.




### Overlay-Netzwerkdiagramm

Das in diesem Beispiel verwendete Overlay-Netzwerk umfasst einen einzelnen Hub mit zwei verbundenen Stationen. Denken Sie daran, dass sowohl DMVPN als auch FlexVPN gleichzeitig aktiv sind, dass jedoch unterschiedliche IP-Adressbereiche verwendet werden.




## Konfigurationen

Diese Konfiguration migriert die beliebteste Bereitstellung von DMVPN Phase 3 über das Enhanced Interior Gateway Routing Protocol (EIGRP) auf FlexVPN mit Border Gateway Protocol (BGP). Cisco empfiehlt die Verwendung von BGP mit FlexVPN, da die Skalierung von Bereitstellungen verbessert wird.

> **Hinweis**: Der Hub beendet die IKEv1 (DMVPN)- und IKEv2 (FlexVPN)-Sitzungen mit derselben IP-Adresse. Dies ist nur mit den neuesten Cisco IOS-Versionen möglich.

### Spoke-Konfiguration

Dies ist eine sehr einfache Konfiguration mit zwei bemerkenswerten Ausnahmen, die den Betrieb von IKEv1 und IKEv2 sowie von zwei Frameworks ermöglichen, die Generic Routing Encapsulation (GRE) über IPsec für den Transport verwenden, um gleichzeitig vorhanden zu sein.

> **Hinweis**: Die relevanten Änderungen an der Konfiguration von Internet Security Association und Key Management Protocol (ISAKMP) und IKEv2 werden fett dargestellt.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport

crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
 tunnel key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub 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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS Release 15.3 ermöglicht die Verknüpfung von IKEv2- und ISAKMP-Profilen in einer *Tunnelschutzkonfiguration*. Neben einigen internen Codeänderungen können IKEv1 und IKEv2 auf demselben Gerät gleichzeitig ausgeführt werden.

Aufgrund der Art, wie Cisco IOS die Profile (IKEv1 oder IKEv2) in Veröffentlichungen vor 15.3 auswählt, führte dies zu einigen Vorbehalten, z. B. Situationen, in denen IKEv1 über den Peer auf IKEv2 initiiert wird. Die Trennung von IKE basiert nun auf Profilebene und nicht auf Schnittstellenebene, was über die neue CLI erreicht wird.

Ein weiteres Upgrade der neuen Cisco IOS-Version ist das Hinzufügen des *Tunnelschlüssels*. Dies ist erforderlich, da DMVPN und FlexVPN dieselbe Quellschnittstelle und dieselbe Ziel-IP-Adresse verwenden. Damit kann der GRE-Tunnel nicht wissen, welche Tunnelschnittstelle zum Entkapseln von Datenverkehr verwendet wird. Mit dem Tunnel-Schlüssel können Sie **tunnel0** und **tunnel1** mit einem kleinen (4 Byte) Overhead voneinander unterscheiden. Auf beiden Schnittstellen kann ein anderer Schlüssel konfiguriert werden. In der Regel müssen Sie jedoch nur einen Tunnel differenzieren.

> **Hinweis**: Wenn DMVPN und FlexVPN dieselbe Schnittstelle gemeinsam nutzen, ist die Option zum gemeinsamen Tunnelschutz nicht erforderlich.

Daher ist die Konfiguration des Spoke-Routing-Protokolls grundlegend. EIGRP und BGP arbeiten separat. EIGRP kündigt nur über die Tunnelschnittstelle an, um Peering über Spoke-to-Spoke-Tunnel zu vermeiden, was die Skalierbarkeit einschränkt. BGP unterhält nur eine Beziehung zum Hub-Router (**10.1.1.1**), um das lokale Netzwerk anzukündigen (**192.168.101.0/24**).

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
```

### Hub-Konfiguration

Sie müssen ähnliche Änderungen an der Konfiguration für den Hub vornehmen, wie sie im Abschnitt **Spoke-Konfiguration** beschrieben sind.

> **Hinweis**: Die relevanten Änderungen an der ISAKMP- und IKEV2-Konfiguration werden fett dargestellt.

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
 ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
```

```
 tunnel protection ipsec profile default
```

Auf der Hub-Seite erfolgt die Bindung zwischen dem IKE-Profil und dem IPsec-Profil auf Profilebene, anders als bei der Spoke-Konfiguration, wo diese über den Befehl **Tunnelschutz** abgeschlossen wird. Beide Ansätze sind praktikable Methoden, um diese Bindung abzuschließen.

Es ist zu beachten, dass die NHRP-Netzwerk-IDs (Next Hop Resolution Protocol) für DMVPN und FlexVPN in der Cloud unterschiedlich sind. In den meisten Fällen ist es unerwünscht, wenn NHRP eine einzige Domäne über beide Frameworks erstellt.

Der Tunnelschlüssel differenziert DMVPN- und FlexVPN-Tunnel auf GRE-Ebene, um dasselbe Ziel zu erreichen, das im Abschnitt **Spoke Configuration** (**Spoke-Konfiguration)** beschrieben wird.

Die Routing-Konfiguration auf dem Hub ist recht einfach. Das Hub-Gerät unterhält zwei Beziehungen zu einem beliebigen Spoke-Gerät: eine, die EIGRP verwendet, und eine, die BGP verwendet. Die BGP-Konfiguration verwendet den Listen-Bereich, um eine langwierige Konfiguration pro Spoke zu vermeiden.

Die zusammengefassten Adressen werden zweimal vorgestellt. Die EIGRP-Konfiguration sendet eine Zusammenfassung mithilfe der **tunnel0-**Konfiguration (IP summary-address EIGRP 100), und das BGP führt eine Zusammenfassung mit der Aggregat-Adresse ein. Die Zusammenfassungen sind erforderlich, um sicherzustellen, dass die NHRP-Umleitung erfolgt, und um die Routing-Updates zu vereinfachen. Sie können eine NHRP-Umleitung senden (ähnlich einer ICMP-Umleitung (Internet Control Message Protocol)), die angibt, ob ein besserer Hop für ein bestimmtes Ziel vorhanden ist, wodurch ein Spoke-to-Spoke-Tunnel erstellt werden kann. Diese Zusammenfassungen werden auch verwendet, um die Anzahl der Routing-Updates zu minimieren, die zwischen Hub und Spoke gesendet werden. Dies ermöglicht eine bessere Skalierung von Konfigurationen.

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0

router bgp 65001
bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
```

# Überprüfen

Die Überprüfung für dieses Konfigurationsbeispiel ist in mehrere Abschnitte unterteilt.

## Prüfungen vor der Migration

Da sowohl DMVPN/EIGRP als auch FlexVPN/BGP gleichzeitig arbeiten, müssen Sie überprüfen, ob die Spoke eine Beziehung über IPsec zu IKEv1 und IKEv2 unterhält und dass die entsprechenden Präfixe über EIGRP und BGP gelernt werden.

In diesem Beispiel zeigt Spoke1, dass zwei Sitzungen mit dem Hub-Router aufrechterhalten werden. einer verwendet IKEv1/Tunnel0 und einer verwendet IKEv2/Tunnel1.

> **Hinweis**: Für jeden Tunnel werden zwei IPsec Security Associations (SAs) (ein eingehender und ein ausgehender) verwaltet.

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Wenn Sie die Routing-Protokolle überprüfen, müssen Sie sicherstellen, dass eine Nachbarschaft gebildet wird und dass die richtigen Präfixe gelernt werden. Dies wird zuerst mit dem EIGRP überprüft. Stellen Sie sicher, dass der Hub als Nachbar angezeigt wird und dass die 192.168.0.0/16-Adresse (die Zusammenfassung) vom Hub aus erfasst wird:

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0
P 192.168.0.0/16, 1 successors, FD is 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

Überprüfen Sie anschließend das BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
```

```
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

Die Ausgabe zeigt, dass die Hub-FlexVPN-IP-Adresse (10.1.1.1) ein Nachbar ist, über den die Spoke ein Präfix (192.168.0.0/16) empfängt. Darüber hinaus informiert das BGP den Administrator, dass ein Fehler in der Routing Information Base (RIB) für das Präfix 192.168.0.0/16 aufgetreten ist. Dieser Fehler tritt auf, weil für dieses Präfix eine bessere Route existiert, die bereits in der Routing-Tabelle vorhanden ist. Diese Route wird von EIGRP generiert und kann anhand der Routing-Tabelle bestätigt werden.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

## Migration

Im vorherigen Abschnitt wurde überprüft, ob sowohl die IPsec- als auch die Routing-Protokolle konfiguriert wurden und wie erwartet funktionieren. Eine der einfachsten Möglichkeiten für die Migration von DMVPN zu FlexVPN auf demselben Gerät besteht darin, die administrative Distanz (AD) zu ändern. In diesem Beispiel hat das interne BGP (iBGP) ein AD von 200 und das EIGRP ein AD von 90.

Damit der Datenverkehr ordnungsgemäß durch das FlexVPN fließen kann, muss das BGP über eine bessere AD-Schnittstelle verfügen. In diesem Beispiel wird die EIGRP-AD für interne und externe Routen auf 230 bzw. 240 geändert. Dadurch wird das BGP-AD (von 200) für das Präfix 192.168.0.0/16 besser vorzuziehen.

Eine weitere Methode, um dies zu erreichen, ist die Verringerung des BGP AD. Das Protokoll, das nach der Migration ausgeführt wird, hat jedoch andere, nicht standardmäßige Werte, die sich auf andere Teile der Bereitstellung auswirken können.

In diesem Beispiel wird der Befehl debug ip routing verwendet, um den Betrieb auf dem Spoke zu überprüfen.

> Hinweis: Wenn die Informationen in diesem Abschnitt in einem Produktionsnetzwerk verwendet werden, vermeiden Sie die Verwendung von Debugbefehlen, und verlassen Sie sich auf die Befehle zum Anzeigen, die im nächsten Abschnitt aufgeführt sind. Außerdem muss der Spoke-EIGRP-Prozess die Adjacency zum Hub wiederherstellen.

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

In dieser Ausgabe sind drei wichtige Maßnahmen zu beachten:

- Das Spoke bemerkt, dass das AD geändert wurde, und deaktiviert die Adjacency.
- In der Routing-Tabelle wird das EIGRP-Präfix eingestellt, und das BGP wird eingeführt.
- Die Adjacency zum Hub über das EIGRP wird wieder online gestellt.

Wenn Sie das AD auf einem Gerät ändern, wirkt sich dies nur auf den Pfad vom Gerät zu den anderen Netzwerken aus. Es hat keinen Einfluss darauf, wie andere Router das Routing durchführen. Nachdem beispielsweise die EIGRP-Entfernung auf Spoke1 erhöht wurde (und FlexVPN in der Cloud verwendet wird, um Datenverkehr weiterzuleiten), verwaltet der Hub die konfigurierten (Standard-)ADs. Dies bedeutet, dass DMVPN verwendet wird, um den Datenverkehr zurück zu Spoke1 zu leiten.

In bestimmten Szenarien kann dies zu Problemen führen, z. B. wenn Firewalls Datenrückverkehr auf derselben Schnittstelle erwarten. Daher sollten Sie das AD in allen Spokes ändern, bevor Sie es auf dem Hub ändern. Der Datenverkehr wird von FlexVPN erst vollständig migriert, nachdem er abgeschlossen ist.

## EIGRP-zu-EIGRP-Migration

Eine Migration von DMVPN zu FlexVPN, bei der nur EIGRP ausgeführt wird, wird in diesem Dokument nicht detailliert beschrieben. Es wird jedoch hier aus Gründen der Vollständigkeit erwähnt.

Es ist möglich, DMVPN und EIGRP derselben EIGRP-AS-Routing-Instanz (Autonomous System) hinzuzufügen. Damit wird die Routing-Adjacency für beide Cloud-Typen eingerichtet. Dies kann zu einem Lastenausgleich führen, der in der Regel nicht empfohlen wird.

Um sicherzustellen, dass entweder FlexVPN oder DMVPN ausgewählt wird, kann ein Administrator pro Schnittstelle verschiedene Delay-Werte zuweisen. Es ist jedoch zu beachten, dass keine Änderungen an den Schnittstellen virtueller Vorlagen möglich sind, während entsprechende Schnittstellen für den virtuellen Zugriff vorhanden sind.

## Prüfungen nach der Migration

Ähnlich wie bei dem im Abschnitt **Prüfungen vor der Migration** verwendeten Prozess müssen das IPsec-Protokoll und das Routing-Protokoll überprüft werden.

Überprüfen Sie zunächst die IPsec:

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Wie zuvor werden zwei Sitzungen angezeigt, von denen beide über zwei aktive IPsec-SAs verfügen.

Auf dem Spoke-System zeigt die aggregierte Route (**192.168.0.0/16**) vom Hub und wird über das BGP erfasst.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

Ebenso muss das Spoke-LAN, dem der Hub vorangestellt wird, über das EIGRP bekannt sein. In diesem Beispiel wird das **Spoke2**-LAN-Subnetz aktiviert:

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
```

```
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

In der Ausgabe wird der Weiterleitungspfad korrekt aktualisiert und zeigt aus einer virtuellen Zugriffsschnittstelle.

## Weitere Überlegungen

In diesem Abschnitt werden einige zusätzliche wichtige Bereiche beschrieben, die für dieses Konfigurationsbeispiel relevant sind.

### Vorhandene Spoke-to-Spoke-Tunnel

Bei einer Migration von EIGRP zum BGP sind die Spoke-to-Spoke-Tunnel nicht betroffen, da das Shortcut-Switching noch in Betrieb ist. Shortcut-Switching auf den Spoke-Systemen fügt eine spezifischere NHRP-Route mit einem AD von 250 ein.

Hier ein Beispiel für eine solche Route:

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

### Kommunikation zwischen migrierten und nicht migrierten Spokes

Wenn ein Spoke, der sich bereits in einem FlexVPN/BGP befindet, mit einem Gerät kommunizieren möchte, für das der Migrationsprozess noch nicht begonnen hat, fließt der Datenverkehr immer über den Hub.

Dies ist der Vorgang, der stattfindet:

1. Das Spoke führt eine Route-Suche für das Ziel durch, die über eine zusammengefasste Route zeigt, die vom Hub angekündigt wird.
2. Das Paket wird an den Hub gesendet.
3. Der Hub empfängt das Paket und führt eine Routensuche für das Ziel durch, die auf eine andere Schnittstelle zeigt, die Teil einer anderen NHRP-Domäne ist.

   **Hinweis**: Die NHRP-Netzwerk-ID in der vorherigen Hub-Konfiguration ist für FlexVPN und DMVPN unterschiedlich.

Selbst wenn die NHRP-Netzwerk-IDs vereinheitlicht sind, kann ein Problem auftreten, wenn die migrierten Spoke-Router Objekte über das FlexVPN-Netzwerk weiterleiten. Dazu gehört auch die Direktive, die zum Konfigurieren von Verknüpfungen-Switching verwendet wird. Die nicht migrierten Spoke-Router versuchen, Objekte über das DMVPN-Netzwerk auszuführen, wobei das spezifische Ziel darin besteht, Verknüpfungs-Switching auszuführen.

# Fehlerbehebung

In diesem Abschnitt werden die beiden Kategorien beschrieben, die normalerweise zur Fehlerbehebung bei der Migration verwendet werden.

## Probleme bei der Einrichtung von Tunneln

Gehen Sie wie folgt vor, wenn die IKE-Aushandlung fehlschlägt:

1. Überprüfen Sie den aktuellen Status mit den folgenden Befehlen:

   **show crypto isakmp sa** - Dieser Befehl gibt die Menge, die Quelle und das Ziel einer IKEv1-Sitzung an.**show crypto ipsec sa**: Dieser Befehl zeigt die Aktivität von IPsec-SAs an.**Hinweis**: Im Gegensatz zu IKEv1 wird in dieser Ausgabe der Wert für die Perfect Forward Secrecy (PFS) Diffie-Hellman (DH)-Gruppe als **PFS (Y/N)** angezeigt**: N, DH-Gruppe:** während der ersten Tunnelverhandlung **keine**; Nach einem erneuten Auftreten werden jedoch die korrekten Werte angezeigt. Dies ist kein Fehler, obwohl das Verhalten in CSCug67056 beschrieben wird. Der Unterschied zwischen IKEv1 und IKEv2 besteht darin, dass die untergeordneten SAs im Rahmen des **AUTH-**Austauschs erstellt werden. Die DH-Gruppe, die unter der Crypto Map konfiguriert wird, wird nur während eines rekey-Vorgangs verwendet. Aus diesem Grund sehen Sie **PFS (J/N): N, DH-Gruppe: keine bis zum ersten Wiederaufflammen.** Bei IKEv1 wird ein anderes Verhalten angezeigt, da die untergeordnete SA-Erstellung während des Schnellmodus erfolgt und die **CREATE_CHILD_SA-**Nachricht Rückstellungen für die Übertragung der Key Exchange-Payload enthält, die die DH-Parameter angibt, um einen neuen gemeinsamen geheimen Schlüssel abzuleiten.**show crypto ikev2 sa** - Dieser Befehl stellt eine Ausgabe bereit, die dem ISAKMP ähnelt, jedoch spezifisch für IKEv2 ist.**show crypto session** - Dieser Befehl stellt die Zusammenfassung der kryptografischen Sitzungen auf diesem Gerät bereit.**show crypto socket** - Dieser Befehl zeigt den Status von Krypto-Sockets an.**show crypto map** - Dieser Befehl zeigt die Zuordnung von IKE- und IPsec-Profilen zu den Schnittstellen.**show ip nhrp** - Dieser Befehl stellt die NHRP-Informationen vom Gerät bereit. Dies eignet sich für Spoke-to-Spoke-Verbindungen in FlexVPN-Konfigurationen sowie für Spoke-to-Spoke- und Spoke-to-Hub-Bindungen in DMVPN-Konfigurationen.
2. Verwenden Sie diese Befehle, um die Tunneleinrichtung zu debuggen:

   **debuggen crypto ikev2debuggen crypto isakmpdebuggen crypto ipseccrypto kmi debuggen**

## Probleme bei der Weiterleitung

Hier sind einige nützliche Befehle, die Sie zur Fehlerbehebung für das EIGRP und die Topologie verwenden können:

- **show bgp summary** - Verwenden Sie diesen Befehl, um die angeschlossenen Nachbarn und deren Status zu überprüfen.
- **show ip eigrp neighbor** - Verwenden Sie diesen Befehl, um die Nachbarn anzuzeigen, die über EIGRP verbunden sind.
- **show bgp**: Verwenden Sie diesen Befehl, um die über das BGP erfassten Präfixe zu überprüfen.
- **show ip eigrp topology** - Verwenden Sie diesen Befehl, um die über EIGRP gelernten Präfixe anzuzeigen.

Es ist wichtig zu wissen, dass sich ein gelerntes Präfix von einem Präfix unterscheidet, das in der Routing-Tabelle installiert ist. Weitere Informationen hierzu finden Sie im Artikel Routing Selection in Cisco Routers Cisco oder im Routing TCP/IP Cisco Press Book.

## Bekannte Einwände

Auf dem ASR1K gibt es eine Einschränkung, die die GRE-Tunnelbehandlung vergleicht. Dies wird unter der Cisco Bug-ID CSCue00443 nachverfolgt. Zu diesem Zeitpunkt enthält die Einschränkung eine geplante Korrektur in Version 3.12 der Cisco IOS XE-Software.

Überwachen Sie diesen Fehler, wenn Sie eine Benachrichtigung wünschen, sobald die Behebung verfügbar ist.