

瞭解安全防火牆SD-WAN部署中的路由控制並對其進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[功能資訊](#)

[部署方案](#)

[雙ISP的雙中心輻射型](#)

[底層拓撲](#)

[重疊拓撲](#)

[組態](#)

[驗證和疑難排解](#)

[所有裝置的通用配置](#)

[Spoke1和2 \(使用HUB1的IBGP和使用HUB2的EBGP \)](#)

[HUB1 \(與輻條對等的IBGP \)](#)

[HUB2 \(與輻條對等的EBGP \)](#)

[路由拓撲](#)

[輻條1](#)

[集線器1](#)

[集線器2](#)

[分支2](#)

[結論](#)

[相關資訊](#)

簡介

本檔案介紹在安全防火牆上使用思科SD-WAN的路由型VPN在BGP中的路由控制。

必要條件

需求

思科建議您瞭解以下主題：

- IKEv2
- 路由型VPN
- 虛擬通道介面(VTI)
- IPsec
- BGP
- BGP屬性，如社群標籤和路由反射器

- 安全防火牆上的SD-WAN功能

採用元件

本檔案中的資訊是根據：

- 思科安全防火牆威脅防禦7.7.10
- 思科安全防火牆管理中心7.7.10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

功能資訊

由於為站點到站點、基於路由的VPN部署了新的SD-WAN，並且為重疊啟用了BGP，思科專注於關鍵BGP屬性以實施無環和安全重疊路由，從而確保底層網路和重疊網路在整個拓撲中保持隔離。此部署還確保無需手動干預即可調整相關屬性。

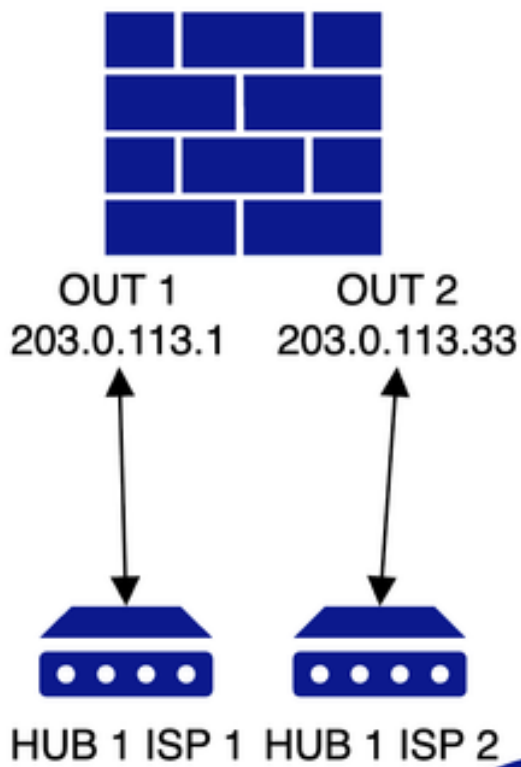
部署方案

選擇在中心點和分支點之間同時包含iBGP和eBGP連線的拓撲。此方法可最大程度地檢視作為SD-WAN解決方案一部分在思科安全防火牆上實施的路由控制。

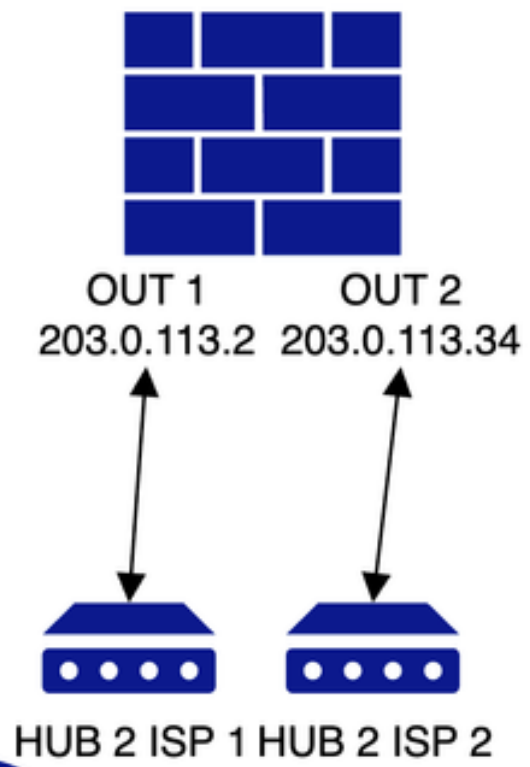
雙ISP的雙中心輻射型

底層拓撲

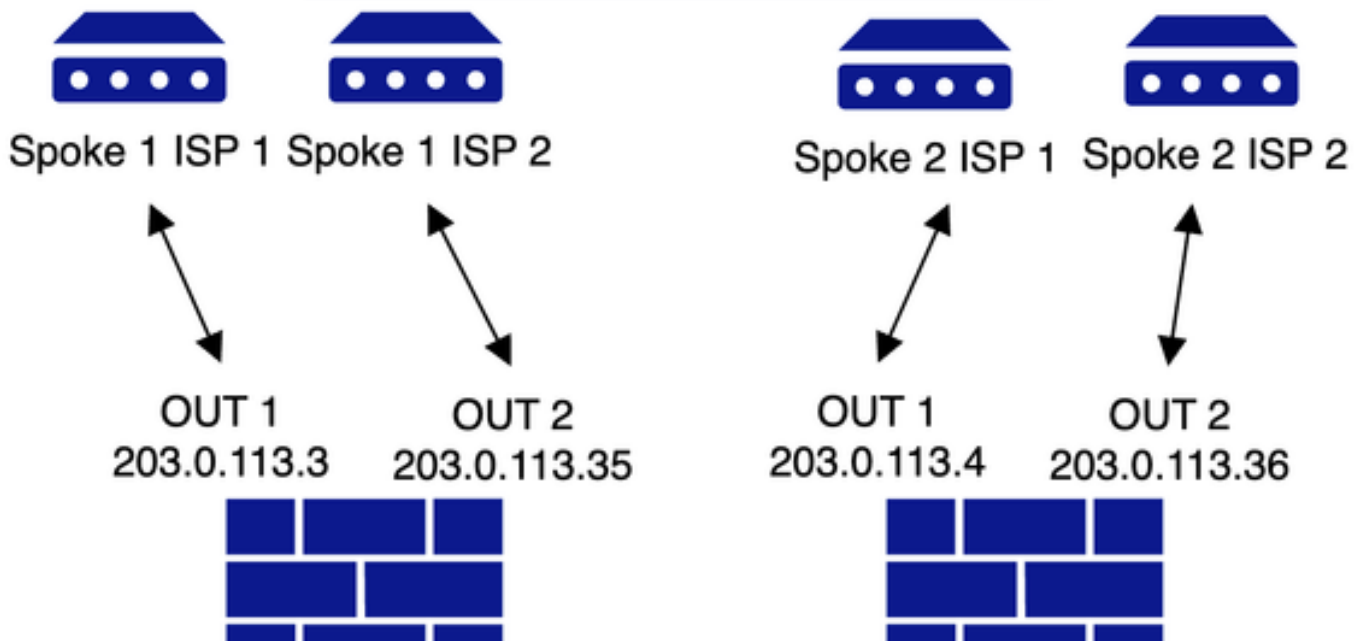
AS65500



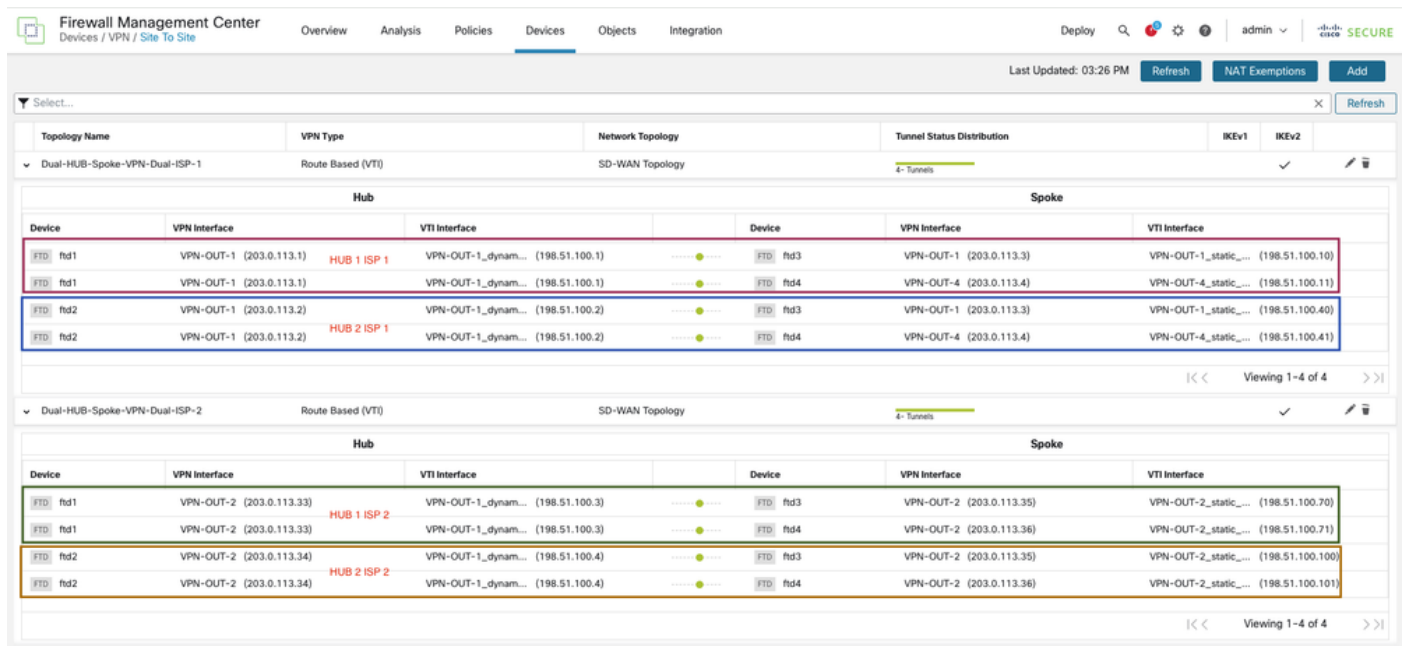
AS65510



Internet



CLI部分中的所有配置均通過SD-WAN配置嚮導應用。不會單獨對BGP配置或任何路由對映配置進行更改或修改。



驗證和疑難排解

社群清單負責篩選傳入和傳出字首。如需詳細說明，請參閱[Cisco Secure Firewall Management Center Device Configuration Guide](#)中Cisco文檔的Community List部分。

所有裝置的通用配置

<#root>

```
firepower# show running-config community-list
```

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

<<<<<<<

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

<<<<<<<<<<<

請注意，雖然兩個拓撲的配置相同，但每個拓撲只有一對入站和出站路由對映，只是命名約定在每個拓撲中是唯一的。在我們的方案中，FMC_VPN_RMAP_COMMUNITY_IN_858939614和FMC_VPN_RMAP_COMMUNITY_OUT_858939614用於拓撲1，而FMC_VPN_RMAP_COMMUNITY_IN_85899420和FMC_VPN_RMAP_COMMUNITY_OUT_85894200用於拓撲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
```

拓撲中裝置間的BGP配置如下所示：

Spoke1和2 (使用HUB1的IBGP和使用HUB2的EBGP)

<#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 (與輻條對等的IBGP)

<#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 (與輻條對等的EBGP)

<#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
```

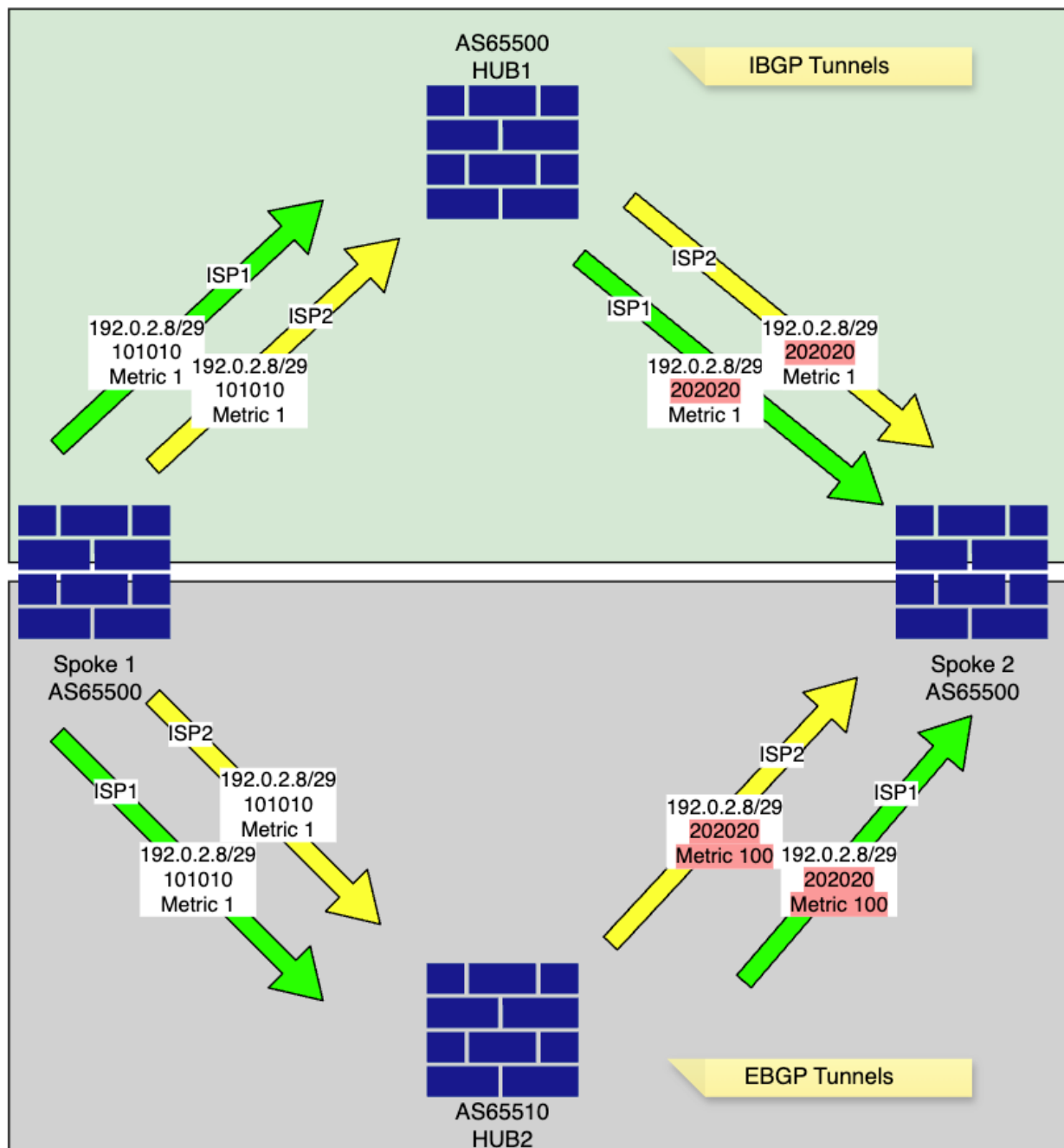
<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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
```

路由拓撲



- 分支將內部網路192.0.2.8/29通告到BGP中，其特定社群標籤為101010，如route-map FMC_VPN_CONNECTED_DIST_RMAP_1010中所配置。

輻條1

<#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

- 輻條會修改其內部網路[192.0.2.8/29](#)的度量值，並將其通告到集線器，如路由對映 FMC_VPN_RMAP_COMMUNITY_OUT_858939614 和 FMC_VPN_RMAP_COMMUNITY_OUT_85899420 中所配置。

<#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 使用社群標籤 101010 獲知分支 1 網路[192.0.2.8/29](#)，並將社群標籤更改為 202020，同時根據配置的路由對映中的定義，保留度量並將其轉發到其他分支。

集線器 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

- HUB2還使用社群標籤101010獲知分支1網路[192.0.2.8/29](#)，並將社群標籤更改為202020，並

將度量更新為100，然後將其轉發到其他分支，如配置的路由對映中所指定。此指標更改由於eBGP對等而生效。這是因為MED（多出口鑑別器）是可選的、非傳遞的BGP屬性，用於透過向AS建議首選入口點來影響傳入流量。MED通常不會在同一AS內的iBGP對等點之間傳播，而是會通告給不同自治系統中的外部BGP(eBGP)對等點。

集線器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	100	0	65500 ?
*	198.51.100.101	1	0	65500 ?
*>	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

- 分支2從HUB1 ISP1和HUB1 ISP2隧道接收分支1網路[192.0.2.8/29](#)，度量為1，而從HUB2

ISP1和HUB2 ISP2隧道接收同一網路，且其下一跳更新為HUB1。

分支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

- 分支2還使用更新的度量將從HUB1獲知的網路（由配置的出站路由對映定義）通告回HUB2。

<#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
```

結論

本文旨在提供後端路由部署的演練，重點介紹BGP內實施的路由控制，以確保應急和冗餘。

總而言之，分支2以及拓撲中的任何其他分支在將其網路通告到BGP域時都使用相同的方法。在此案例中，最重要的路由控制是社群清單過濾，它確保只有此拓撲中的網路才會通告給其他對等體，防止意外的網路傳播。

此外，[MED Multi-exit Discriminator](#)屬性用於影響eBGP對等點的路由選擇，確保通過配置為主HUB的iBGP對等點獲取的路由優先於通過eBGP從輔助HUB獲取的字首。

通過進行拓撲調整（例如為輔助HUB配置iBGP），可以消除在將同一網路通告到其他分支之前，需要進行MED操縱和反向社群標籤的入站路由對映。

相關資訊

- 如需其他協助，請聯絡TAC。需要有效的支援合約：思科[全球支援聯絡人](#)。
- 您還可以訪問[Cisco VPN社群](#)以瞭解其他見解和趨勢討論。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。