FlexVPN-handleiding in redundante hubontwerp met een configuratievoorbeeld met dubbele cloud

Inhoud

Inleiding

Dit document beschrijft hoe u een gesproken netwerk in een FlexVPN-netwerk kunt configureren met gebruik van het FlexVPN-clientconfiguratieblok in een scenario waarin meerdere knooppunten beschikbaar zijn.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexVPN
- Cisco-routingprotocollen

Gebruikte componenten

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

- Cisco G2 Series geïntegreerde services router (ISR)
- Cisco IOS versie 15.2M

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

Voor overtollige doeleinden, zou een gesproken kunnen met meerdere knooppunten moeten verbinden. Redundantie van de spaakzijde maakt continu gebruik mogelijk zonder één enkel punt van falen op de hub.

De twee meest gebruikelijke FlexVPN redundante hub ontwerpen die de spaakconfiguratie gebruiken zijn:

- **Dubbele wolkenbenadering**, waarbij een gesproken wordt heeft twee aparte tunnels die te allen tijde actief zijn op beide hubs.
- **Failover-benadering**, waarbij een spits een actieve tunnel heeft met één hub op een bepaald moment in de tijd.

Beide benaderingen hebben een unieke reeks voor- en nadelen.

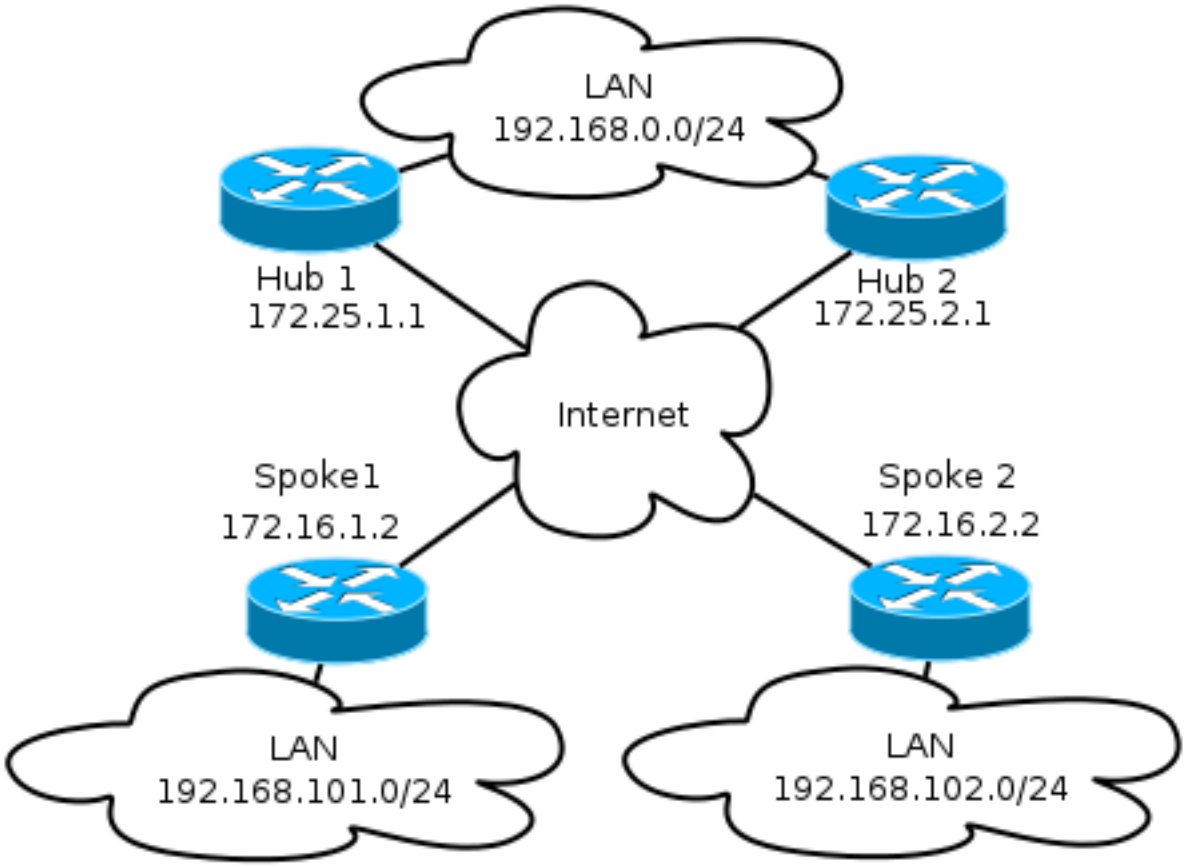
benaderen	Pros	Cons
Dubbele cloud	• Snellere terugwinning tijdens mislukking, gebaseerd op het routeren van protocol timers • Meer mogelijkheden om verkeer tussen knooppunten te verdelen aangezien de verbinding met beide knooppunten actief is	• Spoke onderhoudt sessie aan beide knooppunten tegelijkertijd, wat middelen beide knooppunten consumeert
failover	• Eenvoudige configuratie - ingebouwd in FlexVPN • Vertrouwt niet op het routingprotocol in een mislukking	• Lagere terugwinningstijd - gebaseerd op Dead Peer Detection (DPD) of (optioneel object tracking • Al het verkeer is gedwongen om tegelijk één hub te reizen.

In dit document wordt de eerste aanpak beschreven. De benadering van deze configuratie is gelijk aan de Dynamic Multipoint VPN (DMVPN) dubbele cloudconfiguratie. De basisconfiguratie van de hub en het praatje is gebaseerd op migratiedocumenten van DMVPN naar FlexVPN. Raadpleeg de FlexVPN-migratie: Harde beweging van DMVPN naar FlexVPN op Hetzelfde artikel van het Apparaat voor een beschrijving van deze configuratie.

Netwerkdiagram

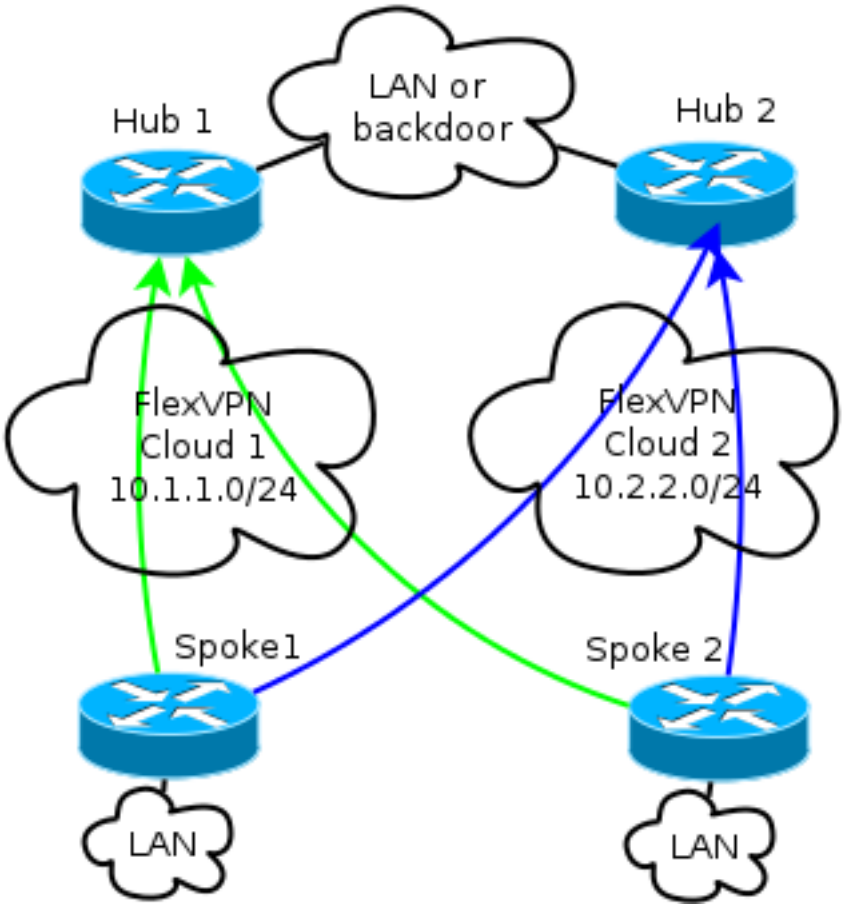
transportnetwerk

Dit diagram illustreert het basale transportnetwerk dat doorgaans in FlexVPN-netwerken wordt gebruikt.



Overlay-netwerk

Het diagram illustreert het overlay netwerk met logische connectiviteit die toont hoe de failover zou moeten werken. Tijdens normaal gebruik onderhouden Spoke 1 en Spoke 2 een relatie met beide knooppunten. Op een mislukking, verandert het routingprotocol van één hub in een ander.



Opmerking: In het diagram tonen de groene lijnen de verbinding en de richting van de Toetsuitwisseling Versie 2 (IKEv2)/Flex sessies aan Hub 1, en de blauwe lijnen wijzen op de verbinding met Hub 2.

Beide knooppunten behouden afzonderlijke IP-adressering in overlay wolken. De **24/**adressering vertegenwoordigt het aantal adressen dat voor deze cloud is toegewezen, en niet de eigenlijke interface-adressering. Dit komt doordat het FlexVPN-knooppunt doorgaans een dynamisch IP-adres toewijst voor de inkomende interface en is gebaseerd op routes die dynamisch via routeopdrachten in het FlexVPN-vergunningsblok zijn ingevoegd.

Spoelconfiguratie

Configuratie van Spoke-tunnelinterface

De typische configuratie die in dit voorbeeld wordt gebruikt is eenvoudig twee tunnelinterfaces met twee afzonderlijke doeladressen.

```
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
```

Om tunnels met een gesproken tekst goed te laten vormen, is een virtuele sjabloon (VT) nodig.

```
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
```

Het gesproken gebruik een ongenummerde interface die de LAN interface in het Virtual Routing and Forwarding (VRF) aangeeft, en die in dit geval mondiaal is. Hoe dan ook, het kan beter zijn om te verwijzen naar een loopback-interface. Dit komt doordat de loopback-interfaces onder bijna alle voorwaarden online blijven.

BGP-configuratie (Spoke Border Gateway Protocol)

Aangezien Cisco iBGP als het routingprotocol aanbeveelt dat in het overlay netwerk wordt gebruikt, vermeldt dit document alleen deze configuratie.

> Opmerking: Spokes moeten BGP bereikbaarheid voor beide knooppunten behouden.

```
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 heeft in deze configuratie geen primair of secundair knooppunt concept. De beheerder beslist of het routingprotocol de voorkeur geeft aan een hub boven een ander of, in sommige scenario's, het in evenwicht brengen van de lading.

SPRAAKfailover en Convergentieoverwegingen

Om de tijd die nodig is voor het opsporen van een defect te minimaliseren, gebruikt u deze twee typische methoden.

- Kort de BGP-timers in. De standaard hold-time oorzaken voor failover.
- Configuratie van de val-over van BGP, die in dit artikel wordt besproken, Ondersteuning van BGP voor Snelle Peering Session Deactivatie.
- Gebruik geen Bidirectional Forwarding Detection (BFD), omdat deze niet wordt aanbevolen in de meeste FlexVPN-implementaties.

Spoke-to-Spoke tunnels en failover

Spoke-to-Speeltunnels gebruiken Next Hop Resolutie Protocol (NHRP) snelswitching. Cisco IOS geeft aan dat die sneltoetsen NHRP-routes zijn, bijvoorbeeld:

```
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
```

Deze routes verlopen niet wanneer de BGP-verbinding verstrijkt; in plaats daarvan worden zij gehouden voor de NHRP-tijd, die standaard twee uur is. Dit betekent dat actieve tunnels met een spits ook in een mislukking in gebruik blijven.

Hub-configuraties

Lokale pools

Zoals besproken in het gedeelte **Netwerkdiagram**, behouden beide knooppunten afzonderlijke IP-adressering.

Hub1

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

Hub2

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

Hub BGP-configuratie

De BGP-configuratie van de hub blijft gelijk aan eerdere voorbeelden.

Deze output komt van Hub 1 met een LAN IP-adres van **192.168.0.1**.

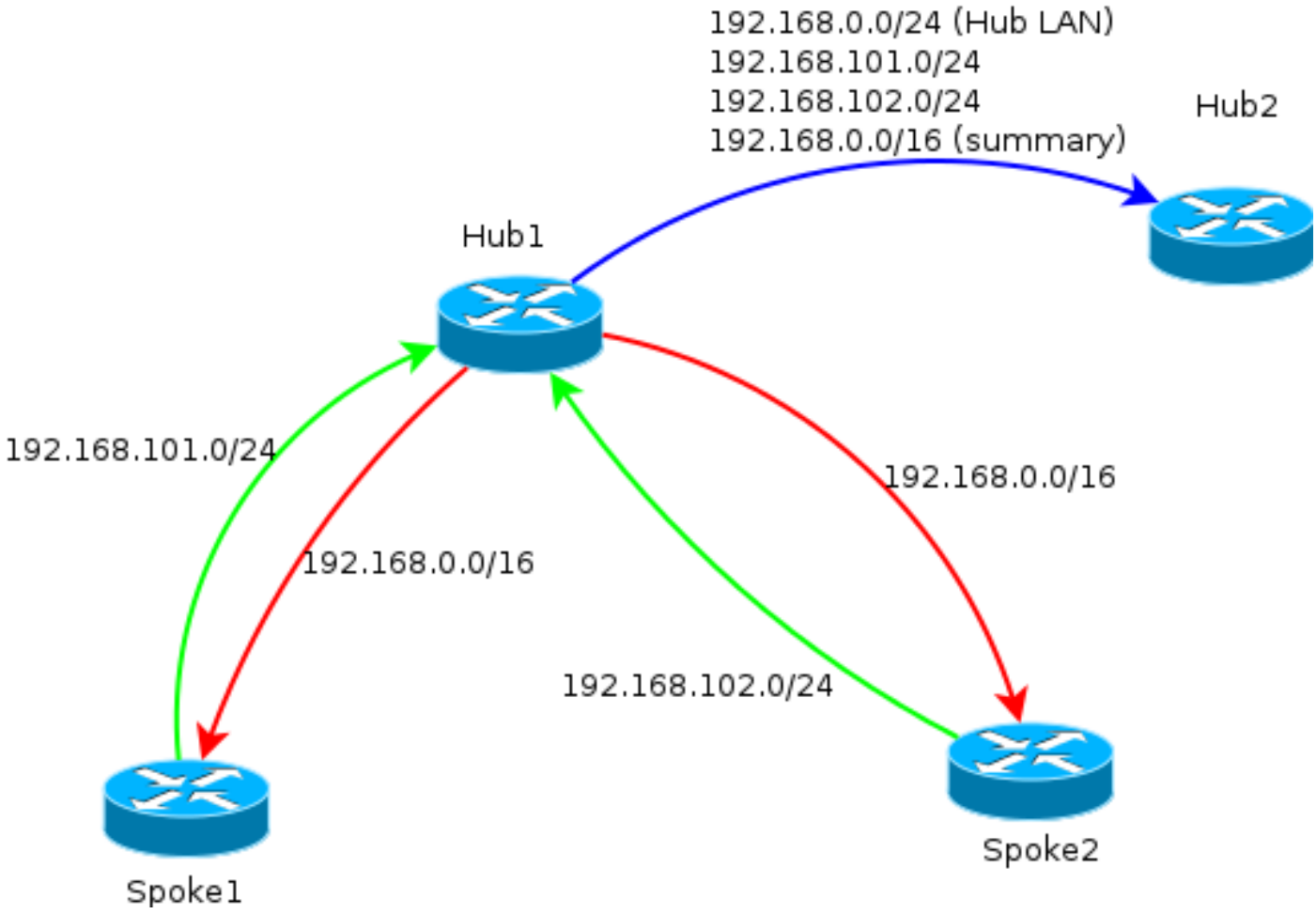
```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor Spokes fall-over
```

```
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
```

In essentie is dit wat er gebeurt:

- Lokale FlexVPN-adrespool is in het BGP-bereik.
- Lokaal netwerk is 192.168.0.0/24.
- Een samenvatting wordt alleen aan woordvoerders geadverteerd. De configuratie van het aggregaat-adres creëert een statische route voor dat prefix via ongeldige0 interface, die een verworpen route is die wordt gebruikt om het verzenden van lijnen te verhinderen.
- Alle specifieke prefixes worden naar de andere hub geadverteerd. Aangezien het ook een iBGP verbinding is, vereist het een route-reflectorconfiguratie.

Dit diagram vertegenwoordigt de uitwisseling van BGP prefixes tussen woords en hubs in één FlexVPN-cloud.



Opmerking: In het diagram representeert de groene lijn informatie die door spaken aan de hub wordt verstrekt, vertegenwoordigt de rode lijn informatie die door elke hub aan de spaken wordt verstrekt (slechts een samenvatting), en de blauwe lijn vertegenwoordigt prefixes die tussen knooppunten worden uitgewisseld.

Verifiëren

Aangezien elke sprak associatie met beide knooppunten behoudt, worden twee IKEv2 sessies gezien met de **show crypto ikev2 als** opdracht.

```
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
```

U kunt de informatie over het routingprotocol als volgt weergeven door deze opdrachten in te voeren:

show bgp ipv4 unicast

show bgp summary

Op de spaken, zou u moeten zien dat het summiere voorvoegsel van de knooppunten wordt ontvangen, en dat de verbindingen met beide knooppunten actief zijn.

```
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
```

Problemen oplossen

Er zijn twee belangrijke blokken voor probleemoplossing:

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

Hier zijn de relevante showopdrachten:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Hier zijn de relevante debug-opdrachten:

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Dit is het relevante routingprotocol:

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

show bgp summary
```