Exemple de configuration de double concentrateur FlexVPN HA

Contenu

Introduction

Ce document décrit comment configurer une conception de redondance complète pour les bureaux distants qui se connectent à un centre de données via un VPN IPSec sur un support réseau non sécurisé, tel qu'Internet.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document sont basées sur les composants technologiques suivants :

- Border Gateway Protocol (BGP) comme protocole de routage au sein du data center et entre les rayons et les concentrateurs dans la superposition VPN.
- Bidirectional Forwarding Detection (BFD) comme mécanisme qui détecte les liaisons descendantes (routeur inactif) qui s'exécutent à l'intérieur du data center uniquement (et non sur les tunnels de superposition).
- Cisco IOS® FlexVPN entre les concentrateurs et les rayons, avec des fonctionnalités de rayon à rayon activées via une commutation à courte distance.
- Transmission tunnel GRE (Generic Routing Encapsulation) entre deux concentrateurs afin d'activer la communication de rayon à rayon, même lorsque les rayons sont connectés à différents concentrateurs.
- Suivi des objets amélioré et routes statiques liées aux objets suivis.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Lorsque vous concevez des solutions d'accès à distance pour le data center, la haute disponibilité (HA) est souvent une condition essentielle pour les applications utilisateur stratégiques.

La solution présentée dans ce document permet une détection et une récupération rapides des scénarios de panne dans lesquels un des concentrateurs de terminaison VPN tombe en panne en raison d'un rechargement, d'une mise à niveau ou d'un problème d'alimentation. Tous les routeurs des bureaux distants (rayons) utilisent ensuite l'autre concentrateur opérationnel immédiatement après la détection de cette défaillance.

Voici les avantages de cette conception :

- Récupération rapide du réseau à partir d'un scénario de concentrateur VPN
- Aucune synchronisation avec état compliquée (telles que les associations de sécurité IPSec (SA), les SA ISAKMP (Internet Security Association and Key Management Protocol) et le cryptage de routage) entre les concentrateurs VPN
- Aucun problème d'anti-relecture dû aux retards dans la synchronisation du numéro de séquence ESP (Encapsulating Security Payload) avec IPSec Stateful HA
- Les concentrateurs VPN peuvent utiliser différents logiciels ou matériels basés sur Cisco IOS/IOS-XE
- Options d'implémentation d'équilibrage de charge flexibles avec BGP comme protocole de routage qui s'exécute dans la superposition VPN

- Routage clair et lisible sur tous les périphériques sans mécanismes cachés qui s'exécutent en arrière-plan
- Connectivité directe satellite à satellite
- Tous les avantages de FlexVPN, notamment l'intégration AAA (Authentication, Authorization, and Accounting) et la qualité de service (QoS) par tunnel

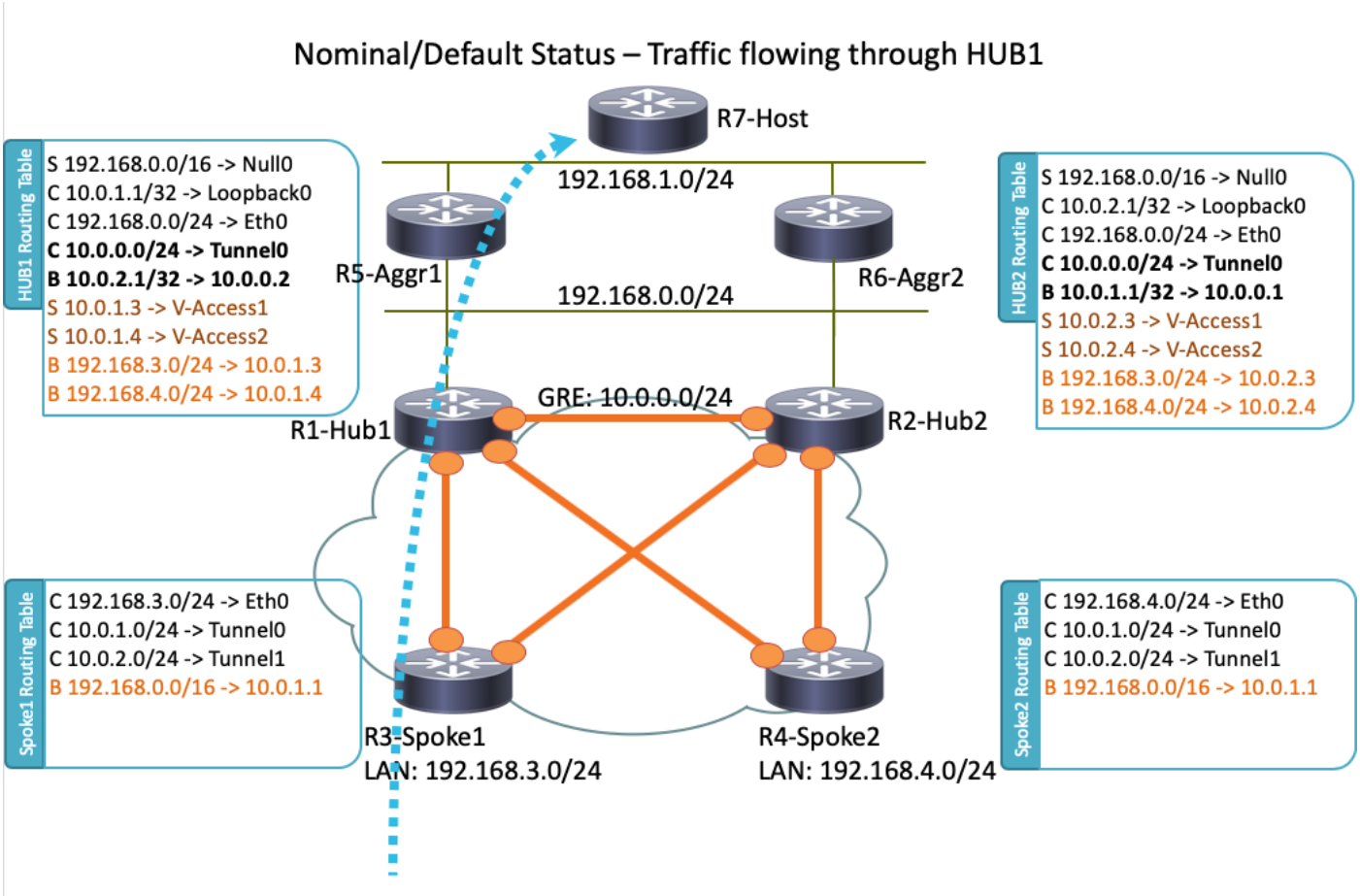
Configuration

Cette section fournit des exemples de scénarios et décrit comment configurer une conception de redondance complète pour les bureaux distants qui se connectent au data center via un VPN IPSec sur un support réseau non sécurisé.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Voici la topologie de réseau utilisée dans ce document :



> **Note**: Tous les routeurs utilisés dans cette topologie exécutent Cisco IOS version 15.2(4)M1 et le nuage Internet utilise un schéma d'adresses de 172.16.0.0/24.

Scénario opérationnel régulier

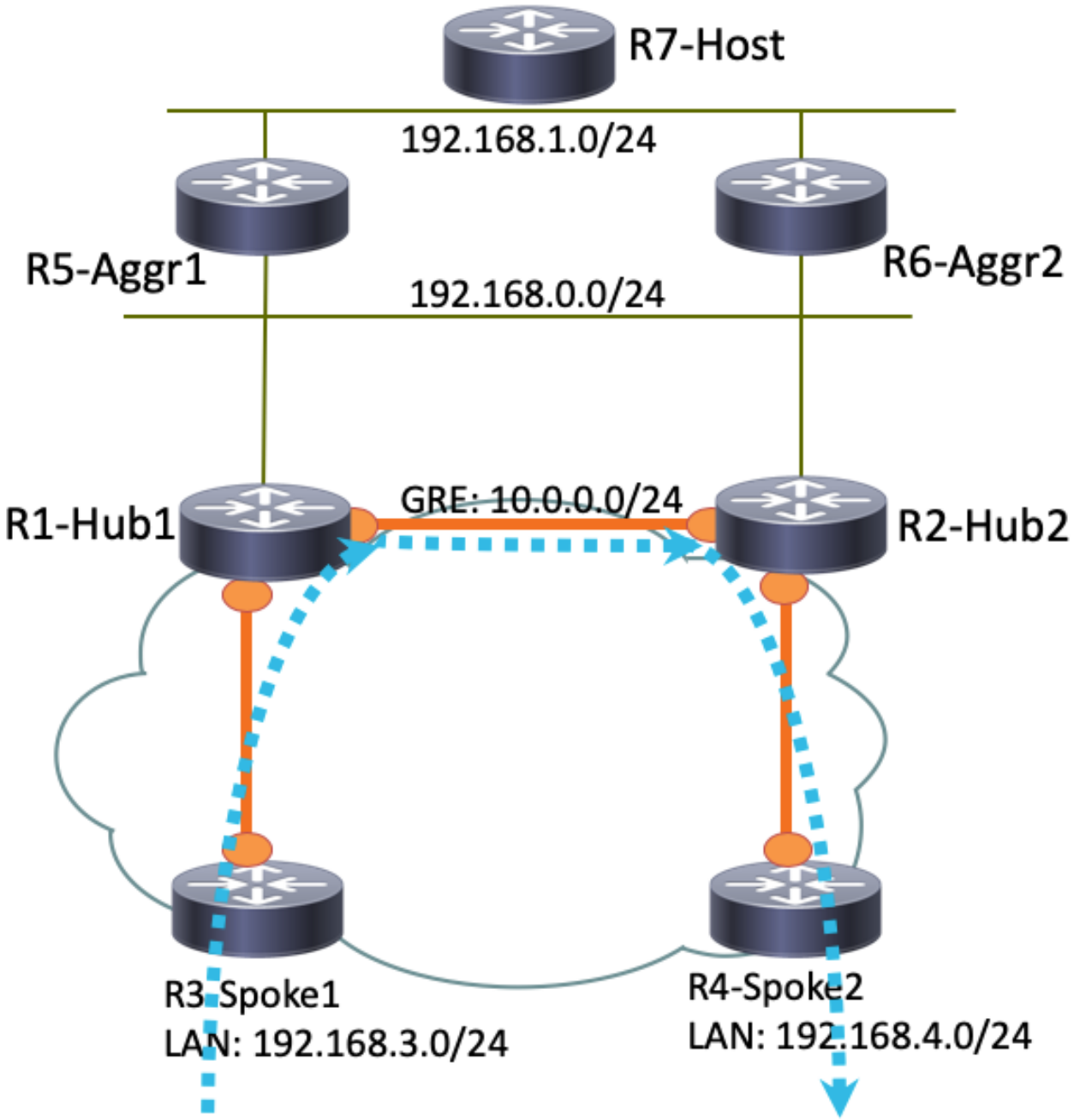
Dans un scénario de fonctionnement normal, lorsque tous les routeurs sont opérationnels, tous les routeurs en étoile acheminent l'ensemble du trafic via le concentrateur par défaut (R1-HUB1). Cette préférence de routage est obtenue lorsque la préférence locale BGP par défaut est définie sur 200 (reportez-vous aux sections suivantes pour plus de détails). Ceci peut être ajusté en fonction des exigences de déploiement, telles que l'équilibrage de charge du trafic.

Spoke-to-Spoke (raccourci)

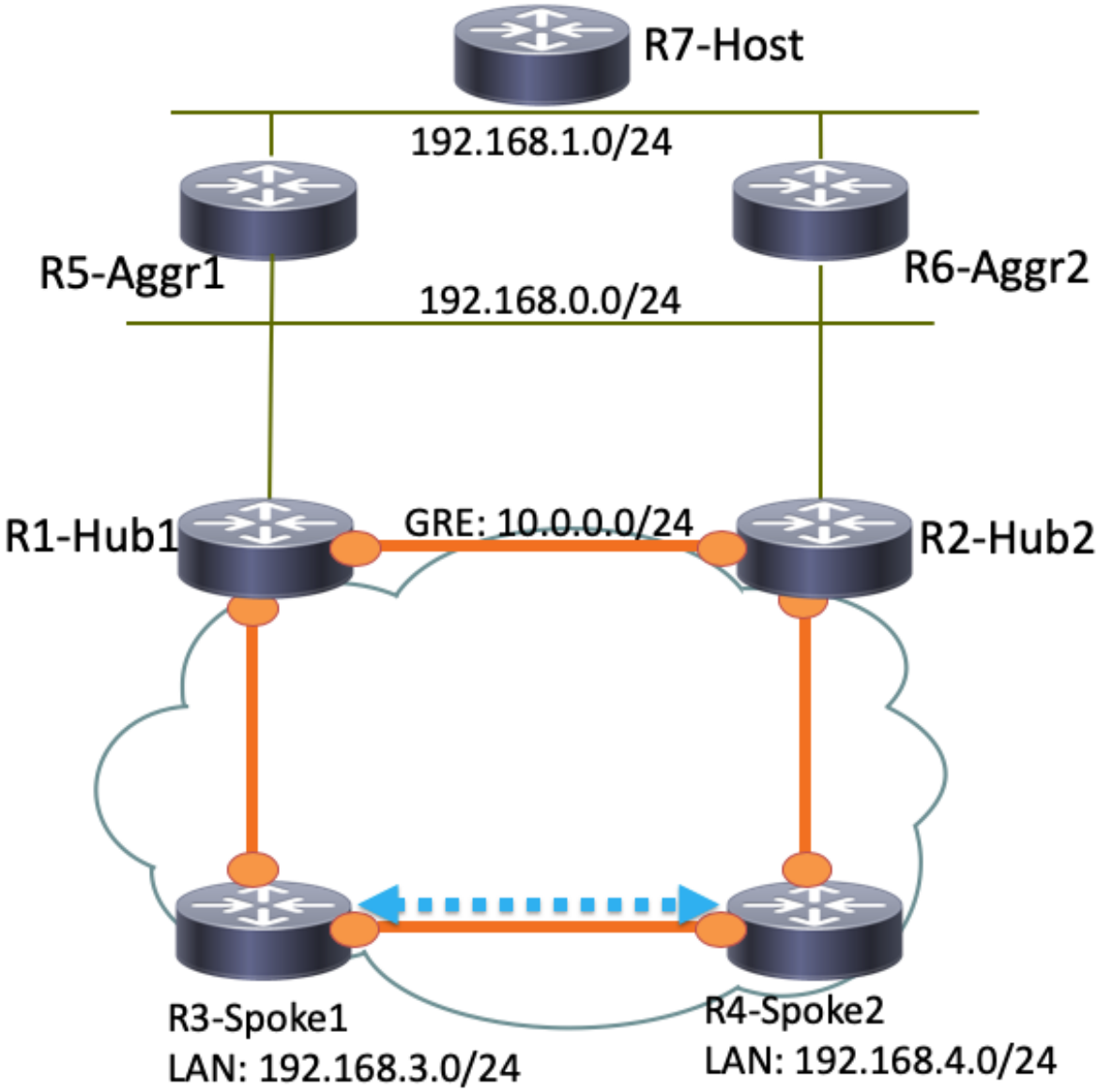
Si R3-Spoke1 initie une connexion à R4-Spoke2, un tunnel de rayon à rayon dynamique est créé avec la configuration de commutation de raccourci.

> **Astuce** : Pour plus d'informations, reportez-vous au guide de configuration Configuration de FlexVPN Spoke to Spoke.

Si R3-Spoke1 est connecté uniquement à R1-HUB1 et que R4-Spoke2 est connecté uniquement à R2-HUB2, une connexion directe de rayon à rayon peut toujours être établie avec le tunnel GRE point à point qui s'exécute entre les concentrateurs. Dans ce cas, le chemin de trafic initial entre R3-Spoke1 et R4-Spoke2 semble similaire à ceci :



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



Tables de routage et sorties pour un scénario opérationnel régulier

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

```
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 la création du tunnel en étoile avec R4-SPOKE2 :

```
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, Tunnel1
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, Tunnel1
C        10.0.2.3/32 is directly connected, Tunnel1
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 comporte deux entrées pour le réseau 192.168.0.0/16 avec des préférences locales différentes (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 :

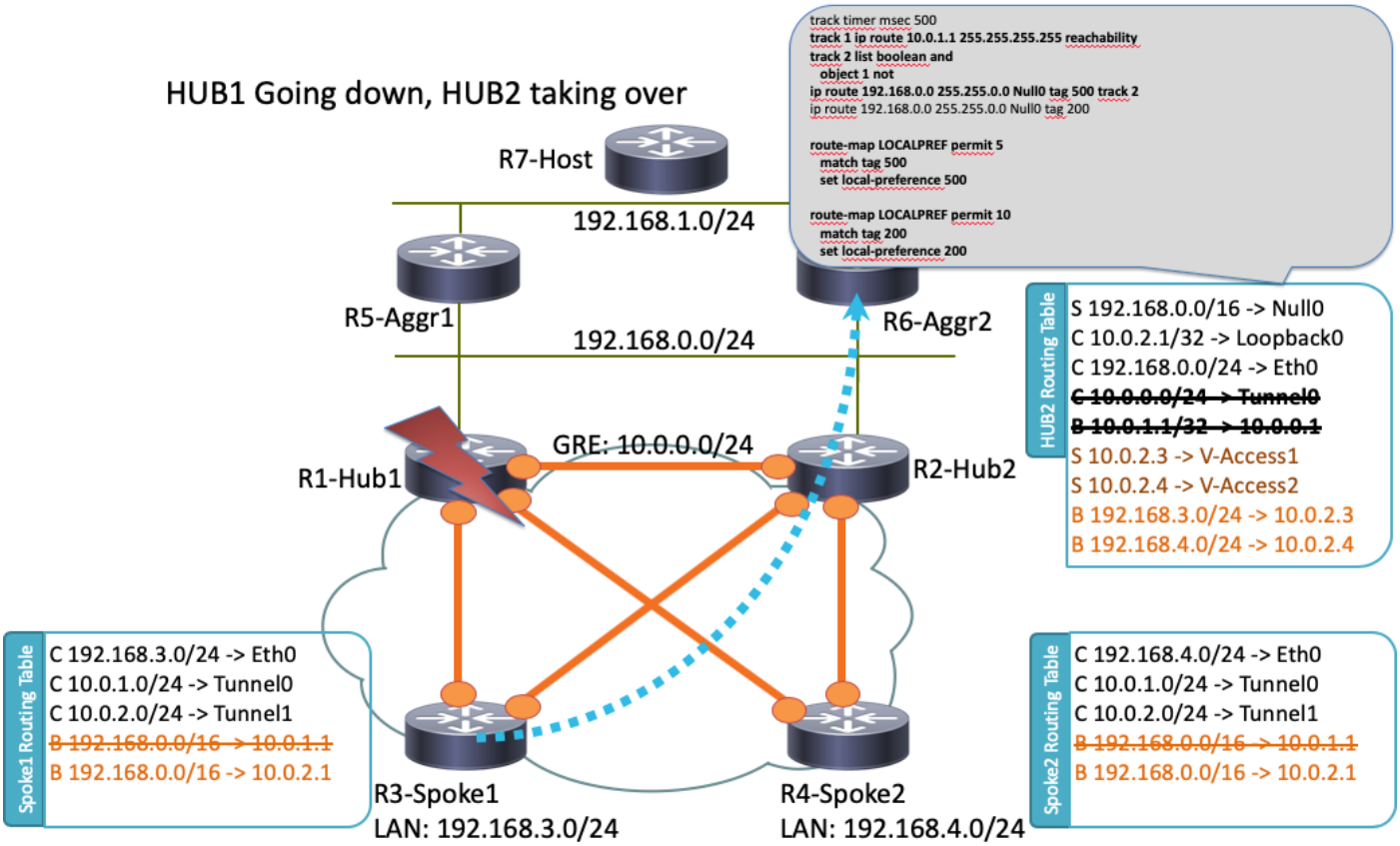
```
R5-LAN1#show ip route
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 192.168.0.1, 00:07:22
B        10.0.0.0/24 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.1/32 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.3/32 [200/0] via 192.168.0.1, 00:07:17
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 défaillance HUB1

Voici un scénario d'arrêt de R1-HUB1 (en raison d'actions telles que des pannes de courant ou une mise à niveau) :



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

1. Le BFD sur R2-HUB2 et sur les routeurs agrégés LAN R5-AGGR1 et R6-AGGR2 détecte l'état down de R1-HUB1. En conséquence, le voisinage BGP s'effondre immédiatement.

2. La détection d'objet de piste pour R2-HUB2 qui détecte la présence du bouclage R1-HUB1 est désactivée (Piste 1 dans l'exemple de configuration).

3. Cet objet suivi désactivé déclenche une autre piste à monter (Logical NOT). Dans cet exemple, la piste 2 monte chaque fois que la piste 1 tombe en panne.

4. Cela déclenche l'ajout d'une entrée de routage IP statique à la table de routage en raison d'une valeur inférieure à 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 routes statiques avec une préférence locale BGP supérieure à la valeur définie pour R1-HUB1. Dans cet exemple, une préférence locale de **500** est utilisée dans le scénario d'échec, au lieu du **200** défini 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 le voir dans les sorties BGP. Notez que l'entrée de 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. Àce stade, les deux rayons (R3-Spoke1 et R4-Spoke2) commencent à envoyer du trafic à R2-HUB2. Toutes ces étapes doivent se dérouler en une seconde. Voici la table de routage sur Spoke 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. Les sessions BGP ultérieures entre les rayons et R1-HUB1 s'arrêtent et la détection DPD (Dead Peer Detection) supprime les tunnels IPSec terminés sur R1-HUB1. Cependant, cela n’a pas d’impact sur le transfert de trafic, puisque R2-HUB2 est déjà utilisé comme passerelle principale de terminaison de tunnel :

```
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 exemples de configuration pour les concentrateurs et les rayons utilisés dans cette topologie.

Configuration de R1-HUB

```
version 15.4
!
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-Template1 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 de 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-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
```

Configuration de R3-SPOKE1

```
hostname R3-SPOKE1
!
aaa new-model
!
aaa authorization network default local
!
!
crypto ikev2 authorization policy default
 route set interface
!
!
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 dpd 10 2 on-demand
 aaa authorization group psk list default default
!
! Tunnel to the HUB1
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
! Tunnel to the HUB2
!
interface Tunnel1
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
interface Ethernet0/0
description INTERNET-CLOUD
 ip address 172.16.0.3 255.255.255.0
!
interface Ethernet0/1
description LAN
 ip address 192.168.3.3 255.255.255.0
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet0/1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel protection ipsec profile default
!
router bgp 1
 bgp log-neighbor-changes
```

```
 timers bgp 15 30
 neighbor 10.0.1.1 remote-as 1
 neighbor 10.0.2.1 remote-as 1
 !
 address-family ipv4
 network 192.168.3.0
 neighbor 10.0.1.1 activate
 neighbor 10.0.2.1 activate
 exit-address-family
```

Configuration de R4-SPOKE2

```
hostname R4-SPOKE2
!
aaa new-model
!
aaa authorization network default local
!
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 dpd 10 2 on-demand
 aaa authorization group psk list default default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 172.16.0.4 255.255.255.0
!
interface Ethernet0/1
 ip address 192.168.4.4 255.255.255.0
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet0/1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 2
 tunnel protection ipsec profile default
!
router bgp 1
 bgp log-neighbor-changes
 timers bgp 15 30
 neighbor 10.0.1.1 remote-as 1
 neighbor 10.0.2.1 remote-as 1
```

```
 !
 address-family ipv4
 network 192.168.4.0
 neighbor 10.0.1.1 activate
 neighbor 10.0.2.1 activate
 exit-address-family
!
```

Configuration de R5-AGGR1

```
hostname R5-LAN1
!
no aaa new-model
!
!
interface Loopback0
 ip address 10.0.5.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.5 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
! HSRP configuration on the LAN side
!
interface Ethernet0/1
 ip address 192.168.1.5 255.255.255.0
 standby 1 ip 192.168.1.254
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 1
 neighbor 192.168.0.1 fall-over bfd
 neighbor 192.168.0.2 remote-as 1
 neighbor 192.168.0.2 fall-over bfd
 !
 address-family ipv4
 redistribute connected
 redistribute static
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.2 activate
 exit-address-family
```

Configuration de R6-AGGR2

```
hostname R6-LAN2
!
interface Loopback0
 ip address 10.0.6.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.6 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
interface Ethernet0/1
 ip address 192.168.1.6 255.255.255.0
 standby 1 ip 192.168.1.254
 standby 1 priority 200
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 1
```

```
 neighbor 192.168.0.1 fall-over bfd
 neighbor 192.168.0.2 remote-as 1
 neighbor 192.168.0.2 fall-over bfd
 !
 address-family ipv4
 redistribute connected
 redistribute static
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.2 activate
 exit-address-family
!
```

Configuration de R7-HOST (simulation de l'hôte dans ce réseau)

```
hostname R7-HOST
!
no aaa new-model
!
interface Ethernet0/0
 ip address 192.168.1.7 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

Remarques importantes sur la configuration

Voici quelques remarques importantes sur les configurations décrites dans les sections précédentes :

- Le tunnel GRE point à point entre les deux concentrateurs est nécessaire pour que la connectivité de rayon à rayon fonctionne dans tous les scénarios, en particulier pour inclure les scénarios dans lesquels certains rayons sont connectés uniquement à l'un des concentrateurs et d'autres à un autre concentrateur.

- La configuration **no bfd echo** dans l'interface de tunnel GRE entre les deux concentrateurs est requise afin d'éviter l'indication de trafic qui est envoyée depuis un autre concentrateur. L'écho BFD a la même adresse IP source et de destination, qui est égale à l'adresse IP du routeur qui envoie l'écho BFD. Puisque ces paquets sont routés par le routeur qui répond, les indications de trafic NHRP sont générées.

- Dans la configuration BGP, le filtrage de route-map qui annonce les réseaux vers des rayons n'est pas nécessaire, mais il rend les configurations plus optimales, car seules les routes agrégées/récapitulatives sont annoncées :

  neighbor SPOKES route-map AGGR out

- Sur les concentrateurs, la configuration **LOCALPREF de la route-map** est requise pour configurer la préférence locale BGP appropriée, et elle filtre les routes statiques redistribuées uniquement vers les routes récapitulatives et les routes en mode de configuration IKEv2.

- Cette conception ne traite pas de la redondance sur les sites des bureaux distants (en étoile). Si la liaison WAN sur le satellite tombe en panne, le VPN ne fonctionne pas non plus. Ajoutez une deuxième liaison au routeur en étoile ou un deuxième routeur en étoile au même emplacement afin de résoudre ce problème.

En résumé, la conception de redondance présentée dans ce document peut être traitée comme une alternative moderne à la fonctionnalité de commutation avec état (SSO)/avec état. Il est extrêmement flexible et peut être affiné afin de répondre à vos besoins spécifiques de déploiement.

Vérification

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

Dépannage

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

Informations connexes

- Fiche technique Cisco IOS FlexVPN
- Configuration de FlexVPN Spoke pour Spoke
- Support et documentation techniques - Cisco Systems