

Exemplo de configuração do hub dual de FlexVPN HA

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes usados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Encenação operacional regular](#)

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

[Tabelas de roteamento e saídas para a encenação operacional regular](#)

[Cenário de falha de HUB1](#)

[Configurações](#)

[Configuração R1-HUB](#)

[Configuração R2-HUB2](#)

[Configuração R3-SPOKE1](#)

[Configuração R4-SPOKE2](#)

[Configuração R5-AGGR1](#)

[Configuração R6-AGGR2](#)

[Configuração R7-HOST \(simulação do HOST nessa rede\)](#)

[Notas de configuração importantes](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar um projeto da redundância direta para os escritórios remotos que conectam a um centro de dados através do VPN IPsec-baseado sobre um media da rede insegura, tal como o Internet.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes usados

A informação neste documento é baseada nestes componentes da tecnologia:

- [Border Gateway Protocol \(BGP\)](#) como o protocolo de roteamento dentro do centro de dados e entre o spokes e o Hubs na folha de prova VPN.
- [Detecção bidirecional da transmissão \(BFD\)](#) como um mecanismo que detecte abaixo dos links (roteador para baixo) que são executados dentro do centro de dados somente (não sobre os túneis da folha de prova).
- [® FlexVPN do Cisco IOS](#) entre o Hubs e o spokes, com as capacidades spoke-to-spoke permitidas através de short-cut o interruptor.
- [Generic Routing Encapsulation \(GRE\) que escava um túnel](#) entre dois Hubs a fim permitir uma comunicação spoke-to-spoke, mesmo quando o spokes é conectado ao Hubs diferente.
- [Rastreamento de objetos aumentado](#) e rotas estáticas amarrados aos objetos seguidos.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Quando você projeta soluções de acesso remoto para o centro de dados, a Alta disponibilidade (HA) é frequentemente uma exigência chave para aplicativos de usuário da missão crítica.

A solução que é apresentada neste documento permite a detecção e a recuperação rápidas dos cenários de falha em qual do Hubs determinação vai abaixo de devido a um reload, a uma elevação, ou a uns problemas de energia. Todo o Roteadores dos escritórios remotos (spokes) usa então o outro hub operacional imediatamente após detecção de tal falha.

Estão aqui as vantagens deste projeto:

- Recuperação rápida da rede de uma encenação do hub-para baixo VPN
- Nenhuma sincronizações complicadas do stateful (tais como as associações de segurança IPsec (SA), o Internet Security Association and Key Management Protocol (ISAKMP) SA, e o Cripto-roteamento) entre o Hubs VPN
- Nenhum problema devido da anti-repetição aos atrasos na sincronização do número de sequência do Encapsulating Security Payload (ESP) com stateful HA do IPsec
- O Hubs VPN pode usar o hardware ou o software baseado IOS/IOS-XE diferente de Cisco

- Escolhas flexíveis da aplicação da função de balanceamento de carga com o BGP como o protocolo de roteamento que é executado na folha de prova VPN
- Roteamento claro e legível em todos os dispositivos sem hidden os mecanismos que são executado no fundo
- Conectividade spoke-to-spoke direta
- Todas as vantagens de [FlexVPN](#), para incluir o Qualidade de Serviço (QoS) da integração e do por-túnel do Authentication, Authorization, and Accounting (AAA)

Configurar

Esta seção fornece exemplos de cenário e descreve como configurar um projeto da redundância direta para os escritórios remotos que conectam ao centro de dados através do VPN IPsec-baseado sobre um media da rede insegura.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Esta é a topologia de rede que é usada neste documento:

Nota: Todo o Roteadores que é usado nesta topologia executa a versão do Cisco IOS 15.2(4)M1, e a nuvem do Internet usa um esquema de endereço de 172.16.0.0/24.

Encenação operacional regular

Em uma encenação operacional normal, quando todo o Roteadores é ascendente e operacional, todo o Roteadores do spoke distribui todo o tráfego através do hub do padrão (R1-HUB1). Esta preferência do roteamento é conseguida quando a preferência local do padrão BGP é ajustada a 200 (refira as seções que seguem para detalhes). Isto pode ser ajustado com base nas exigências do desenvolvimento, tais como a função de balanceamento de carga do tráfego.

Spoke-to-spoke (atalho)

Se R3-Spoke1 inicia uma conexão a R4-Spoke2, um túnel spoke-to-spoke dinâmico está criado com a configuração do interruptor do atalho.

Dica: Para mais detalhes, refira o [FlexVPN configurando falou ao](#) guia de [configuração de](#)

[raio](#).

Se R3-Spoke1 está conectado somente a R1-HUB1, e R4-Spoke2 está conectado somente a R2-HUB2, uma conexão spoke-to-spoke direta pode ainda ser conseguida com o túnel GRE ponto a ponto que é executado entre os Hubs. Neste caso, o caminho de tráfego inicial entre R3-Spoke1 e R4-Spoke2 parecem similares a este:

Desde que R1-Hub1 recebe o pacote na interface de acesso virtual, que tem o mesmo ID de rede do Next Hop Resolution Protocol (NHRP) que aquele no túnel GRE, a indicação do tráfego é enviada para o R3-Spoke1. Isto provoca a criação spoke-to-spoke do túnel dinâmico:

Tabelas de roteamento e saídas para a encenação operacional regular

Está aqui a tabela de roteamento R1-HUB1 em uma encenação operacional regular:

```
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
```

Está aqui a tabela de roteamento R3-SPOKE1 em uma encenação operacional regular depois que o túnel spoke-to-spoke com R4-SPOKE2 é criado:

```
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
```

Em R3-Spoke1, a tabela de BGP tem duas entradas para a rede **192.168.0.0/16** com preferências locais diferentes (R1-Hub1 é preferido):

```
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
```

Está aqui a tabela de roteamento R5-AGGR1 em uma encenação operacional regular:

```
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

```

Está aqui a tabela de roteamento R7-HOST em uma encenação operacional regular:

```

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

```

Cenário de falha de HUB1

Está aqui para baixo uma encenação R1-HUB1 (devido às ações tais como interrupções de energia ou uma elevação):

Nesta encenação, esta sequência de evento ocorre:

1. O BFD em R2-HUB2 e no Roteadores R5-AGGR1 e R6-AGGR2 do agregado LAN detecta o status baixo de R1-HUB1. Em consequência, a vizinhança de BGP vai imediatamente para baixo.
2. A detecção do objeto da trilha para R2-HUB2 que detecta a presença do laço de retorno R1-HUB1 vai para baixo (trilha 1 no exemplo de configuração).
3. Isto tragado seguiu o objeto provoca uma outra trilha para ir acima (lógico NÃO). Neste exemplo, a trilha 2 vai acima sempre que a trilha 1 vai para baixo.
4. Isto provoca uma entrada de roteamento do IP Estático a ser adicionada à tabela de roteamento devido a um valor que seja mais baixo do que a distância administrativa padrão.

Está aqui a configuração relevante:

```

! 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 redistribui estas rotas estáticas com uma preferência local BGP que seja maior do que o valor que é ajustado para R1-HUB1. Neste exemplo, uma preferência local de **500** é usada no cenário de falha, em vez dos **200** que é ajustado por 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

```

! Em R3-Spoke1, você pode ver este nas saídas BGP. Note que a entrada ao r1 ainda existe, mas não é usada:

```

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. Neste momento, ambo o spokes (R3-Spoke1 e R4-Spoke2) começa a enviar o tráfego a R2-HUB2. Todas estas etapas devem ocorrer dentro do segundo. Está aqui a tabela de roteamento no 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. Umass sessões de BGP mais atrasadas entre o spokes e o R1-HUB1 vão para baixo, e o Dead Peer Detection (DPD) remove os túneis de IPsec que são terminados em R1-HUB1. Contudo, isto não impacta o encaminhamento de tráfego, desde que R2-HUB2 é usado já como o gateway determinação principal:

```

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

```

Configurações

Esta seção fornecem configurações de amostra para o Hubs e o spokes que são usados nesta topologia.

Configuração 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-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

```

Configuração 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

```

Configuração 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

```

Configuração 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

```

Configuração 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
```

Configuração 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

```

Configuração R7-HOST (simulação do HOST nessa rede)

```

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

```

Notas de configuração importantes

Estão aqui algumas observações importantes sobre as configurações que são descritas nas seções anterior:

- O túnel GRE ponto a ponto entre os dois Hubs é exigido para que a Conectividade spoke-to-spoke trabalhe em todos os cenários, para incluir especificamente aquelas encenações em que algum do spokes é conectado somente a um do Hubs e a outro a um outro hub.
- **Nenhuma** configuração do **eco do bfd** na interface do túnel GRE entre os dois Hubs é exigida a fim evitar a indicação do tráfego que é mandada de um outro hub. O eco BFD tem o mesmo endereço IP de origem e de destino, que é igual ao endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador que envia o eco BFD. Desde que estes pacotes são distribuídos para trás pelo roteador que responde, as indicações do tráfego NHRP são geradas.

- Na configuração de BGP, a filtração do mapa de rotas que anuncia as redes para o spokes não é exigida, mas ele faz as configurações mais ótimas desde que somente agregado/rotas sumárias são anunciados:
`neighbor SPOKES route-map AGGR out`
- No Hubs, a configuração do **mapa de rotas LOCALPREF** é exigida a fim estabelecer a preferência local apropriada BGP, e filtra as rotas estáticas redistribuídas às rotas somente do sumário e do modo de configuração IKEv2.
- Este projeto não endereça a Redundância em lugar do escritório remoto (spoke). Se o link MACILENTO no spoke vai para baixo, o VPN igualmente não trabalha. Adicionar um segundo link ao roteador do spoke ou adicionar um segundo roteador do spoke dentro do mesmo lugar a fim endereçar esta edição.

Em resumo, o projeto da Redundância que é apresentado neste documento pode ser tratado como uma alternativa moderna à característica do Stateful Switchover (SSO) /Stateful. É altamente flexível e pode ser ajustado a fim cumprir suas exigências específicas do desenvolvimento.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Folha de dados de FlexVPN do Cisco IOS](#)
- [Configurar FlexVPN falou ao spoke](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)