

Comprendre et dépanner le contrôle de route dans les déploiements SD-WAN de pare-feu sécurisé

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations sur les fonctionnalités](#)

[Scénario de déploiement](#)

[Deux concentrateurs et satellites avec deux FAI](#)

[Topologie sous-jacente](#)

[Topologie de recouvrement](#)

[Configuration](#)

[Vérifiez et dépannez](#)

[Configuration commune à tous les périphériques](#)

[Spoke1 et 2 \(IBGP avec HUB1 et EBGP avec HUB2\)](#)

[HUB1 \(appairage IBGP avec les satellites\)](#)

[HUB2 \(appairage EBGP avec les satellites\)](#)

[Topologie de routage](#)

[Rayon1](#)

[CONCENTRATEUR 1](#)

[CONCENTRATEUR 2](#)

[Rayon 2](#)

[Conclusion](#)

[Informations connexes](#)

Introduction

Ce document décrit le contrôle de routage dans BGP pour les VPN basés sur des routes utilisant Cisco SD-WAN sur un pare-feu sécurisé.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEv2
- VPN reposant sur des routes
- Interfaces de tunnel virtuel (VTI)

- IPsec
- BGP
- Attributs BGP tels que les balises de communauté et les réflecteurs de route
- Fonctionnalité SD-WAN sur pare-feu sécurisé

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Cisco Secure Firewall Threat Defense 7.7.10
- Cisco Secure Firewall Management Center 7.7.10

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations sur les fonctionnalités

Avec le nouveau déploiement SD-WAN pour VPN site à site basé sur route avec BGP activé pour la superposition, Cisco se concentre sur les attributs BGP clés pour mettre en oeuvre un routage de superposition sécurisé et sans boucle, garantissant que les réseaux sous-jacents et superposés restent séparés dans toute la topologie. Ce déploiement garantit également qu'aucune intervention manuelle n'est nécessaire pour ajuster les attributs appropriés.

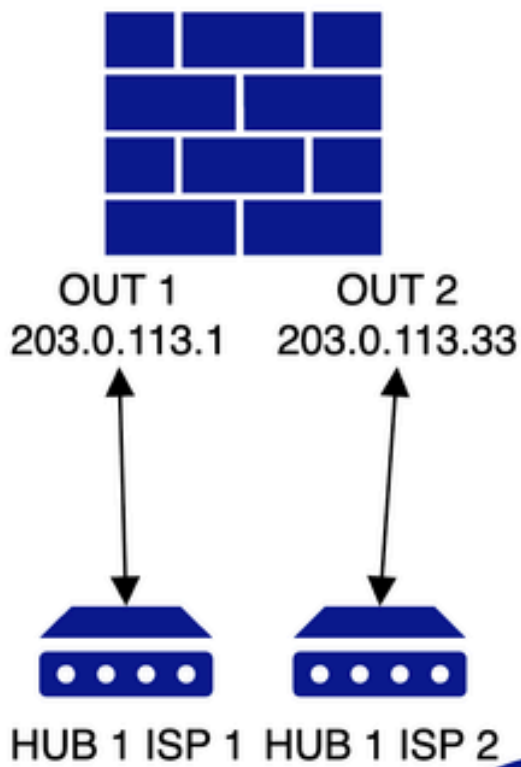
Scénario de déploiement

Sélectionnez une topologie qui inclut à la fois les connexions iBGP et eBGP entre le concentrateur et le rayon. Cette approche offre une visibilité maximale sur les contrôles de routage mis en oeuvre dans le cadre de la solution SD-WAN sur les pare-feu sécurisés Cisco.

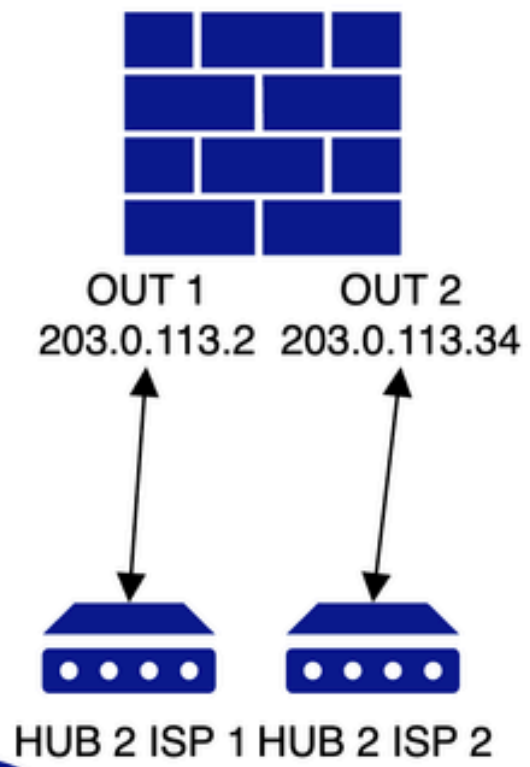
Deux concentrateurs et satellites avec deux FAI

Topologie sous-jacente

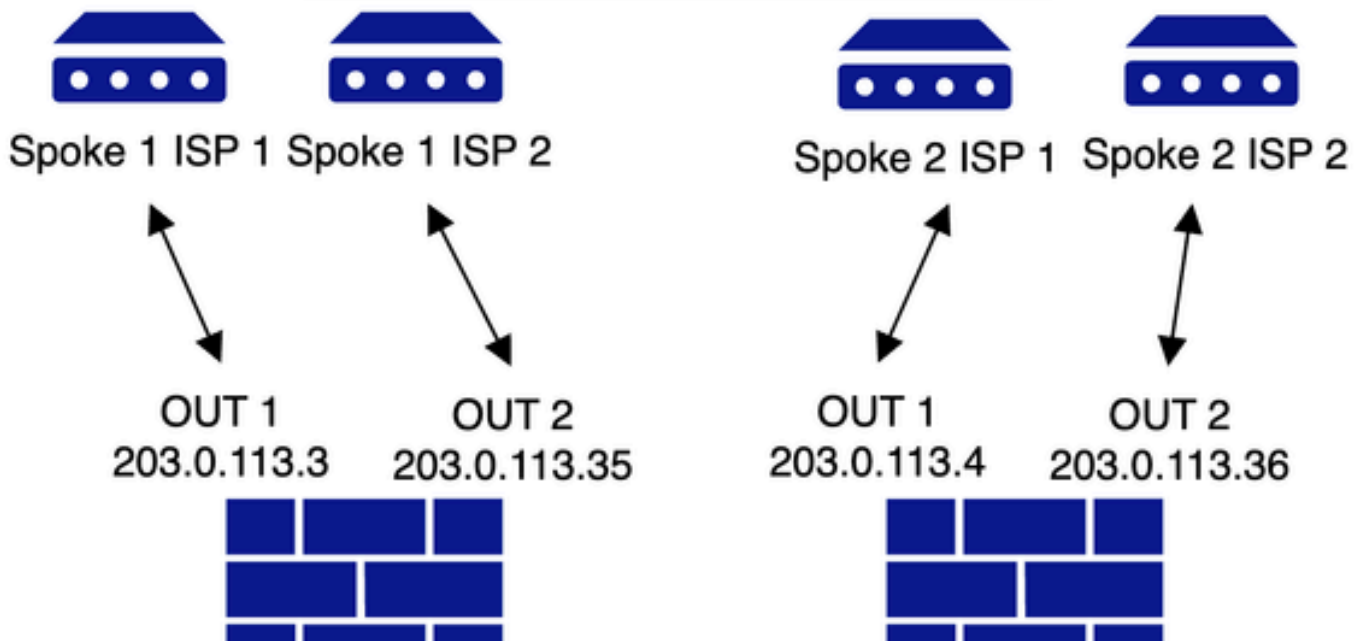
AS65500



AS65510



Internet



```
community-list standard FMC_VPN_COMMUNITY_101010 permit 101010
```

```
<<<<<<<<<<
```

```
community-list standard FMC_VPN_COMMUNITY_202020 permit 202020
```

```
<<<<<<<<<<
```

Notez qu'il existe une seule paire de route-maps entrante et sortante par topologie, bien que les configurations soient identiques pour les deux topologies, seule la convention d'attribution de noms est unique par topologie. Dans notre scénario, FMC_VPN_RMAP_COMMUNITY_IN_8589939614 et FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 sont pour la topologie 1 tandis que FMC_VPN_RMAP_COMMUNITY_IN_8589942200 et FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 concernent la topologie 2.

```
<#root>
```

```
firepower# show running-config route-map
```

```
Topology 1
```

```
Inbound
```

```
route-map
```

```
FMC_VPN_RMAP_COMMUNITY_IN_8589939614
```

```
    permit 10  
    match community FMC_VPN_COMMUNITY_101010 exact-match
```

```
    set community 202020
```

```
route-map
```

```
FMC_VPN_RMAP_COMMUNITY_IN_8589939614
```

```
    permit 20  
    match community FMC_VPN_COMMUNITY_202020 exact-match
```

```
Outbound
```

```
route-map
```

```
FMC_VPN_RMAP_COMMUNITY_OUT_8589939614
```

```
    permit 10  
    match community FMC_VPN_COMMUNITY_101010 exact-match  
    set metric 1
```

```
route-map
```

```
FMC_VPN_RMAP_COMMUNITY_OUT_8589939614
```

```
    permit 20  
    match community FMC_VPN_COMMUNITY_202020 exact-match  
    set metric 100
```

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

deny 100

Topology 2

Inbound

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589942200

permit 10

match community FMC_VPN_COMMUNITY_101010 exact-match

set community 202020

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589942200

permit 20

match community FMC_VPN_COMMUNITY_202020 exact-match

Outbound

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

permit 10

match community FMC_VPN_COMMUNITY_101010 exact-match

set metric 1

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

permit 20

match community FMC_VPN_COMMUNITY_202020 exact-match

set metric 100

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

deny 100

Common Across All The Hubs & Spokes Wherever Redistribution Of Inside Network Is Present

route-map

FMC_VPN_CONNECTED_DIST_RMAP_101010

permit 10

match interface inside

set community 101010

La configuration BGP sur les périphériques de la topologie est présentée :

Spoke1 et 2 (IBGP avec HUB1 et EBGP avec HUB2)

<#root>

firepower# show running-config router bgp

```
router bgp 65500
  bgp log-neighbor-changes
  address-family ipv4 unicast
  neighbor 198.51.100.1 remote-as 65500
```

<<<<< tunnel from spokes to HUB 1 via ISP1

```
neighbor 198.51.100.1 activate
neighbor 198.51.100.1 send-community
neighbor 198.51.100.1 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589939614 in
neighbor 198.51.100.1 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 out
neighbor 198.51.100.2 remote-as 65510
```

<<<<< tunnel from spokes to HUB 2 via ISP1

```
neighbor 198.51.100.2 ebgp-multihop 2
neighbor 198.51.100.2 activate
neighbor 198.51.100.2 send-community
neighbor 198.51.100.2 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589939614 in
neighbor 198.51.100.2 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 out
neighbor 198.51.100.3 remote-as 65500
```

<<<<< tunnel from spokes to HUB 1 via ISP2

```
neighbor 198.51.100.3 activate
neighbor 198.51.100.3 send-community
neighbor 198.51.100.3 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589942200 in
neighbor 198.51.100.3 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 out
neighbor 198.51.100.4 remote-as 65510
```

<<<<< tunnel from spokes to HUB 2 via ISP2

```
neighbor 198.51.100.4 ebgp-multihop 2
neighbor 198.51.100.4 activate
neighbor 198.51.100.4 send-community
neighbor 198.51.100.4 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589942200 in
neighbor 198.51.100.4 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 out
redistribute connected route-map FMC_VPN_CONNECTED_DIST_RMAP_101010
```

<<<<<< route-map to redistribute inside network into BGP

```
maximum-paths 8
maximum-paths ibgp 8
no auto-summary
no synchronization
exit-address-family
```

HUB1 (appairage IBGP avec les satellites)

<#root>

```
firepower# show running-config router bgp
```

```
router bgp 65500
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 198.51.100.10 remote-as 65500
```

```
<<<<< tunnel from HUB 1 to Spoke 1 via ISP 1
```

```
neighbor 198.51.100.10 activate
neighbor 198.51.100.10 send-community
neighbor 198.51.100.10 route-reflector-client
neighbor 198.51.100.10 next-hop-self
neighbor 198.51.100.10 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589939614 in
neighbor 198.51.100.10 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 out
neighbor 198.51.100.11 remote-as 65500
```

```
<<<<< tunnel from HUB 1 to Spoke 2 via ISP 1
```

```
neighbor 198.51.100.11 activate
neighbor 198.51.100.11 send-community
neighbor 198.51.100.11 route-reflector-client
neighbor 198.51.100.11 next-hop-self
neighbor 198.51.100.11 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589939614 in
neighbor 198.51.100.11 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 out
neighbor 198.51.100.70 remote-as 65500
```

```
<<<<< tunnel from HUB 1 to Spoke 1 via ISP 2
```

```
neighbor 198.51.100.70 activate
neighbor 198.51.100.70 send-community
neighbor 198.51.100.70 route-reflector-client
neighbor 198.51.100.70 next-hop-self
neighbor 198.51.100.70 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589942200 in
neighbor 198.51.100.70 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 out
neighbor 198.51.100.71 remote-as 65500
```

```
<<<<< tunnel from HUB 1 to Spoke 2 via ISP 2
```

```
neighbor 198.51.100.71 activate
neighbor 198.51.100.71 send-community
neighbor 198.51.100.71 route-reflector-client
neighbor 198.51.100.71 next-hop-self
neighbor 198.51.100.71 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589942200 in
neighbor 198.51.100.71 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 out
no auto-summary
no synchronization
exit-address-family
```

HUB2 (appairage EBGp avec les satellites)

```
<#root>
```

```
firepower# show running-config router bgp
```

```
router bgp 65510
  bgp log-neighbor-changes
  address-family ipv4 unicast
  neighbor 198.51.100.40 remote-as 65500
```

<<<< tunnel from HUB 2 to Spoke 1 via ISP 1

```
neighbor 198.51.100.40 ebgp-multihop 2
neighbor 198.51.100.40 activate
neighbor 198.51.100.40 send-community
neighbor 198.51.100.40 next-hop-self
neighbor 198.51.100.40 as-override
neighbor 198.51.100.40 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589939614 in
neighbor 198.51.100.40 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 out
neighbor 198.51.100.41 remote-as 65500
```

<<<< tunnel from HUB 2 to Spoke 2 via ISP 1

```
neighbor 198.51.100.41 ebgp-multihop 2
neighbor 198.51.100.41 activate
neighbor 198.51.100.41 send-community
neighbor 198.51.100.41 next-hop-self
neighbor 198.51.100.41 as-override
neighbor 198.51.100.41 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589939614 in
neighbor 198.51.100.41 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 out
neighbor 198.51.100.100 remote-as 65500
```

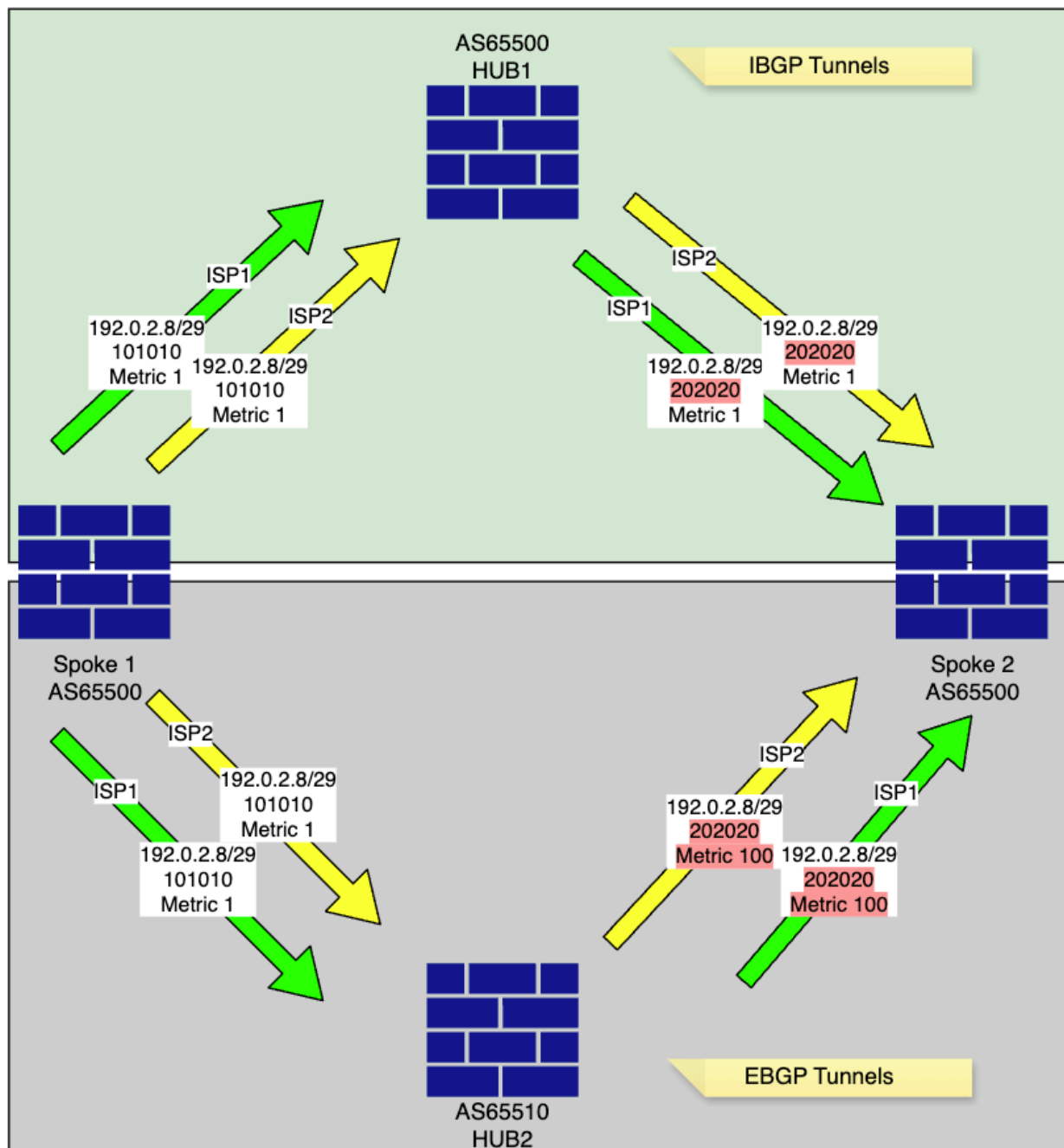
<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
neighbor 198.51.100.100 ebgp-multihop 2
neighbor 198.51.100.100 activate
neighbor 198.51.100.100 send-community
neighbor 198.51.100.100 next-hop-self
neighbor 198.51.100.100 as-override
neighbor 198.51.100.100 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589942200 in
neighbor 198.51.100.100 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 out
neighbor 198.51.100.101 remote-as 65500
```

<<<< tunnel from HUB 2 to Spoke 2 via ISP 2

```
neighbor 198.51.100.101 ebgp-multihop 2
neighbor 198.51.100.101 activate
neighbor 198.51.100.101 send-community
neighbor 198.51.100.101 next-hop-self
neighbor 198.51.100.101 as-override
neighbor 198.51.100.101 route-map FMC_VPN_RMAP_COMMUNITY_IN_8589942200 in
neighbor 198.51.100.101 route-map FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 out
no auto-summary
no synchronization
exit-address-family
```

Topologie de routage



- Le satellite annonce son réseau interne, [192.0.2.8/29](#), dans BGP avec une balise de communauté spécifique de 101010, comme configuré dans la route-map FMC_VPN_CONNECTED_DIST_RMAP_1010.

Rayon1

<#root>

Spoke1# show bgp community 101010 exact-match <<<< to verify the exact network redistributed into BGP

BGP table version is 4, local router ID is 203.0.113.35
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
 r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.0.2.8/29	0.0.0.0	0		32768	?

<<<<<<<<< local inside network

- Le rayon modifie la valeur métrique pour son réseau interne, [192.0.2.8/29](#), et l'annonce aux concentrateurs, comme configuré dans les route-maps FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 et FMC_VPN_RMAP_COMMUNITY_OUT_858994200.

<#root>

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

```
permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match
set metric 1
```

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

```
permit 20
match community FMC_VPN_COMMUNITY_202020 exact-match
set metric 100
```

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

```
deny 100
```

- HUB1 apprend le réseau Spoke 1 [192.0.2.8/29](#) avec la balise community 101010, et change la balise community en 202020 tout en conservant la métrique avant de la transmettre à d'autres satellites, comme défini dans les route-maps configurées.

CONCENTRATEUR 1

<#root>

Route-Map for ISP1 DVTI

Inbound

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589939614

```
permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match
set community 202020
```

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589939614

permit 20
match community FMC_VPN_COMMUNITY_202020 exact-match

Outbound

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match
set metric 1
set ip next-hop 198.51.100.1

<<<<<<<<< only next-hop is changed in ISP2 tunnel route-map with ISP2 DVTI IP

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

permit 20
match community FMC_VPN_COMMUNITY_202020 exact-match
set metric 100
set ip next-hop 198.51.100.1

<<<<<<<<< only next-hop is changed in ISP2 tunnel route-map with ISP2 DVTI IP

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

deny 100

Route-Map for ISP2 DVTI

Inbound

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589942200

permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match
set community 202020

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589942200

permit 20
match community FMC_VPN_COMMUNITY_202020 exact-match

Outbound

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match

```
set metric 1
set ip next-hop 198.51.100.3
```

<<<<<<<< only next-hop is changed in ISP2 tunnel route-map with ISP2 DVTI IP

```
route-map
FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

  permit 20
  match community FMC_VPN_COMMUNITY_202020 exact-match
  set metric 100
  set ip next-hop 198.51.100.3
```

<<<<<<<< only next-hop is changed in ISP2 tunnel route-map with ISP2 DVTI IP

```
route-map
FMC_VPN_RMAP_COMMUNITY_OUT_8589942200

  deny 100
```

<#root>

HUB1# show bgp community 202020 exact-match <<<< this will confirm if received prefixes have community t

BGP table version is 5, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
 r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* i192.0.2.8/29	198.51.100.70	1	100	0	?
*>i	198.51.100.10	1	100	0	?
* i192.0.2.16/29	198.51.100.71	1	100	0	?
*>i	198.51.100.11	1	100	0	?

<#root>

HUB1# show bgp 192.0.2.8 <<<< this will display available paths in BGP for the network

BGP routing table entry for 192.0.2.8/29, version 4
Paths: (2 available, best #2, table default)
 Advertised to update-groups:
 1 2
 Local, (Received from a RR-client)
 198.51.100.70 from 198.51.100.70 (203.0.113.35)

<<<<< spoke 1 ISP 2 tunnel to HUB 1

Origin incomplete, metric 1, localpref 100, valid, internal
Community: 202020

Local, (Received from a RR-client)
198.51.100.10 from 198.51.100.10 (203.0.113.35)

<<<< spoke 1 ISP 1 tunnel to HUB 1

Origin incomplete, metric 1, localpref 100, valid, internal, best
Community: 202020

<<<< community updated as per the route-map configured on spoke side

<#root>

HUB1# show route 192.0.2.8

Routing entry for 192.0.2.8 255.255.255.248
Known via "bgp 65500", distance 200, metric 1, type internal
Last update from 198.51.100.10 0:09:18 ago
Routing Descriptor Blocks:

* 198.51.100.10, from 198.51.100.10, 0:09:18 ago

Route metric is 1, traffic share count is 1
AS Hops 0
MPLS label: no label string provided

<#root>

HUB1# show bgp ipv4 unicast neighbors 198.51.100.10 routes <<<<< to check specific prefixes learnt via

BGP table version is 5, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.8/29	198.51.100.10	1	100	0	?

<<< preferred route

Total number of prefixes 1

<#root>

HUB1# show bgp ipv4 unicast neighbors 198.51.100.70 routes <<<<< to check specific prefixes learnt via

BGP table version is 5, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* i192.0.2.8/29	198.51.100.70	1	100	0	?

Total number of prefixes 1

- Le HUB2 apprend également le réseau Spoke 1 [192.0.2.8/29](#) avec la balise community 101010, et modifie la balise community en 202020 et met à jour la métrique sur 100 avant de la transférer vers d'autres satellites, comme spécifié dans les route-maps configurées. Cette modification de métrique prend effet en raison de l'appairage eBGP. En effet, MED (Multi-Exit Discriminator) est un attribut BGP facultatif non transitif utilisé pour influencer le trafic entrant en suggérant un point d'entrée préféré dans un AS. MED n'est généralement pas propagé entre les homologues iBGP au sein du même AS et est plutôt annoncé aux homologues BGP externes (eBGP) dans différents systèmes autonomes.

CONCENTRATEUR 2

<#root>

HUB2# show bgp community 202020 exact-match <<<< this will confirm if received prefixes have community

BGP table version is 5, local router ID is 198.51.100.4
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
 r RIB-failure, S Stale, m multipath
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.1				

100

0 65500 ?

<<<<< advertised back by spoke 2 ISP1 to HUB2 previously learnt via HUB1 iBGP

* 198.51.100.1

100

0 65500 ?

<<<<< advertised back by spoke 2 ISP2 to HUB2 previously learnt via HUB1 iBGP

* 198.51.100.100 1 0 65500 ?

<<<<< advertised by spoke 2 ISP tunnel

*> 198.51.100.40 1 0 65500 ?

<<<<< advertised and preferred by spoke 1 ISP 1 tunnel

* 192.0.2.16/29	198.51.100.1	100	0	65500 ?
* 198.51.100.1	198.51.100.1	100	0	65500 ?
* 198.51.100.101	198.51.100.101	1	0	65500 ?
*> 198.51.100.41	198.51.100.41	1	0	65500 ?

<#root>

HUB2# show bgp 192.0.2.8 <<<< this will display available paths in BGP for the network

BGP routing table entry for 192.0.2.8/29, version 4

Paths: (4 available, best #4, table default)

Advertised to update-groups:

1 2

65500

198.51.100.1 (inaccessible) from 198.51.100.41 (203.0.113.36)

<<<<< advertised back by spoke 2 ISP1 to HUB2 previously learnt via HUB1 iBGP

Origin incomplete, metric 100, localpref 100, valid, external

Community:

202020

65500

198.51.100.1 (inaccessible) from 198.51.100.101 (203.0.113.36)

<<<<< advertised back by spoke 2 ISP2 to HUB2 previously learnt via HUB1 iBGP

Origin incomplete, metric 100, localpref 100, valid, external

Community:

202020

65500

198.51.100.100 from 198.51.100.100 (203.0.113.35)

<<<<< advertised by spoke 1 ISP 2 tunnel

Origin incomplete, metric 1, localpref 100, valid, external

Community:

202020

65500

198.51.100.40 from 198.51.100.40 (203.0.113.35)

<<<<< advertised and preferred by spoke 1 ISP 1 tunnel

Origin incomplete, metric 1, localpref 100, valid, external, best

Community:

202020

<#root>

HUB2# show bgp ipv4 unicast neighbors 198.51.100.40 routes <<<<< to check specific prefixes learnt via

BGP table version is 5, local router ID is 198.51.100.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.0.2.8/29	198.51.100.40	1		0	65500 ?

<<<< preferred

* 192.0.2.16/29	198.51.100.1	100		0	65500 ?
-----------------	--------------	-----	--	---	---------

Total number of prefixes 2

<#root>

HUB2# show bgp ipv4 unicast neighbors 198.51.100.41 routes <<<<< to check specific prefixes learnt via

BGP table version is 5, local router ID is 198.51.100.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.1	100		0	65500 ?

<<<<<

*> 192.0.2.16/29	198.51.100.41	1		0	65500 ?
------------------	---------------	---	--	---	---------

Total number of prefixes 2

<#root>

HUB2# show bgp ipv4 unicast neighbors 198.51.100.100 routes <<<<< to check specific prefixes learnt via

BGP table version is 5, local router ID is 198.51.100.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.100	1		0	65500 ?

<<<<<

* 192.0.2.16/29	198.51.100.1	100		0	65500 ?
-----------------	--------------	-----	--	---	---------

Total number of prefixes 2

<#root>

HUB2# show bgp ipv4 unicast neighbors 198.51.100.101 routes <<<<< to check specific prefixes learnt via

BGP table version is 5, local router ID is 198.51.100.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.1	100		0	65500 ?

<<<<<

* 192.0.2.16/29	198.51.100.101	1		0	65500 ?
-----------------	----------------	---	--	---	---------

Total number of prefixes 2

- Spoke 2 reçoit le réseau Spoke 1 [192.0.2.8/29](#) à la fois des tunnels HUB1 ISP1 et HUB1 ISP2 avec une métrique de 1, tandis qu'il reçoit le même réseau des tunnels HUB2 ISP1 et HUB2 ISP2 avec un tronçon suivant mis à jour de HUB1.

Rayon 2

<#root>

Spoke2# show bgp community 202020 exact-match <<<< this will confirm if received prefixes have community

BGP table version is 8, local router ID is 203.0.113.36
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*mi192.0.2.8/29	198.51.100.3	1	100	0	?
*					

>

i	198.51.100.1	1	100	0	?
---	--------------	---	-----	---	---

<<<< HUB1 ISP1 route preferred

*	198.51.100.2	100		0	65510	65510	?
*	198.51.100.4	100		0	65510	65510	?
* 192.0.2.16/29	198.51.100.4	100		0	65510	65510	?
*	198.51.100.2	100		0	65510	65510	?

<#root>

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589939614

permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match

set community 202020

route-map

FMC_VPN_RMAP_COMMUNITY_IN_8589956263

permit 20
match community FMC_VPN_COMMUNITY_202020 exact-match

- Spoke 2 annonce également les réseaux appris de HUB1 vers HUB2, comme défini par la

route-map sortante configurée, avec la métrique mise à jour.

<#root>

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

permit 10
match community FMC_VPN_COMMUNITY_101010 exact-match
set metric 1

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

permit 20
match community FMC_VPN_COMMUNITY_202020 exact-match
set metric 100

<<<<<

route-map

FMC_VPN_RMAP_COMMUNITY_OUT_8589939614

deny 100

<#root>

Spoke2# show bgp ipv4 unicast neighbors 198.51.100.2 advertised-routes <<<<< to check specific prefixes

BGP table version is 8, local router ID is 203.0.113.36
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.8/29	198.51.100.1	1	100	0	?

<<<<<<<

*> 192.0.2.16/29	0.0.0.0	0		32768	?
------------------	---------	---	--	-------	---

Total number of prefixes 2

<#root>

Spoke2# show bgp ipv4 unicast neighbors 198.51.100.4 advertised-routes <<<<< to check specific prefixes

BGP table version is 8, local router ID is 203.0.113.36
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
---------	----------	--------	--------	--------	------

```
*>i192.0.2.8/29      198.51.100.1      1      100      0  ?
```

```
<<<<<<<
```

```
*> 192.0.2.16/29      0.0.0.0      0      32768  ?
```

```
Total number of prefixes 2
```

Conclusion

L'objectif de ce document est de fournir une présentation du déploiement du routage principal, avec un accent sur les contrôles de routage implémentés dans BGP pour assurer à la fois la contingence et la redondance.

En résumé, le satellite 2 ainsi que tous les autres satellites de la topologie utilisent la même approche lors de l'annonce de leurs réseaux dans le domaine BGP. Le contrôle de routage le plus important dans ce scénario est le filtrage de liste de communauté, qui garantit que seuls les réseaux de cette topologie sont annoncés à d'autres homologues, empêchant ainsi la propagation accidentelle du réseau.

En outre, l'attribut [MED Multi-exit Discriminator](#) est utilisé pour influencer la sélection de route pour les homologues eBGP, garantissant que les routes apprises via l'homologue iBGP configuré en tant que concentrateur principal sont préférées aux préfixes appris depuis le concentrateur secondaire via eBGP.

En effectuant des ajustements topologiques, tels que la configuration d'iBGP pour le concentrateur secondaire, vous pouvez éliminer le besoin de manipulation MED et de route-maps entrantes qui retournent les balises de communauté avant d'annoncer le même réseau à d'autres rayons.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le TAC. Un contrat d'assistance valide est requis : [Contacts d'assistance internationale Cisco](#).
- Vous pouvez également visiter la [communauté VPN Cisco](#) pour obtenir des informations supplémentaires et discuter des tendances.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.