Konfigurationsbeispiel für FlexVPN Spoke in redundantem Hub-Design mit dualem Cloud-Ansatz

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.

Konfigurieren

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.

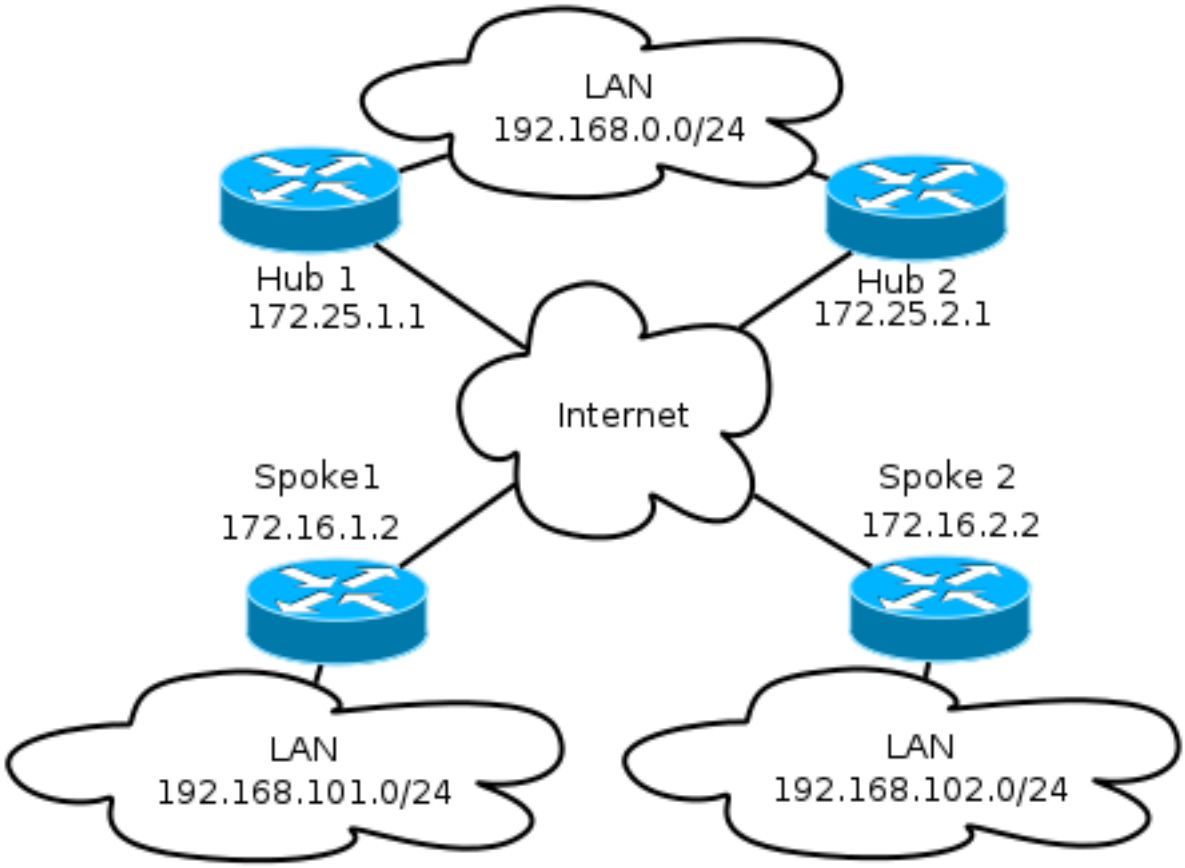
Ansatz	Vorteile	Verbindungen
Duale Cloud	• Schnellere Wiederherstellung bei Ausfällen basierend auf Routing-Protokoll-Timern • Mehr Möglichkeiten zur Verteilung des Datenverkehrs zwischen Hubs, da die Verbindung zu beiden Hubs aktiv ist	• Spoke führt die Sitzung mit beiden Hubs gleichzeitig durch, wodurch Ressourcen 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 (DPD oder (optional) Objektverfolgung • Der gesamte Datenverkehr wird gezwungen, jeweils zu einem Hub zu gelangen.

Dieses Dokument beschreibt den ersten Ansatz. Der Ansatz für diese Konfiguration ähnelt der Konfiguration für Dynamic Multipoint VPN (DMVPN) in der dualen Cloud. Die grundlegende Konfiguration von Hub and Spoke basiert auf den Migrationsdokumenten von DMVPN zu FlexVPN. Informationen zur FlexVPN-Migration: Artikel zur Beschreibung dieser Konfiguration "Hard Move from DMVPN to FlexVPN on Dieseldevices" (Harter Wechsel von DMVPN zu FlexVPN auf den gleichen Geräten).

Netzwerkdiagramm

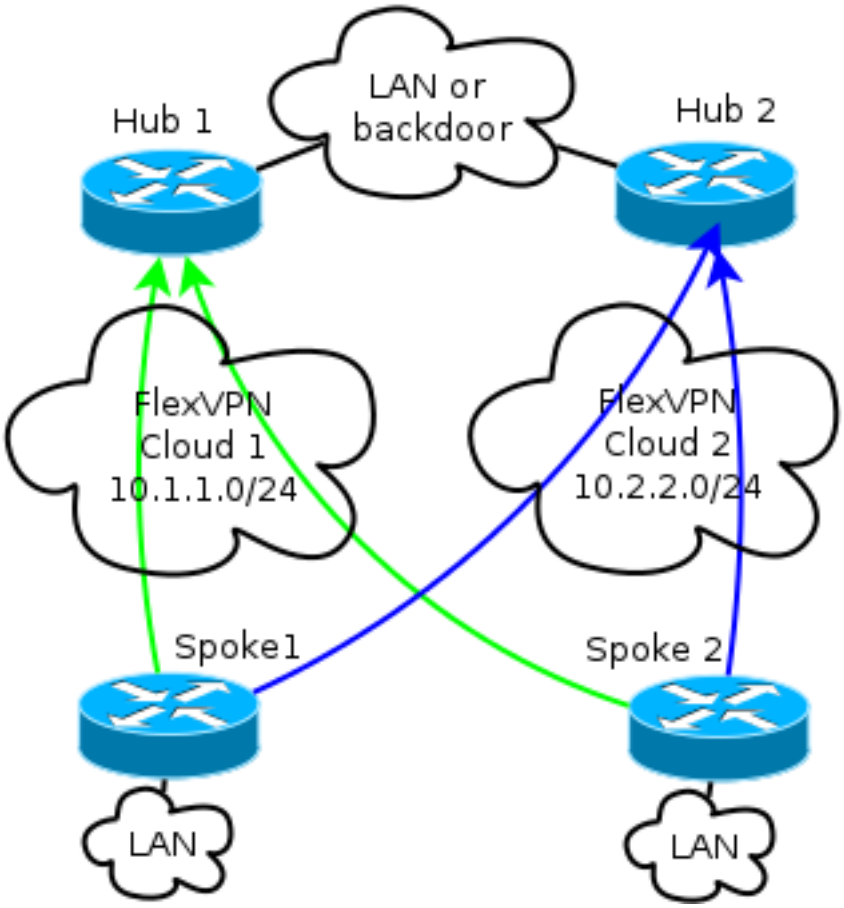
Transportnetz

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



Overlay-Netzwerk

Das 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 eine Beziehung zu beiden Hubs. Bei einem Ausfall wechselt das Routing-Protokoll von einem Hub zu einem anderen.



Hinweis: Die grünen Linien im Diagramm zeigen die Verbindung und Richtung der Internet Key Exchange Version 2 (IKEv2)/Flex-Sitzungen mit Hub 1 an, und die blauen Linien zeigen die Verbindung mit Hub 2 an.

Beide Hubs behalten eine separate IP-Adressierung in Overlay-Clouds bei. Die **/24-**Adressierung stellt den Pool der Adressen dar, die dieser Cloud zugewiesen sind, 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.

Spoke-Konfigurationen

Konfiguration der Spoke-Tunnel-Schnittstelle

Die in diesem Beispiel verwendete typische Konfiguration besteht lediglich aus zwei Tunnelschnittstellen mit zwei separaten Zieladressen.

```
interface Tunnel1
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 path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
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 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Damit sich Spoke-to-Spoke-Tunnel ordnungsgemäß bilden können, ist eine virtuelle Vorlage (Virtual Template, VT) erforderlich.

```
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
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Die Spoke-Anwendung verwendet eine nicht nummerierte Schnittstelle, die die LAN-Schnittstelle im VRF (Virtual Routing and Forwarding) angibt, das in diesem Fall global ist. Es kann jedoch besser sein, auf eine Loopback-Schnittstelle zu verweisen. Das liegt daran, dass Loopback-Schnittstellen unter fast allen Bedingungen online bleiben.

Konfiguration des Spoke Border Gateway Protocol (BGP)

Da Cisco iBGP als Routing-Protokoll für das Overlay-Netzwerk empfiehlt, wird in diesem Dokument nur diese Konfiguration erwähnt.

> **Hinweis**: Spokes müssen die BGP-Erreichbarkeit für beide Hubs aufrechterhalten.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

FlexVPN in dieser Konfiguration hat kein primäres oder sekundäres Hub-Konzept. Der Administrator entscheidet, ob das Routing-Protokoll einen Hub einem anderen vorzieht oder, in einigen Fällen, einen Lastenausgleich durchführt.

Überlegungen zu Spoke-Failover und -Konvergenz

Um die Zeit zu minimieren, die ein Spoke benötigt, um Fehler zu erkennen, verwenden Sie die folgenden beiden typischen Methoden.

- Verkürzen Sie die BGP-Timer. Die Standard-Haltezeit verursacht Failover.
- Konfigurieren Sie das BGP-Failover, das in diesem Artikel beschrieben wird: BGP-Unterstützung für die Deaktivierung von Fast Peering Session.
- Bidirectional Forwarding Detection (BFD) sollte nicht verwendet werden, da dies in den meisten FlexVPN-Bereitstellungen nicht empfohlen wird.

Spoke-to-Spoke-Tunnel und Failover

Spoke-to-Spoke-Tunnel verwenden das Next Hop Resolution Protocol (NHRP)-Shortcut-Switching. Cisco IOS gibt an, dass es sich bei diesen Verknüpfungen um NHRP-Routen handelt, z. B.:

```
Spoke1#show ip route nhrp
(...)

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Diese Routen laufen nicht ab, wenn die BGP-Verbindung abläuft. Stattdessen werden sie für die NHRP-Holdtime gehalten, die standardmäßig zwei Stunden beträgt. Dies bedeutet, dass aktive Spoke-to-Spoke-Tunnel auch bei einem Ausfall in Betrieb bleiben.

Hub-Konfigurationen

Lokale Pools

Wie im Abschnitt **Netzwerkdiagramm** beschrieben, behalten beide Hubs eine separate IP-Adressierung bei.

Hub 1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Hub 2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

Hub-BGP-Konfiguration

Die Hub-BGP-Konfiguration ähnelt weiterhin den vorherigen Beispielen.

Diese Ausgabe stammt von Hub 1 mit der LAN-IP-Adresse **192.168.0.1**.

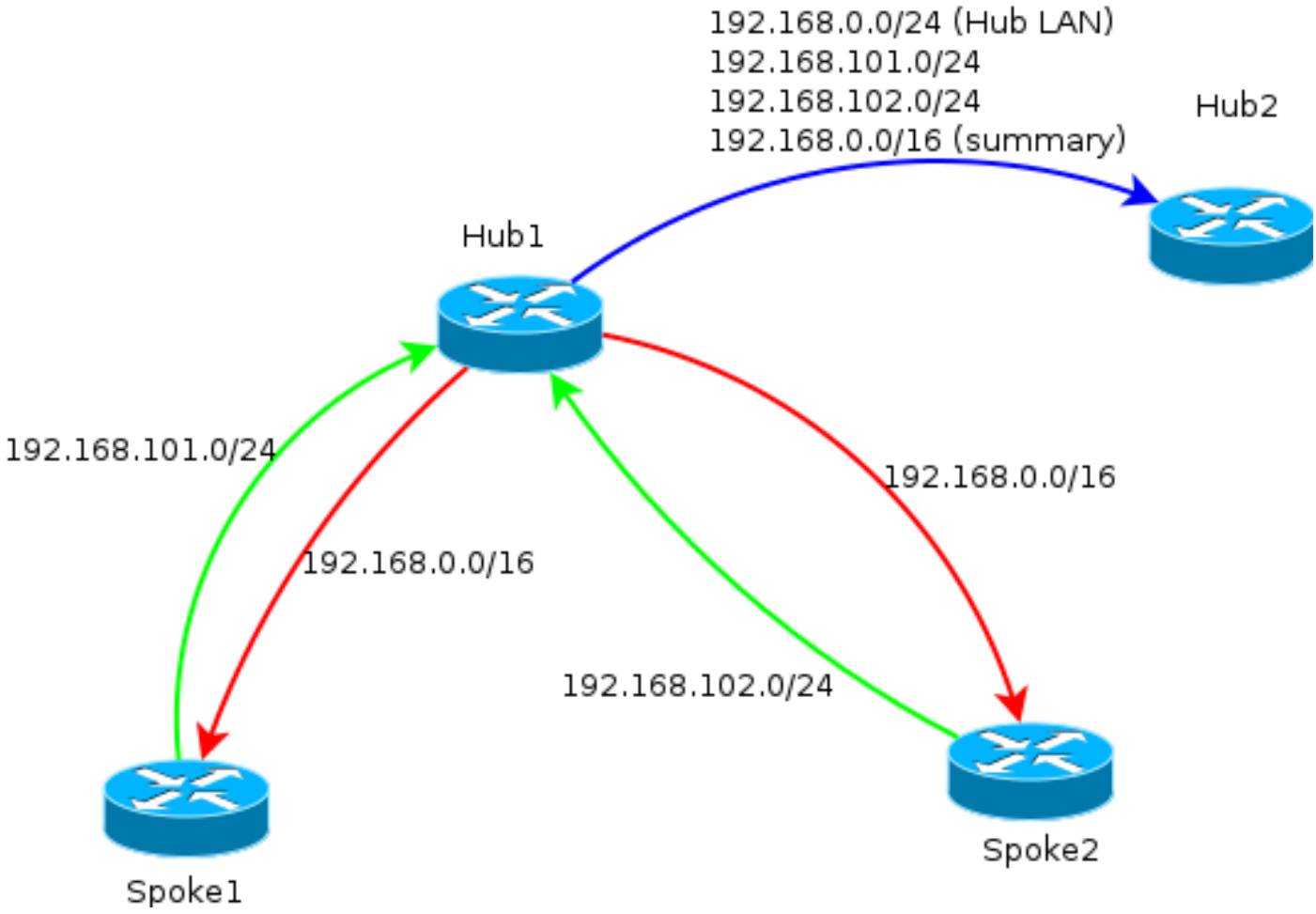
```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
```

```
neighbor Spokes fall-over
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

route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

Im Wesentlichen ist dies das, was getan wird:

- Der lokale FlexVPN-Adresspool liegt im BGP-Listen-Bereich.
- Das lokale Netzwerk ist 192.168.0.0/24.
- Eine Zusammenfassung wird nur an Spokes weitergegeben. Bei der Konfiguration der Aggregate-Adresse wird für dieses Präfix eine statische Route über die Null0-Schnittstelle erstellt. Diese Route wird verwendet, um Routing-Schleifen zu verhindern.
- Alle Präfixe werden dem anderen Hub mitgeteilt. Da es sich auch um eine iBGP-Verbindung handelt, ist eine Routen-Reflektor-Konfiguration erforderlich.

Dieses Diagramm stellt den Austausch von BGP-Präfixen zwischen Stationen und Hubs in einer FlexVPN-Cloud dar.



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

Überprüfen

Da beide Spokes weiterhin mit beiden Hubs verbunden sind, werden zwei IKEv2-Sitzungen mit dem Befehl **show crypto ikev2 as** angezeigt.

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

Geben Sie folgende Befehle ein, um die Routing-Protokollinformationen anzuzeigen:

```
show bgp ipv4 unicast

show bgp summary
```

In den Stationen sollten Sie sehen, dass das Zusammenfassungspräfix von den Hubs empfangen wird und dass die Verbindungen zu beiden Hubs aktiv sind.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, 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
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

Fehlerbehebung

Zur Fehlerbehebung sind zwei Hauptblöcke erforderlich:

- Internet Key Exchange (IKE)
- Internet Protocol Security (IPsec)

Hier sind die relevanten Show-Befehle:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Hier sind die relevanten Debugbefehle:

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Das relevante Routing-Protokoll ist wie folgt:

```
show bgp ipv4 unicast (or show ip bgp)

show bgp summary
```