Esempio di configurazione di FlexVPN HA Dual Hub

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Premesse
- Configurazione
  - Esempio di rete
  - Scenario operativo regolare
  - Spoke-to-Spoke (collegamento)
  - Tabelle e output di routing per uno scenario operativo regolare
  - Scenario di errore HUB1
  - Configurazioni
    - Configurazione di R1-HUB
    - Configurazione R2-HUB2
    - Configurazione R3-SPOKE1
    - Configurazione R4-SPOKE2
    - Configurazione R5-AGGR1
    - Configurazione R6-AGGR2
    - Configurazione di R7-HOST (simulazione dell'HOST nella rete)
  - Note importanti sulla configurazione
- Verifica
- Risoluzione dei problemi
- Informazioni correlate

Introduzione

In questo documento viene descritto come configurare una struttura di ridondanza completa per gli uffici remoti che si connettono a un data center tramite VPN basata su IPSec su un supporto di rete non sicuro, ad esempio Internet.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sui seguenti componenti tecnologici:

- Border Gateway Protocol (BGP) come protocollo di routing all'interno del data center e tra spoke e hub nella VPN overlay.
- BFD (Bidirectional Forwarding Detection) è un meccanismo che rileva i collegamenti non attivi (router inattivo) che vengono eseguiti solo all'interno del data center (non sui tunnel di sovrapposizione).
- Cisco IOS® FlexVPN tra hub e spoke, con funzionalità spoke-to-spoke abilitate tramite switching di collegamento.
- Tunneling GRE (Generic Routing Encapsulation) tra due hub per abilitare la comunicazione spoke, anche quando gli spoke sono connessi a hub diversi.
- Tracciamento avanzato degli oggetti e route statiche collegate agli oggetti tracciati.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si progettano soluzioni di accesso remoto per il centro dati, l'alta disponibilità (HA, High Availability) è spesso un requisito chiave per le applicazioni utente mission-critical.

La soluzione presentata in questo documento consente il rilevamento e il ripristino rapido in caso di guasto in cui uno degli hub VPN terminanti si guasti a causa di un ricaricamento, un aggiornamento o un problema di alimentazione. Tutti i router (spoke) degli uffici remoti utilizzano quindi l'altro hub operativo immediatamente dopo il rilevamento di tale guasto.

Ecco i vantaggi di questo design:

- Ripristino rapido della rete da uno scenario di hub-down VPN
- Nessuna complicata sincronizzazione stateful, ad esempio associazioni di sicurezza IPSec, associazioni di sicurezza Internet Security Association and Key Management Protocol (ISAKMP) e routing crittografato, tra gli hub VPN
- Nessun problema di anti-replay a causa di ritardi nella sincronizzazione del numero di sequenza ESP (Encapsulating Security Payload) con HA stateful IPSec
- Gli hub VPN possono utilizzare hardware o software basati su Cisco IOS/IOS-XE diversi
- Scelte flessibili di implementazione per il bilanciamento del carico con BGP come protocollo di routing in esecuzione nella sovrimpressione VPN

- Routing chiaro e leggibile su tutti i dispositivi senza meccanismi nascosti in esecuzione in background
- Connettività spoke-to-spoke diretta
- Tutti i vantaggi di FlexVPN, per includere l'integrazione di autenticazione, autorizzazione e accounting (AAA) e QoS (Quality of Service) per tunnel

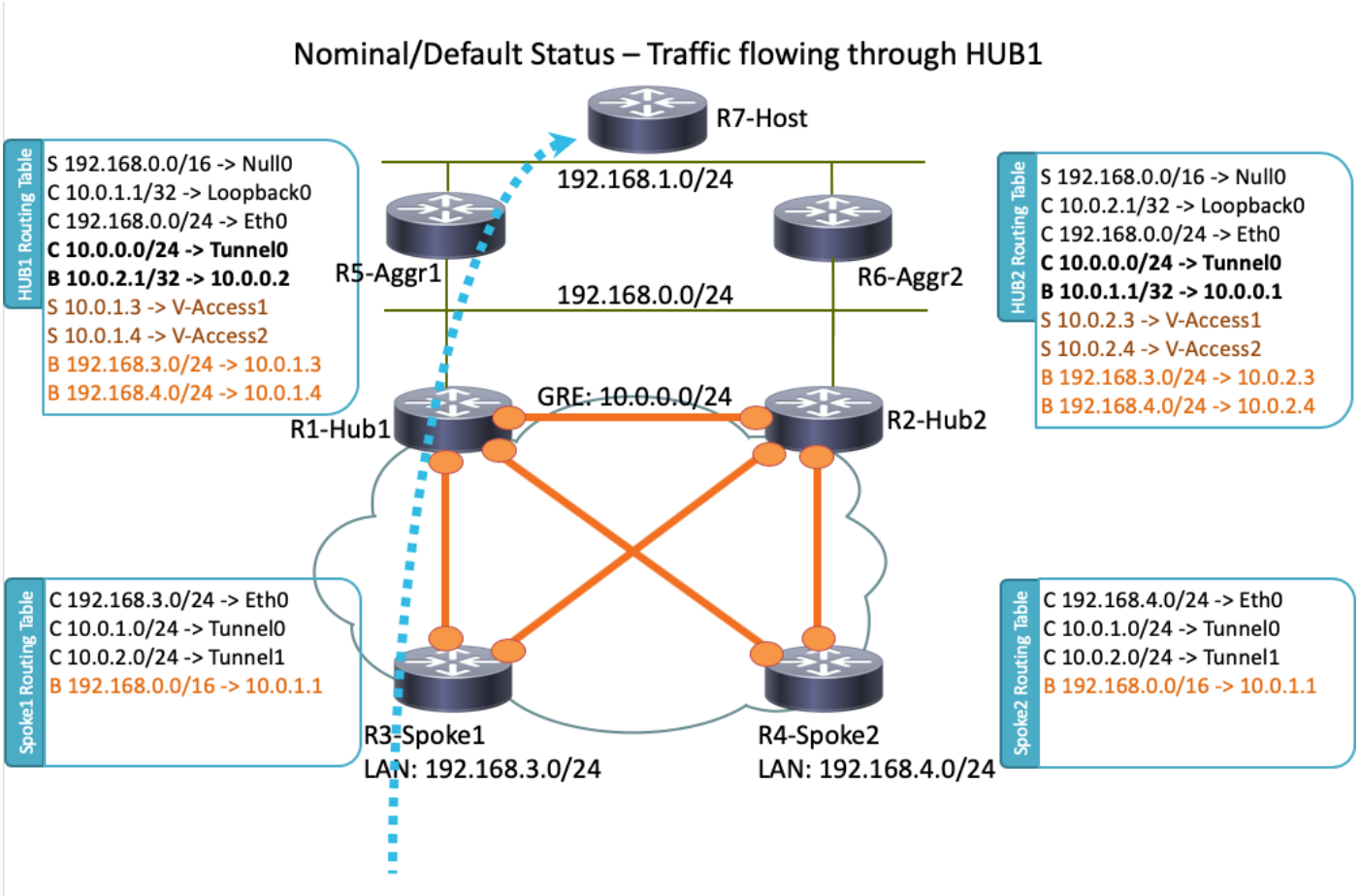
Configurazione

In questa sezione vengono illustrati alcuni scenari di esempio e viene descritto come configurare una struttura di ridondanza completa per gli uffici remoti che si connettono al centro dati tramite VPN basata su IPSec su un supporto di rete non protetto.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Questa è la topologia di rete utilizzata nel presente documento:



Nota: Tutti i router utilizzati in questa topologia eseguono Cisco IOS versione 15.2(4)M1 e Internet Cloud utilizza uno schema di indirizzi di 172.16.0.0/24.

Scenario operativo regolare

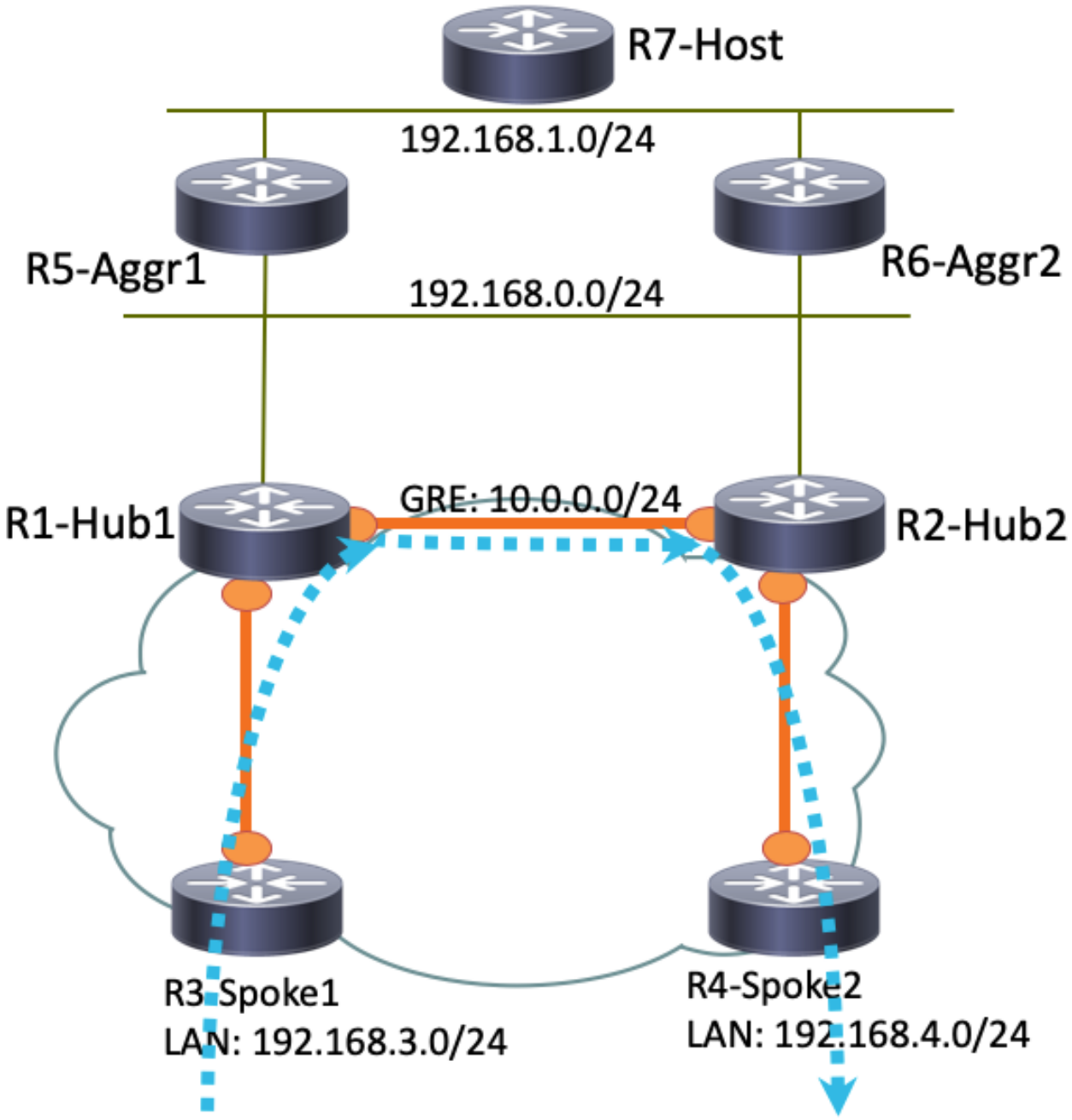
In uno scenario operativo normale, quando tutti i router sono attivi e operativi, tutti i router spoke indirizzano tutto il traffico attraverso l'hub predefinito (R1-HUB1). Questa preferenza di routing viene raggiunta quando la preferenza locale BGP predefinita è impostata su 200 (per ulteriori informazioni, fare riferimento alle sezioni che seguono). Questa preferenza può essere modificata in base ai requisiti di distribuzione, ad esempio il bilanciamento del carico del traffico.

Spoke-to-Spoke (collegamento)

Se R3-Spoke1 avvia una connessione a R4-Spoke2, viene creato un tunnel spoke dinamico con la configurazione di commutazione tramite collegamento.

Suggerimento: Per ulteriori informazioni, consultare la guida alla configurazione di FlexVPN Spoke to Spoke.

Se R3-Spoke1 è connesso solo a R1-HUB1 e R4-Spoke2 è connesso solo a R2-HUB2, è comunque possibile ottenere una connessione spoke diretta con il tunnel GRE point-to-point in esecuzione tra gli hub. In questo caso, il percorso iniziale del traffico tra R3-Spoke1 e R4-Spoke2 sarà simile al seguente:



Poiché R1-Hub1 riceve il pacchetto sull'interfaccia di accesso virtuale, che ha lo stesso ID di rete NHRP (Next Hop Resolution Protocol) di quello del tunnel GRE, l'indicazione del traffico viene inviata al router R3-Spoke1. In questo modo viene attivata la creazione dinamica del tunnel spoke:

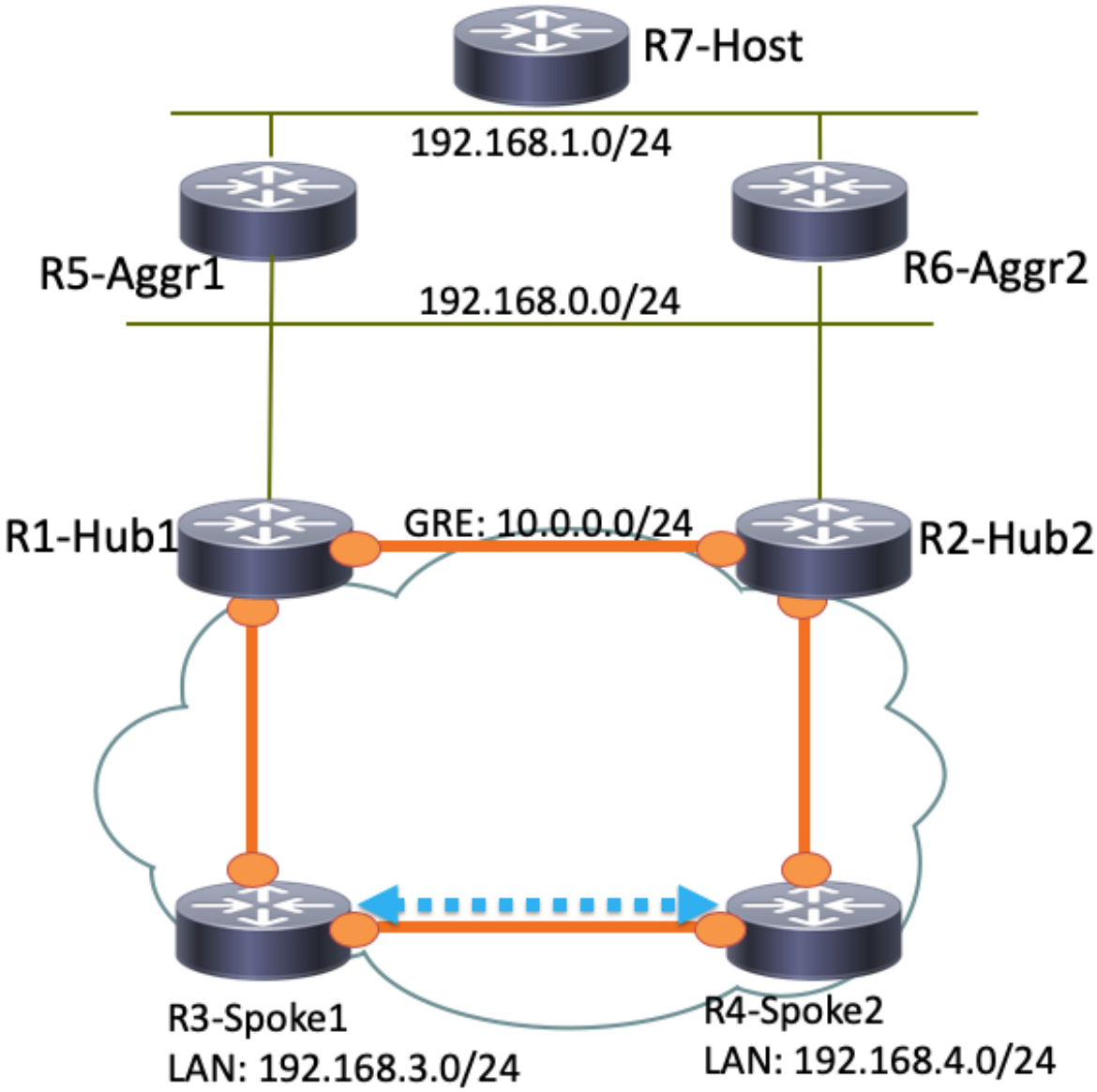


Tabelle e output di routing per uno scenario operativo regolare

Di seguito è riportata la tabella di routing R1-HUB1 in uno scenario operativo normale:

<#root>

```
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
```

Di seguito è riportata la tabella di routing R3-SPOKE1 in uno scenario operativo normale dopo la creazione del tunnel spoke-to-spoke con R4-SPOKE2:

<#root>

```
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
```

Su R3-Spoke1, la tabella BGP ha due voci per la rete 192.168.0.0/16 con preferenze locali diverse (preferibilmente R1-Hub1):

<#root>

```
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
```

Di seguito è riportata la tabella di routing R5-AGGR1 in uno scenario operativo normale:

<#root>

```
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
```

Di seguito è riportata la tabella di routing R7-HOST in uno scenario operativo normale:

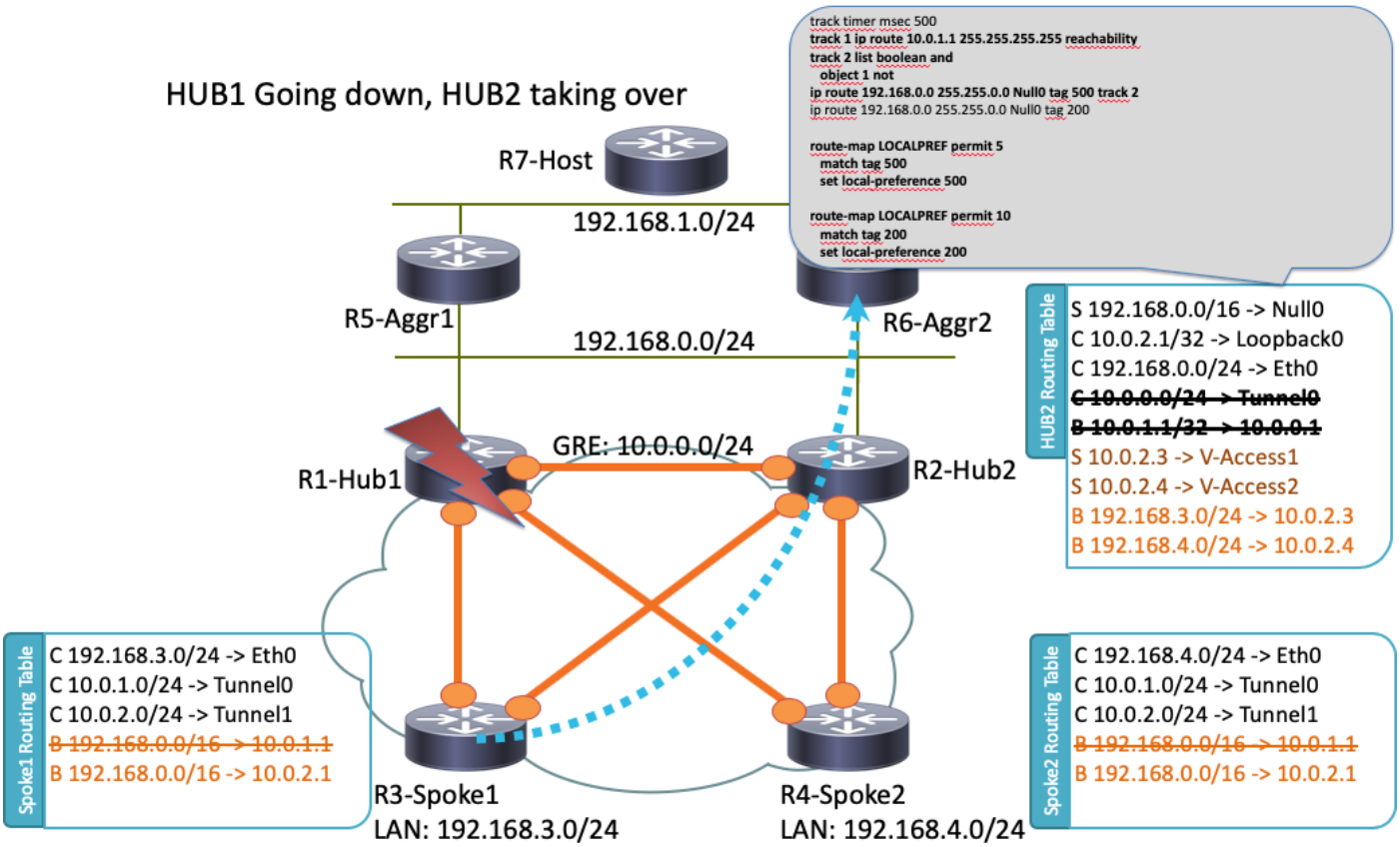
<#root>

```
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
```

Scenario di errore HUB1

Di seguito è riportato uno scenario di interruzione di R1-HUB1 (a causa di azioni quali interruzioni dell'alimentazione o un aggiornamento):



In questo scenario si verifica la sequenza di eventi seguente:

1. Il BFD su R2-HUB2 e sui router aggregati LAN R5-AGR1 e R6-AGR2 rilevano lo stato di inattività di R1-HUB1. Di conseguenza, il vicinato BGP si blocca immediatamente.

2. Il rilevamento oggetti traccia per R2-HUB2 che rileva la presenza del loopback R1-HUB1 si interrompe (traccia 1 nella configurazione di esempio).

3. Questo oggetto registrato abbassato attiva un'altra traccia (NOT logico). In questo esempio, il Track 2 diventa attivo ogni volta che il Track 1 diventa inattivo.

4. In questo modo, viene aggiunta una voce di routing IP statico alla tabella di routing a causa di un valore inferiore alla distanza amministrativa predefinita. Di seguito è riportata la configurazione rilevante:

<#root>

```
! 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 ridistribuisce queste route statiche con una preferenza BGP locale maggiore del valore impostato per R1-HUB1. In questo esempio viene utilizzata una preferenza locale di 500 nello scenario di errore, anziché la preferenza 200 impostata da R1-HUB1:

<#root>

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


!
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 200


!
```

Su R3-Spoke1, questo è visibile nelle uscite BGP. Si noti che la voce R1 esiste ancora, ma non viene utilizzata:

<#root>

```
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. A questo punto, entrambi i raggi (R3-Spoke1 e R4-Spoke2) iniziano a inviare traffico a R2-HUB2. Tutti questi passaggi devono avvenire entro un secondo. Di seguito è riportata la tabella di routing per il raggio 3:

<#root>

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. Le sessioni BGP successive tra gli spoke e R1-HUB1 si interrompono e il DPD (Dead Peer Detection) rimuove i tunnel IPSec terminati su R1-HUB1. Tuttavia, ciò non influisce sull'inoltro del traffico, poiché R2-HUB2 è già utilizzato come gateway principale che termina il tunnel:

<#root>

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
```

Configurazioni

In questa sezione vengono fornite configurazioni di esempio per gli hub e gli spoke utilizzati in questa topologia.

Configurazione di R1-HUB

<#root>

```
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
```

Configurazione R2-HUB2

<#root>

```
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
```

Configurazione 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
```

Configurazione 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
!
```

Configurazione 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
```

Configurazione 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
!
```

Configurazione di R7-HOST (simulazione dell'HOST nella rete)

```
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
```

Note importanti sulla configurazione

Di seguito sono riportate alcune note importanti sulle configurazioni descritte nelle sezioni precedenti:

- Il tunnel GRE point-to-point tra i due hub è necessario per il funzionamento della connettività spoke in tutti gli scenari, in particolare per includere gli scenari in cui alcuni spoke sono connessi solo a uno degli hub e altri a un altro hub.

- Per evitare la segnalazione del traffico inviato da un altro hub, è necessario configurare l'eco no bfd nell'interfaccia del tunnel GRE tra i due hub. L'eco BFD ha lo stesso indirizzo IP di origine e di destinazione, che è uguale all'indirizzo IP del router che invia l'eco BFD. Poiché questi pacchetti vengono reindirizzati dal router che risponde, vengono generate le indicazioni del traffico NHRP.

- Nella configurazione BGP, il filtro route-map che annuncia le reti verso lo spoke non è richiesto, ma rende le configurazioni più ottimali poiché vengono annunciate solo le route di aggregazione/riepilogo:

  <#root>

  neighbor SPOKES route-map AGGR out

- Sugli hub, la configurazione route-map LOCALPREF è necessaria per impostare la preferenza locale BGP appropriata e filtra le route statiche ridistribuite solo alle route in modalità di configurazione riepilogo e IKEv2.

- Questa progettazione non riguarda la ridondanza nelle sedi di uffici remoti (spoke). Se il collegamento WAN sullo spoke si interrompe, anche la VPN non funziona. Per risolvere il problema, aggiungere un secondo collegamento al router spoke o aggiungere un secondo router spoke nella stessa posizione.

In sintesi, il progetto di ridondanza presentato in questo documento può essere trattato come un'alternativa moderna alla funzione di passaggio con stato (SSO)/con stato. È estremamente flessibile e può essere ottimizzato per soddisfare i requisiti di installazione specifici.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Scheda tecnica di Cisco IOS FlexVPN
- Configurazione di FlexVPN Spoke to Spoke
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).