

FlexVPN ha conjuguent exemple de configuration de hub

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Scénario opérationnel régulier](#)

[Spoke-to-spoke \(raccourci\)](#)

[Tableaux et sorties de routage pour le scénario opérationnel régulier](#)

[Scénario de panne HUB1](#)

[Configurations](#)

[Configuration R1-HUB](#)

[Configuration R2-HUB2](#)

[Configuration R3-SPOKE1](#)

[Configuration R4-SPOKE2](#)

[Configuration R5-AGGR1](#)

[Configuration R6-AGGR2](#)

[Configuration R7-HOST \(simulation d'HÔTE dans ce réseau\)](#)

[Importantes notes de configuration](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer une pleine conception de Redondance pour les bureaux distants qui se connectent à Data Center par l'intermédiaire du VPN basé sur IPSec au-dessus d'un support réseau non sécurisé, tel que l'Internet.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur ces composants de technologie :

- [Protocole BGP \(Border Gateway Protocol\)](#) comme protocole de routage dans Data Center et entre les rai et les Concentrateurs dans le recouvrement VPN.
- [Détection bidirectionnelle d'expédition](#) (BFD) comme mécanisme qui le détecte en bas des liens (routeur vers le bas) qu'exécuté à l'intérieur de Data Center seulement (pas au-dessus des tunnels de recouvrement).
- [Cisco IOS® FlexVPN](#) entre les hub and spoke, avec des capacités de spoke-to-spoke activées par l'intermédiaire de raccourcir la commutation.
- [Encapsulation de routage générique \(GRE\) perçant un tunnel](#) entre deux Concentrateurs afin d'activer la transmission de spoke-to-spoke, même lorsque les rai sont connectés à différents Concentrateurs.
- Artères [améliorées de Suivi d'objets](#) et de charge statique attachées aux objets dépistés.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Quand vous concevez des solutions d'accès distant pour Data Center, la Haute disponibilité (ha) est souvent une condition requise principale pour des applications utilisateur critiques.

La solution qui est présentée dans ce document permet la détection rapide et la reprise des scénarios de panne dans lesquels des Concentrateurs de VPN-terminaison descendent en raison d'une recharge, d'une mise à jour, ou des problèmes d'alimentation. Tous les Routeurs distants de bureaux (rai) utilisent alors l'autre hub opérationnel immédiatement à la découverte d'une telle panne.

Voici les avantages de cette conception :

- Reprise rapide de réseau d'un scénario de hub-vers le bas VPN
- Aucune synchronisations compliquées d'avec état (telles qu'associations de sécurité IPsec (SAS), Protocole ISAKMP (Internet Security Association and Key Management Protocol) SAS, et Crypto-routage) entre les Concentrateurs VPN
- Aucun problèmes d'anti-relecture dus aux retards dans la synchronisation de numéro de séquence de Protocole ESP (Encapsulating Security Payload) avec l'avec état ha d'IPsec

- Les Concentrateurs VPN peuvent utiliser le matériel ou le logiciel basé par IOS/IOS-XE différent de Cisco
- Choix flexibles d'implémentation d'Équilibrage de charge avec le BGP comme protocole de routage qui fonctionne dans le recouvrement VPN
- Routage clair et accessible en lecture sur tous les périphériques sans les mécanismes masqués qui fonctionnent à l'arrière-plan
- Connectivité directe de spoke-to-spoke
- Tous les avantages de [FlexVPN](#), pour inclure le Qualité de service (QoS) d'intégration et de par-tunnel d'Authentification, autorisation et comptabilité (AAA)

Configurez

Cette section fournit des exemples de scénario et décrit comment configurer une pleine conception de Redondance pour les bureaux distants qui se connectent à Data Center par l'intermédiaire du VPN basé sur IPSec au-dessus d'un support réseau non sécurisé.

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

[Diagramme du réseau](#)

C'est la topologie du réseau qui est utilisée dans ce document :

Remarque: Tous les Routeurs qui sont utilisés dans cette topologie exécutent la version 15.2(4)M1 de Cisco IOS, et le nuage Internet utilisent un schéma d'adresse de 172.16.0.0/24.

Scénario opérationnel régulier

Dans un scénario opérationnel normal, quand tous les Routeurs sont hauts et opérationnels, tous les routeurs en étoile conduisent tout les trafic par le hub par défaut (R1-HUB1). Cette préférence de routage est réalisée quand la préférence locale BGP de par défaut est placée à 200 (référez-vous aux sections qui suivent pour des détails). Ceci peut être ajusté a basé sur les conditions requises de déploiement, telles que l'Équilibrage de charge du trafic.

Spoke-to-spoke (raccourci)

Si R3-Spoke1 initie une connexion à R4-Spoke2, un tunnel dynamique de spoke-to-spoke est créé avec la configuration de commutation de raccourci.

Conseil : Pour plus de détails, référez-vous au [FlexVPN configurant a parlé au](#) guide de [configuration en étoile](#).

Si R3-Spoke1 est connecté seulement à R1-HUB1, et R4-Spoke2 est connecté seulement à R2-HUB2, une connexion directe de spoke-to-spoke peut encore être réalisée avec le tunnel du Point à point GRE qui fonctionne entre les Concentrateurs. Dans ce cas, le chemin initial du trafic entre R3-Spoke1 et R4-Spoke2 ressemble à ceci :

Puisque R1-Hub1 reçoit le paquet sur l'interface d'accès virtuel, qui a le même ID de réseau de Protocole NHRP (Next Hop Resolution Protocol) que celui sur le tunnel GRE, l'indication du trafic est envoyée vers le R3-Spoke1. Ceci déclenche la création dynamique de tunnel de spoke-to-spoke :

Tableaux et sorties de routage pour le scénario opérationnel régulier

Voici la table de routage R1-HUB1 dans un scénario opérationnel régulier :

```
R1-HUB1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
S      10.0.0.0/8 is directly connected, Null0
C      10.0.0.0/24 is directly connected, Tunnel0
L      10.0.0.1/32 is directly connected, Tunnel0
C      10.0.1.1/32 is directly connected, Loopback0
S      10.0.1.2/32 is directly connected, Virtual-Access1
S      10.0.1.3/32 is directly connected, Virtual-Access2
B      10.0.2.1/32 [200/0] via 10.0.0.2, 00:05:40
B      10.0.2.3/32 [200/0] via 10.0.0.2, 00:05:40
B      10.0.2.4/32 [200/0] via 10.0.0.2, 00:05:40
B      10.0.5.1/32 [200/0] via 192.168.0.5, 00:05:40
B      10.0.6.1/32 [200/0] via 192.168.0.6, 00:05:40
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.0.0/24 is directly connected, Ethernet0/0
L      172.16.0.1/32 is directly connected, Ethernet0/0
S      192.168.0.0/16 is directly connected, Null0
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.0.0/24 is directly connected, Ethernet0/2
L      192.168.0.1/32 is directly connected, Ethernet0/2
B      192.168.1.0/24 [200/0] via 192.168.0.5, 00:05:40
B      192.168.3.0/24 [200/0] via 10.0.1.4, 00:05:24
B      192.168.4.0/24 [200/0] via 10.0.1.5, 00:05:33
```

Voici la table de routage R3-SPOKE1 dans un scénario opérationnel régulier après que le tunnel

de spoke-to-spoke avec R4-SPOKE2 soit créé :

```
R3-SPOKE1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
B       10.0.0.0/8 [200/0] via 10.0.1.1, 00:06:27
H       10.0.0.1/32 is directly connected, 00:06:38, Tunnell
S %    10.0.1.1/32 is directly connected, Tunnel0
C       10.0.1.3/32 is directly connected, Tunnel0
H       10.0.1.4/32 is directly connected, 00:01:30, Virtual-Access1
S       10.0.2.1/32 is directly connected, Tunnell
C       10.0.2.3/32 is directly connected, Tunnell
H       10.0.2.4/32 [250/1] via 10.0.2.3, 00:01:30, Virtual-Access1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/24 is directly connected, Ethernet0/0
L       172.16.0.3/32 is directly connected, Ethernet0/0
B       192.168.0.0/16 [200/0] via 10.0.1.1, 00:06:27
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, Ethernet0/1
L       192.168.3.3/32 is directly connected, Ethernet0/1
192.168.4.0/32 is subnetted, 1 subnets
H       192.168.4.4 [250/1] via 10.0.1.3, 00:01:30, Virtual-Access1
```

Sur R3-Spoke1, la table BGP a deux entrées pour le réseau 192.168.0.0/16 avec différents locaux-préférence (R1-Hub1 est préféré) :

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
```

```
BGP routing table entry for 192.168.0.0/16, version 8
Paths: (2 available, best #2, table default)
Not advertised to any peer
Refresh Epoch 1
Local
 10.0.2.1 from 10.0.2.1 (10.0.2.1)
  Origin incomplete, metric 0, localpref 100, valid, internal
  rx pathid: 0, tx pathid: 0
Refresh Epoch 1
Local
 10.0.1.1 from 10.0.1.1 (10.0.1.1)
  Origin incomplete, metric 0, localpref 200, valid, internal, best
  rx pathid: 0, tx pathid: 0x0
```

Voici la table de routage R5-AGGR1 dans un scénario opérationnel régulier :

```
R5-LAN1#show ip route
```

```
10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B       10.0.0.0/8 [200/0] via 192.168.0.1, 00:07:22
B       10.0.0.0/24 [200/0] via 192.168.0.1, 00:07:22
B       10.0.1.1/32 [200/0] via 192.168.0.1, 00:07:22
B       10.0.1.3/32 [200/0] via 192.168.0.1, 00:07:17
B       10.0.1.4/32 [200/0] via 192.168.0.1, 00:07:16
B       10.0.2.1/32 [200/0] via 192.168.0.2, 15:44:13
B       10.0.2.3/32 [200/0] via 192.168.0.2, 15:44:13
B       10.0.2.4/32 [200/0] via 192.168.0.2, 15:44:13
```

```

C      10.0.5.1/32 is directly connected, Loopback0
B      10.0.6.1/32 [200/0] via 192.168.0.6, 00:07:22
      172.16.0.0/24 is subnetted, 1 subnets
B      172.16.0.0 [200/0] via 192.168.0.1, 00:07:22
B      192.168.0.0/16 [200/0] via 192.168.0.1, 00:07:22
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.0.0/24 is directly connected, Ethernet0/0
L      192.168.0.5/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, Ethernet0/1
L      192.168.1.5/32 is directly connected, Ethernet0/1
B      192.168.3.0/24 [200/0] via 10.0.1.3, 00:07:06
B      192.168.4.0/24 [200/0] via 10.0.1.4, 00:07:15

```

Voici la table de routage R7-HOST dans un scénario opérationnel régulier :

```

R7-HOST#show ip route
S*    0.0.0.0/0 [1/0] via 192.168.1.254
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, Ethernet0/0
L      192.168.1.7/32 is directly connected, Ethernet0/0

```

Scénario de panne HUB1

Voici vers le bas un scénario R1-HUB1 (dû aux actions telles que des pannes de courant ou une mise à jour) :

Dans ce scénario, cette séquence d'opérations se produit :

1. Le BFD sur R2-HUB2 et sur les Routeurs R5-AGGR1 et R6-AGGR2 d'agrégat de RÉSEAU LOCAL détectent l'état inactif de R1-HUB1. En conséquence, la proximité BGP descend immédiatement.
2. La détection d'objet de piste pour R2-HUB2 qui détecte la présence du bouclage R1-HUB1 descend (piste 1 en exemple de configuration).
3. Ceci avalé a dépisté l'objet déclenche une autre piste pour monter (logique PAS). Dans cet exemple, la piste 2 monte toutes les fois que la piste 1 descend.

4. Ceci déclenche une entrée statique de Routage IP à ajouter à la table de routage due à une valeur qui est inférieure que la distance administrative par défaut. Voici la configuration appropriée :

```

! Routes added when second HUB is down
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2

! Default static routes are with Tag 200 and admin distance of 150
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200

```

5. R2-HUB2 redistribue ces artères statiques avec un local-preference BGP qui est plus grand que la valeur qui est placée pour R1-HUB1. Dans cet exemple, un local-preference de **500** est utilisé dans le scénario de panne, au lieu des **200** qui est placé par R1-HUB1 :

```

route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
route-map LOCALPREF permit 10

```

```
match tag 200
set local-preference 200
```

! Sur R3-Spoke1, vous pouvez voir ceci dans les sorties BGP. Notez que l'entrée à R1 existe toujours, mais elle n'est pas utilisée :

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
BGP routing table entry for 192.168.0.0/16, version 10
Paths: (2 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
Local
 10.0.2.1 from 10.0.2.1 (10.0.2.1)
   Origin incomplete, metric 0, localpref 500, valid, internal, best
   rx pathid: 0, tx pathid: 0x0
Refresh Epoch 1
Local
 10.0.1.1 from 10.0.1.1 (10.0.1.1)
   Origin incomplete, metric 0, localpref 200, valid, internal
   rx pathid: 0, tx pathid: 0
```

6. En ce moment, les deux rais (R3-Spoke1 et R4-Spoke2) commencent à envoyer le trafic à R2-HUB2. Toutes ces étapes devraient se produire dans un délai d'une seconde. Voici la table de routage sur le rai 3 :

```
R3-SPOKE1#show ip route
 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B    10.0.0.0/8 [200/0] via 10.0.2.1, 00:00:01
S    10.0.1.1/32 is directly connected, Tunnel0
C    10.0.1.3/32 is directly connected, Tunnel0
S    10.0.2.1/32 is directly connected, Tunnel1
C    10.0.2.3/32 is directly connected, Tunnel1
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.0.0/24 is directly connected, Ethernet0/0
L    172.16.0.3/32 is directly connected, Ethernet0/0
B    192.168.0.0/16 [200/0] via 10.0.2.1, 00:00:01
 192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, Ethernet0/1
L    192.168.3.3/32 is directly connected, Ethernet0/1
```

7. De plus défuntées sessions BGP entre les rais et le R1-HUB1 descend, et Dead Peer Detection (DPD) retire les tunnels d'IPSec qui sont terminés sur R1-HUB1. Cependant, ceci n'affecte pas l'expédition du trafic, puisque R2-HUB2 est déjà utilisé comme passerelle de tunnel-terminaison principale :

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
BGP routing table entry for 192.168.0.0/16, version 10
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
Local
 10.0.2.1 from 10.0.2.1 (10.0.2.1)
   Origin incomplete, metric 0, localpref 500, valid, internal, best
   rx pathid: 0, tx pathid: 0x0
```

Configurations

Cette section fournit des configurations d'échantillon pour les hub and spoke qui sont utilisés dans cette topologie.

Configuration R1-HUB

```

!
hostname R1-HUB1
!
aaa new-model
!
aaa authorization network default local
!
aaa session-id common
!
! setting track timers to the lowest possible (the lower this value is
! the faster router will react
track timer ip route msec 500
!
! Monitoring of HUB2's loopback present in routing table
! If it is present it will mean that HUB2 is alive
track 1 ip route 10.0.2.1 255.255.255.255 reachability
!
! Monitoring of loopback of R5-AGGR-1
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
! Monitoring of loopback of R6-AGGR-2
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
! Track 2 should be UP only when HUB2 is not available and both AGGRE routers are up
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!

! IKEv2 Config Exchange configuration (IP addresses for spokes are assigned from pool)
crypto ikev2 authorization policy default
  pool SPOKES
  route set interface
  route accept any tag 20
!
!
! IKEv2 profile for Spokes - Smart Defaults used
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  aaa authorization group psk list default default
  virtual-template 1
!
interface Loopback0
  ip address 10.0.1.1 255.255.255.255
!
! GRE Tunnel configured to second HUB. It is required for spoke-to-spoke connectivity
! to work in all possible circumstances
! no BFD echo configuration is required to avoid Traffic Indication sent by remote HUB
! (BFD echo is having the same source and destination IP address)
!
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  ip nhrp network-id 1
  ip nhrp redirect
bfd interval 50 min_rx 50 multiplier 3
no bfd echo
  tunnel source Ethernet0/2
  tunnel destination 192.168.0.2
!
interface Ethernet0/0

```



```

ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/2
ip address 192.168.0.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Templatel type tunnel
ip unnumbered Loopback0
ip nhrp network-id 1
ip nhrp redirect
tunnel protection ipsec profile default
!
! BGP Configuration
router bgp 1
bgp log-neighbor-changes
! dynamic peer-groups are used for AGGR routers and SPOKES
bgp listen range 192.168.0.0/24 peer-group DC
bgp listen range 10.0.1.0/24 peer-group SPOKES
! BGP timers configured
timers bgp 15 30
neighbor SPOKES peer-group
neighbor SPOKES remote-as 1
neighbor DC peer-group
neighbor DC remote-as 1
! Within DC BFD is used to determine neighbour status
neighbor DC fall-over bfd
neighbor 10.0.0.2 remote-as 1
! BFD is used to detect HUB2 status
neighbor 10.0.0.2 fall-over bfd
!
address-family ipv4
redistribute connected
! route-map which determines what should be the local-pref
redistribute static route-map LOCALPREF
neighbor SPOKES activate
! to spokes only Aggregate/Summary routes are sent
neighbor SPOKES route-map AGGR out
neighbor DC activate
neighbor DC route-reflector-client
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 route-reflector-client
exit-address-family
!
ip local pool SPOKES 10.0.1.2 10.0.1.254
!
! When HUB2 goes down Static Routes with Tag 500 are added and admin distance of 1
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
! Default static routes are with Tag 200 and admin distance of 150
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
match tag 500
set local-preference 500
!
route-map LOCALPREF permit 10

```

```
match tag 200
set local-preference 200
!
route-map LOCALPREF permit 15
match tag 20
```

Configuration R2-HUB2

```
hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
object 1 not
object 3
object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
pool SPOKES
route set interface
route accept any tag 20
!
!
crypto ikev2 profile default
match identity remote any
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization group psk list default default
virtual-template 1
!
!
interface Loopback0
ip address 10.0.2.1 255.255.255.255
!
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
ip nhrp network-id 1
ip nhrp redirect
bfd interval 50 min_rx 50 multiplier 3
no bfd echo
tunnel source Ethernet0/2
tunnel destination 192.168.0.1
!
interface Ethernet0/0
ip address 172.16.0.2 255.255.255.0
!
interface Ethernet0/2
ip address 192.168.0.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Templatel type tunnel
```

```

ip unnumbered Loopback0
ip nhrp network-id 1
ip nhrp redirect
tunnel protection ipsec profile default
!
router bgp 1
  bgp log-neighbor-changes
  bgp listen range 192.168.0.0/24 peer-group DC
  bgp listen range 10.0.2.0/24 peer-group SPOKES
  timers bgp 15 30
  neighbor SPOKES peer-group
  neighbor SPOKES remote-as 1
  neighbor DC peer-group
  neighbor DC remote-as 1
  neighbor DC fall-over bfd
  neighbor 10.0.0.1 remote-as 1
  neighbor 10.0.0.1 fall-over bfd
  !
  address-family ipv4
    redistribute connected
    redistribute static route-map LOCALPREF
    neighbor SPOKES activate
    neighbor SPOKES route-map AGGR out
    neighbor DC activate
    neighbor DC route-reflector-client
    neighbor 10.0.0.1 activate
    neighbor 10.0.0.1 route-reflector-client
  exit-address-family
  !
ip local pool SPOKES 10.0.2.2 10.0.2.254
ip forward-protocol nd
!
!
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
  match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
route-map LOCALPREF permit 10
  match tag 200
  set local-preference 100
!
route-map LOCALPREF permit 15
  match tag 20

```

Configuration R3-SPOKE1

```

hostname R2-HUB2
!
aaa new-model
!

```

```
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
  pool SPOKES
  route set interface
  route accept any tag 20
!
!
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  aaa authorization group psk list default default
  virtual-template 1
!
!
interface Loopback0
  ip address 10.0.2.1 255.255.255.255
!
interface Tunnel0
  ip address 10.0.0.2 255.255.255.0
  ip nhrp network-id 1
  ip nhrp redirect
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  tunnel source Ethernet0/2
  tunnel destination 192.168.0.1
!
interface Ethernet0/0
  ip address 172.16.0.2 255.255.255.0
!
interface Ethernet0/2
  ip address 192.168.0.2 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Templatel type tunnel
  ip unnumbered Loopback0
  ip nhrp network-id 1
  ip nhrp redirect
  tunnel protection ipsec profile default
!
router bgp 1
  bgp log-neighbor-changes
  bgp listen range 192.168.0.0/24 peer-group DC
  bgp listen range 10.0.2.0/24 peer-group SPOKES
  timers bgp 15 30
  neighbor SPOKES peer-group
  neighbor SPOKES remote-as 1
  neighbor DC peer-group
  neighbor DC remote-as 1
```

```

neighbor DC fall-over bfd
neighbor 10.0.0.1 remote-as 1
neighbor 10.0.0.1 fall-over bfd
!
address-family ipv4
redistribute connected
redistribute static route-map LOCALPREF
neighbor SPOKES activate
neighbor SPOKES route-map AGGR out
neighbor DC activate
neighbor DC route-reflector-client
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 route-reflector-client
exit-address-family
!
ip local pool SPOKES 10.0.2.2 10.0.2.254
ip forward-protocol nd
!
!
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
  match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
route-map LOCALPREF permit 10
  match tag 200
  set local-preference 100
!
route-map LOCALPREF permit 15
  match tag 20

```

Configuration R4-SPOKE2

```

hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability

```

```
!  
!  
crypto ikev2 authorization policy default  
  pool SPOKES  
  route set interface  
  route accept any tag 20  
!  
!  
crypto ikev2 profile default  
  match identity remote any  
  authentication remote pre-share key cisco  
  authentication local pre-share key cisco  
  aaa authorization group psk list default default  
  virtual-template 1  
!  
!  
interface Loopback0  
  ip address 10.0.2.1 255.255.255.255  
!  
interface Tunnel0  
  ip address 10.0.0.2 255.255.255.0  
  ip nhrp network-id 1  
  ip nhrp redirect  
  bfd interval 50 min_rx 50 multiplier 3  
  no bfd echo  
  tunnel source Ethernet0/2  
  tunnel destination 192.168.0.1  
!  
interface Ethernet0/0  
  ip address 172.16.0.2 255.255.255.0  
!  
interface Ethernet0/2  
  ip address 192.168.0.2 255.255.255.0  
  bfd interval 50 min_rx 50 multiplier 5  
!  
interface Virtual-Templatel type tunnel  
  ip unnumbered Loopback0  
  ip nhrp network-id 1  
  ip nhrp redirect  
  tunnel protection ipsec profile default  
!  
router bgp 1  
  bgp log-neighbor-changes  
  bgp listen range 192.168.0.0/24 peer-group DC  
  bgp listen range 10.0.2.0/24 peer-group SPOKES  
  timers bgp 15 30  
  neighbor SPOKES peer-group  
  neighbor SPOKES remote-as 1  
  neighbor DC peer-group  
  neighbor DC remote-as 1  
  neighbor DC fall-over bfd  
  neighbor 10.0.0.1 remote-as 1  
  neighbor 10.0.0.1 fall-over bfd  
!  
  address-family ipv4  
  redistribute connected  
  redistribute static route-map LOCALPREF  
  neighbor SPOKES activate  
  neighbor SPOKES route-map AGGR out  
  neighbor DC activate  
  neighbor DC route-reflector-client  
  neighbor 10.0.0.1 activate  
  neighbor 10.0.0.1 route-reflector-client  
  exit-address-family
```

```

!
ip local pool SPOKES 10.0.2.2 10.0.2.254
ip forward-protocol nd
!
!
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
  match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
route-map LOCALPREF permit 10
  match tag 200
  set local-preference 100
!
route-map LOCALPREF permit 15
  match tag 20

```

Configuration R5-AGGR1

```

hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
  pool SPOKES
  route set interface
  route accept any tag 20
!
!
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  aaa authorization group psk list default default
  virtual-template 1

```

```
!  
!  
interface Loopback0  
 ip address 10.0.2.1 255.255.255.255  
!  
interface Tunnel0  
 ip address 10.0.0.2 255.255.255.0  
 ip nhrp network-id 1  
 ip nhrp redirect  
 bfd interval 50 min_rx 50 multiplier 3  
 no bfd echo  
 tunnel source Ethernet0/2  
 tunnel destination 192.168.0.1  
!  
interface Ethernet0/0  
 ip address 172.16.0.2 255.255.255.0  
!  
interface Ethernet0/2  
 ip address 192.168.0.2 255.255.255.0  
 bfd interval 50 min_rx 50 multiplier 5  
!  
interface Virtual-Templatel type tunnel  
 ip unnumbered Loopback0  
 ip nhrp network-id 1  
 ip nhrp redirect  
 tunnel protection ipsec profile default  
!  
router bgp 1  
 bgp log-neighbor-changes  
 bgp listen range 192.168.0.0/24 peer-group DC  
 bgp listen range 10.0.2.0/24 peer-group SPOKES  
 timers bgp 15 30  
 neighbor SPOKES peer-group  
 neighbor SPOKES remote-as 1  
 neighbor DC peer-group  
 neighbor DC remote-as 1  
 neighbor DC fall-over bfd  
 neighbor 10.0.0.1 remote-as 1  
 neighbor 10.0.0.1 fall-over bfd  
!  
 address-family ipv4  
 redistribute connected  
 redistribute static route-map LOCALPREF  
 neighbor SPOKES activate  
 neighbor SPOKES route-map AGGR out  
 neighbor DC activate  
 neighbor DC route-reflector-client  
 neighbor 10.0.0.1 activate  
 neighbor 10.0.0.1 route-reflector-client  
 exit-address-family  
!  
 ip local pool SPOKES 10.0.2.2 10.0.2.254  
 ip forward-protocol nd  
!  
!  
 ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2  
 ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2  
 ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200  
 ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200  
!  
!  
 ip prefix-list AGGR seq 5 permit 192.168.0.0/16  
 ip prefix-list AGGR seq 10 permit 10.0.0.0/8  
!
```



```
route-map AGGR permit 10
  match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
route-map LOCALPREF permit 10
  match tag 200
  set local-preference 100
!
route-map LOCALPREF permit 15
  match tag 20
```

Configuration R6-AGGR2

```
hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
  pool SPOKES
  route set interface
  route accept any tag 20
!
!
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  aaa authorization group psk list default default
  virtual-template 1
!
!
interface Loopback0
  ip address 10.0.2.1 255.255.255.255
!
interface Tunnel0
  ip address 10.0.0.2 255.255.255.0
  ip nhrp network-id 1
  ip nhrp redirect
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  tunnel source Ethernet0/2
  tunnel destination 192.168.0.1
!
```

```
interface Ethernet0/0
 ip address 172.16.0.2 255.255.255.0
!
interface Ethernet0/2
 ip address 192.168.0.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Templatel type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 1
 bgp log-neighbor-changes
 bgp listen range 192.168.0.0/24 peer-group DC
 bgp listen range 10.0.2.0/24 peer-group SPOKES
 timers bgp 15 30
 neighbor SPOKES peer-group
 neighbor SPOKES remote-as 1
 neighbor DC peer-group
 neighbor DC remote-as 1
 neighbor DC fall-over bfd
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 fall-over bfd
!
 address-family ipv4
  redistribute connected
  redistribute static route-map LOCALPREF
  neighbor SPOKES activate
  neighbor SPOKES route-map AGGR out
  neighbor DC activate
  neighbor DC route-reflector-client
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 route-reflector-client
  exit-address-family
!
 ip local pool SPOKES 10.0.2.2 10.0.2.254
 ip forward-protocol nd
!
!
 ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
 ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
 ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
 ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
 ip prefix-list AGGR seq 5 permit 192.168.0.0/16
 ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
 route-map AGGR permit 10
  match ip address prefix-list AGGR
!
 route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
 route-map LOCALPREF permit 10
  match tag 200
  set local-preference 100
!
 route-map LOCALPREF permit 15
  match tag 20
```

Configuration R7-HOST (simulation d'HÔTE dans ce réseau)

```
hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500
!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
  pool SPOKES
  route set interface
  route accept any tag 20
!
!
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  aaa authorization group psk list default default
  virtual-template 1
!
!
interface Loopback0
  ip address 10.0.2.1 255.255.255.255
!
interface Tunnel0
  ip address 10.0.0.2 255.255.255.0
  ip nhrp network-id 1
  ip nhrp redirect
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  tunnel source Ethernet0/2
  tunnel destination 192.168.0.1
!
interface Ethernet0/0
  ip address 172.16.0.2 255.255.255.0
!
interface Ethernet0/2
  ip address 192.168.0.2 255.255.255.0
  bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  ip nhrp network-id 1
  ip nhrp redirect
  tunnel protection ipsec profile default
!
router bgp 1
  bgp log-neighbor-changes
```

```

bgp listen range 192.168.0.0/24 peer-group DC
bgp listen range 10.0.2.0/24 peer-group SPOKES
timers bgp 15 30
neighbor SPOKES peer-group
neighbor SPOKES remote-as 1
neighbor DC peer-group
neighbor DC remote-as 1
neighbor DC fall-over bfd
neighbor 10.0.0.1 remote-as 1
neighbor 10.0.0.1 fall-over bfd
!
address-family ipv4
redistribute connected
redistribute static route-map LOCALPREF
neighbor SPOKES activate
neighbor SPOKES route-map AGGR out
neighbor DC activate
neighbor DC route-reflector-client
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 route-reflector-client
exit-address-family
!
ip local pool SPOKES 10.0.2.2 10.0.2.254
ip forward-protocol nd
!
!
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
  match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
  match tag 500
  set local-preference 500
!
route-map LOCALPREF permit 10
  match tag 200
  set local-preference 100
!
route-map LOCALPREF permit 15
  match tag 20

```

Importantes notes de configuration

Voici quelques informations importantes au sujet des configurations qui sont décrites dans les sections précédentes :

- Le tunnel du Point à point GRE entre les deux Concentrateurs exigé pour que la Connectivité de spoke-to-spoke fonctionne dans tous les scénarios, inclure spécifiquement ces scénarios dans lesquels certains des rais est sont connectés seulement à un des Concentrateurs et à d'autres à un autre hub.
- **L'aucune** configuration de **bfd echo** dans l'interface de tunnel GRE entre les deux

Concentrateurs n'est exigée afin d'éviter l'indication du trafic qui est envoyée d'un autre hub. Le bfd echo a la mêmes source et adresse IP de destination, qui est égale à l'adresse IP du routeur qui envoie le bfd echo. Puisque ces paquets sont conduits de retour par le routeur qui répond, les indications du trafic de NHRP sont générées.

- En configuration BGP, le filtrage de route-map qui annonce les réseaux vers des rai n'est pas exigé, mais il rend les configurations plus optimales puisque seulement l'agrégat/routes récapitulatives sont annoncés :
`neighbor SPOKES route-map AGGR out`
- Sur les Concentrateurs, la configuration du **route-map LOCALPREF** est exigée afin d'installer la préférence locale appropriée BGP, et elle filtre les artères statiques redistribuées aux artères seulement de résumé et de mode de configuration IKEv2.
- Cette conception n'adresse pas la Redondance aux emplacements distants de bureau (rai). Si le lien WAN sur le rai descend, le VPN également ne fonctionne pas. Ajoutez un deuxième lien au routeur en étoile ou ajoutez un deuxième routeur en étoile dans le même emplacement afin d'aborder cette question.

En résumé, la conception de Redondance qui est présentée dans ce document peut être traitée comme alternative moderne à la caractéristique du basculement d'avec état (SSO) /Stateful. Il est fortement flexible et peut être réglé avec précision afin de répondre à vos exigences spécifiques de déploiement.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

[Informations connexes](#)

- [Fiche technique de FlexVPN de Cisco IOS](#)
- [Configurer FlexVPN a parlé au rai](#)
- [Support et documentation techniques - Cisco Systems](#)