Konfigurationsbeispiel für FlexVPN Spoke in redundantem Hub-Design mit FlexVPN-Client-Baustein

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Spoke-Sitzung in einem FlexVPN-Netzwerk mithilfe des FlexVPN-Client-Konfigurationsblocks in einem Szenario konfiguriert wird, in dem mehrere Hubs verfügbar sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FlexVPN
- Cisco Routing-Protokolle

Verwendete Komponenten

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

- Cisco Integrated Service Router der G2-Serie (ISR)
- Cisco IOS® Version 15.2M

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

Aus Redundanzgründen muss ein Spoke-System möglicherweise mit mehreren Hubs verbunden werden. Redundanz auf der Spoke-Seite ermöglicht einen unterbrechungsfreien Betrieb ohne Single Point of Failure auf der Hub-Seite.

Die zwei häufigsten redundanten FlexVPN-Hub-Designs, die die Spoke-Konfiguration verwenden, sind:

- **Dual-Cloud-Ansatz**, bei dem ein Spoke-System über zwei separate Tunnel verfügt, die jeweils für beide Hubs aktiv sind.
- **Failover-Ansatz**, bei dem ein Spoke-System zu einem bestimmten Zeitpunkt über einen aktiven Tunnel mit einem Hub verfügt.

Beide Ansätze haben einen einzigartigen Satz von Vor- und Nachteilen.

Ansatz	Vorteile	Verbindungen
Duale Cloud	• Schnellere Wiederherstellung bei einem Ausfall auf Basis von Routing-Protokoll-Timern • Mehr Möglichkeiten zur Verteilung des Datenverkehrs zwischen Hubs, da die Verbindungen zu beiden Hubs aktiv sind	• Spoke führt die Sitzung mit beiden Hub gleichzeitig durch, wodurch Ressourcer beiden Hubs beansprucht werden.
Failover	• Einfache Konfiguration - integriert in FlexVPN • Verlässt sich bei einem Ausfall nicht auf ein Routing-Protokoll	• Langsamere Wiederherstellungszeit - basierend auf Dead Peer Detection (DF oder (optional) Objektverfolgung • Der gesamte Datenverkehr muss zu ein Hub nach dem anderen geleitet werden

Dieses Dokument beschreibt den zweiten Ansatz.

Konfigurieren

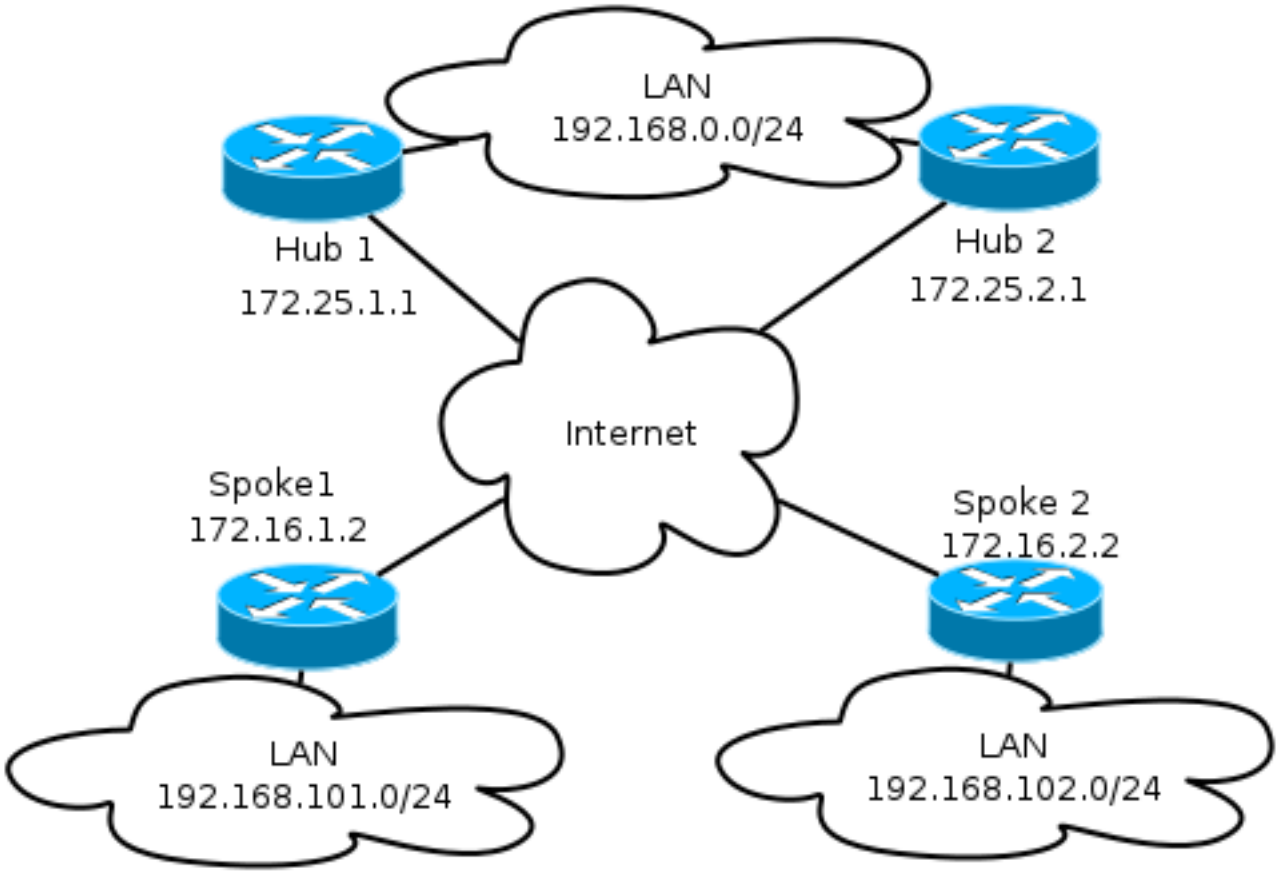
Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramme

Diese Diagramme zeigen sowohl die Transport- als auch die Overlay-Topologiediagramme.

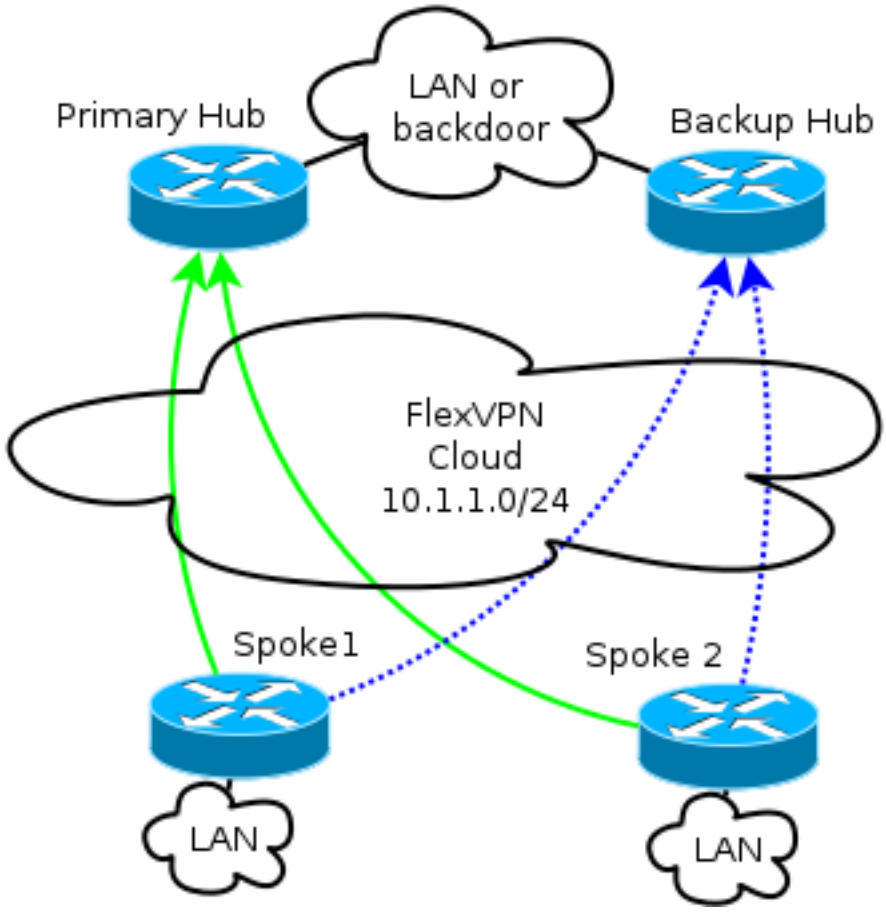
Transportnetz

Dieses Diagramm zeigt das grundlegende Transportnetzwerk, das normalerweise in FlexVPN-Netzwerken verwendet wird.



Overlay-Netzwerk

Dieses Diagramm zeigt das Overlay-Netzwerk mit logischer Konnektivität, die zeigt, wie das Failover funktionieren soll. Während des normalen Betriebs pflegen Spoke 1 und Spoke 2 nur eine Beziehung zu einem Hub.



Hinweis: Im Diagramm zeigen die durchgehenden grünen Linien die Verbindung und die Richtung der primären Internet Key Exchange Version 2 (IKEv2)/Flex-Sitzungen an. Die blau gestrichenen Linien zeigen die Sicherungsverbindung an, falls die Internet Key Exchange (IKE)-Sitzung zum primären Hub ausfällt.

Die **/24-**Adressierung stellt den Pool der für diese Cloud reservierten Adressen dar und nicht die tatsächliche Schnittstellenadressierung. Der Grund hierfür ist, dass der FlexVPN-Hub in der Regel eine dynamische IP-Adresse für die Spoke-Schnittstelle zuweist und sich auf Routen stützt, die dynamisch über Routen-Befehle im FlexVPN-Autorisierungsblock eingefügt wurden.

Grundkonfiguration von Spoke und Hub

Die grundlegende Konfiguration des "Hub and Spoke" basiert auf den Migrationsdokumenten von Dynamic Multipoint VPN (DMVPN) zu FlexVPN. Diese Konfiguration wird in der FlexVPN-Migration beschrieben: Artikel zum Hard Move from DMVPN to FlexVPN on same Devices.

Spoke-Konfigurationsanpassung

Spoke-Konfiguration - Client-Konfigurationsblock

Die Spoke-Konfiguration muss durch den Client-Konfigurationsblock erweitert werden.

In der Basiskonfiguration werden mehrere Peers angegeben. Der Peer mit der höchsten Präferenz

(niedrigste Zahl) wird vor anderen berücksichtigt.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

Die Tunnelkonfiguration muss geändert werden, damit das Tunnelziel basierend auf dem FlexVPN-Client-Konfigurationsblock dynamisch ausgewählt werden kann.

```
interface Tunnel1
 tunnel destination dynamic
```

Der FlexVPN-Client-Konfigurationsblock ist unbedingt an eine Schnittstelle gebunden und nicht an das IKEv2- oder IPsec-Profil.

Der Client-Konfigurationsblock bietet mehrere Optionen, um die Failover-Zeit und die Vorgänge anzupassen. Dazu gehören die Verwendung von Verfolgungsobjekten, die Wählsicherung und die Funktionen von Sicherungsgruppen.

Bei der Basiskonfiguration stützt sich der Spoke auf DPDs, um festzustellen, ob ein Spoke nicht reagiert, und löst eine Änderung aus, sobald der Peer für tot erklärt wird. Die Option, DPD zu verwenden, ist aufgrund der Funktionsweise von DPDs nicht schnell. Ein Administrator möchte die Konfiguration möglicherweise durch Objektverfolgung oder ähnliche Erweiterungen erweitern.

Weitere Informationen finden Sie im Kapitel **FlexVPN Client Configuration** (Konfiguration des FlexVPN-Clients) des Cisco IOS-Konfigurationsleitfadens, das im Abschnitt **Zugehörige Informationen** am Ende dieses Dokuments verlinkt ist.

Konfiguration des vollen Spokes - Referenz

```
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 ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

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 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Hub-Konfiguration

Obwohl die meisten Hub-Konfigurationen unverändert bleiben, müssen mehrere Aspekte berücksichtigt werden. Die meisten von ihnen betreffen eine Situation, in der eine oder mehrere Spokes mit einem Hub verbunden sind, während andere in Beziehung zu einem anderen Hub bleiben.

Spoke-Adressen

Da Stationen IP-Adressen von Hubs beziehen, ist es normalerweise wünschenswert, dass Hubs Adressen aus verschiedenen Subnetzen oder einem anderen Teil eines Subnetzes zuweisen.

Beispiel:

Hub 1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

Hub 2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

Dies verhindert Überschneidungen, auch wenn die Adressen nicht außerhalb der FlexVPN-Cloud geroutet werden, was die Fehlerbehebung beeinträchtigen kann.

Hub-Overlay-Adresse

Beide Hubs können dieselbe IP-Adresse auf einer virtuellen Vorlagenschnittstelle beibehalten. Dies kann sich jedoch in einigen Fällen auf die Fehlerbehebung auswirken. Diese Designauswahl erleichtert die Bereitstellung und Planung, da der Spoke-Server nur über eine Peer-Adresse für das Border Gateway Protocol (BGP) verfügen muss.

In einigen Fällen ist dies nicht unbedingt wünschenswert oder erforderlich.

Routing

Die Hubs müssen Informationen über die verbundenen Stationen austauschen.

Hubs müssen in der Lage sein, die spezifischen Routen von Geräten auszutauschen, mit denen sie verbunden sind, und dennoch eine Zusammenfassung für die Stationen bereitstellen können.

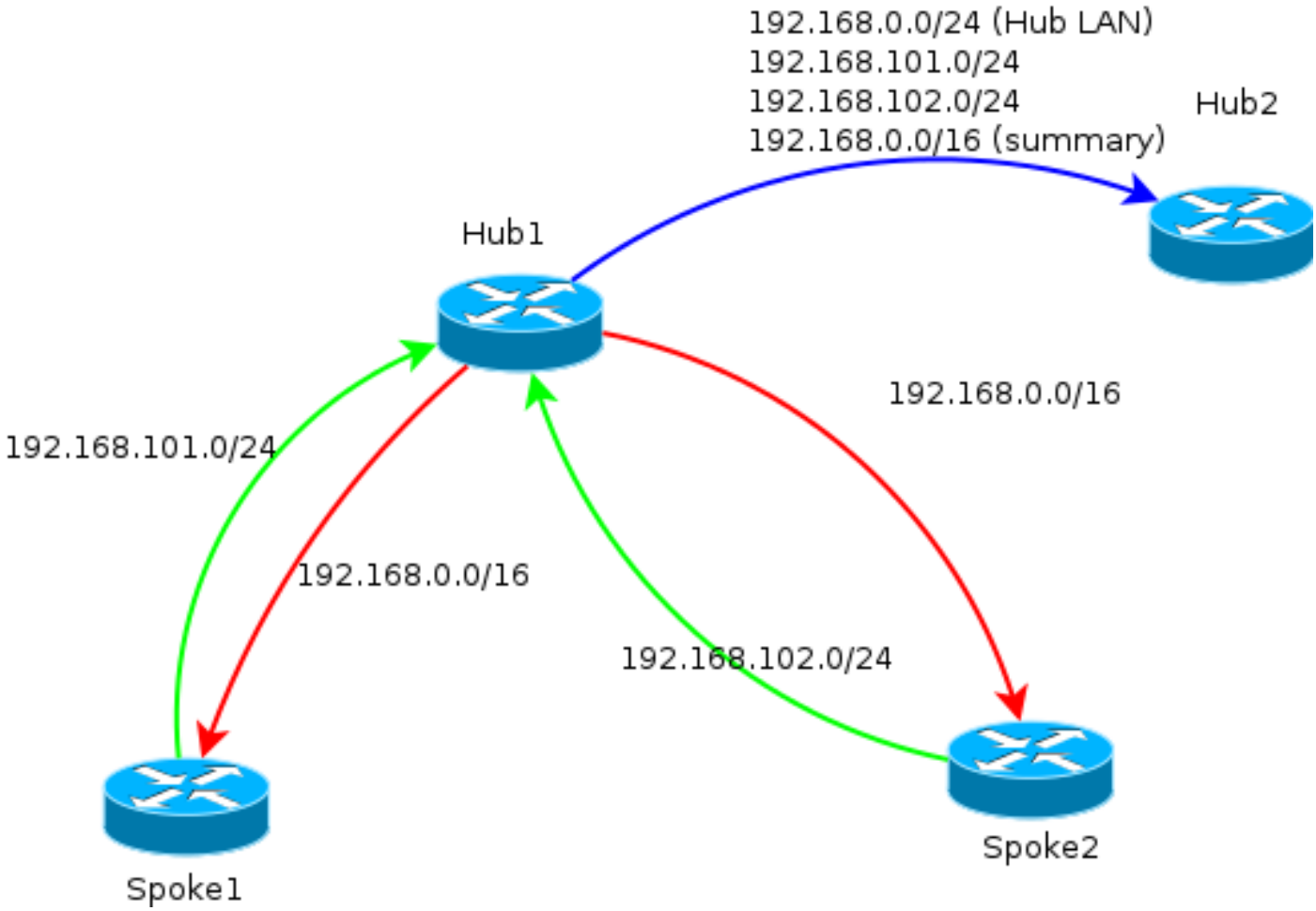
Da Cisco empfiehlt, iBGP mit FlexVPN und DMVPN zu verwenden, wird nur dieses Routing-Protokoll angezeigt.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

Diese Konfiguration ermöglicht:

- Dynamischer Listener von den Adressen, die den Stationen zugewiesen sind
- Werbenetzwerk von 192.168.0.0/24
- Anzeigenübersicht Route von 192.168.0.0/16 zu allen Stationen. Die Konfiguration der Aggregat-Adresse erstellt eine statische Route für dieses Präfix über die Null0-Schnittstelle. Hierbei handelt es sich um eine Rückwurfroute, die verwendet wird, um Routing-Schleifen zu verhindern.
- Weiterleitung bestimmter Präfixe an den anderen Hub
- Routen-Reflektor-Client, um sicherzustellen, dass die Hubs Informationen austauschen, die sie von Spokes gelernt haben

Dieses Diagramm stellt den Präfixaustausch in BGP in dieser Konfiguration aus Sicht eines der Hubs dar.



Hinweis: In diesem Diagramm stellt die grüne Linie Informationen dar, die von den Stationen zum Hub bereitgestellt werden, die rote Linie stellt Informationen dar, die von jedem Hub zu den Stationen bereitgestellt werden (nur Zusammenfassung), und die blaue Linie stellt die Präfixe dar, die zwischen den Hubs ausgetauscht werden.

Verwendung von Netzwerkübersichten

Zusammenfassungen sind in einigen Szenarien möglicherweise nicht anwendbar oder erwünscht. Seien Sie vorsichtig, wenn Sie die Ziel-IP in Präfixen festlegen, da iBGP den nächsten Hop standardmäßig nicht überschreibt.

Zusammenfassungen werden in Netzwerken empfohlen, die den Status häufig ändern. Unstabile Internetverbindungen erfordern beispielsweise Zusammenfassungen, um: Vermeiden Sie das Entfernen und Hinzufügen von Präfixen, beschränken Sie die Anzahl der Updates, und ermöglichen Sie den meisten Konfigurationen eine ordnungsgemäße Skalierung.

Spoke-to-Spoke-Tunnel

Im Szenario und in der Konfiguration, die im vorherigen Abschnitt erwähnt wurden, können Stationen verschiedener Hubs keine direkten Spoke-to-Spoke-Tunnel einrichten. Der Datenverkehr zwischen Stationen, die mit verschiedenen Hubs verbunden sind, fließt über die zentralen Geräte.

Dafür gibt es eine einfache Lösung. Es ist jedoch erforderlich, dass das Next Hop Resolution Protocol (NHRP) mit derselben Netzwerk-ID zwischen den Hubs aktiviert ist. Dies ist beispielsweise möglich, wenn Sie einen Point-to-Point Generic Routing Encapsulation (GRE)-Tunnel zwischen Hubs erstellen. Dann ist IPsec nicht erforderlich.

Überprüfen

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.

Der Befehl **show crypto ikev2 sa** informiert Sie darüber, wo das Spoke aktuell verbunden ist.

Mit dem Befehl **show crypto ikev2 client flexvpn** kann ein Administrator den aktuellen Zustand des FlexVPN-Client-Vorgangs ermitteln.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

Bei einem erfolgreichen Failover mit der Konfiguration für die **Anzeigeprotokollierung** wird diese Ausgabe auf dem Spoke-Gerät protokolliert:

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

In dieser Ausgabe wird die Spoke-Verbindung vom **Hub 172.25.1.1**, der Flex_Client-Client-Konfigurationsblock erkennt Fehler und erzwingt eine Verbindung zu **172.25.2.1**, wenn ein Tunnel hochfährt, und einem Spoke wird eine IP-Adresse von **10.1.1.177** zugewiesen.

Fehlerbehebung

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.

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

Hier sind die relevanten Debugbefehle:

- **debuggen crypto ikev2**
- **Debug-Radius**

Zugehörige Informationen

- FlexVPN und Internet Key Exchange Version 2 Konfigurationsleitfaden, Cisco IOS Version 15 M&T
- Technischer Support und Dokumentation - Cisco Systems