

セキュアファイアウォールSD-WANの導入におけるルート制御の理解およびトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[機能情報](#)

[導入シナリオ](#)

[デュアルISPを使用したデュアルハブアンドスポーク](#)

[アンダーレイトポロジ](#)

[オーバーレイトポロジ](#)

[コンフィギュレーション](#)

[確認とトラブルシューティング](#)

[すべてのデバイスで共通の設定](#)

[Spoke1および2 \(HUB1を使用するIBGPおよびHUB2を使用するEBGP \)](#)

[HUB1 \(スポークとのIBGPピアリング \)](#)

[HUB2 \(スポークとのEBGPピアリング \)](#)

[ルーティングトポロジ](#)

[スポーク1](#)

[ハブ1](#)

[ハブ2](#)

[スポーク2](#)

[結論](#)

[関連情報](#)

はじめに

このドキュメントでは、セキュアファイアウォール上でCisco SD-WANを使用したルートベースのVPNに対するBGPでのルーティング制御について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IKEv2
- ルートベースのVPN
- 仮想トンネルインターフェイス(VTI)

- IPSec
- BGP
- コミュニティタグやルートルリフレクタなどのBGPアトリビュート
- セキュアファイアウォール上のSD-WAN機能

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Secure Firewall脅威対策7.7.10
- Cisco Secure Firewall Management Center 7.7.10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能情報

BGPをオーバーレイに対して有効にしたサイト間、ルートベースのVPNに対する新しいSD-WANの導入により、シスコはループのない安全なオーバーレイルーティングを実装する主要なBGP属性に重点を置き、アンダーレイネットワークとオーバーレイネットワークがトポロジ全体で分離された状態を維持できるようにします。また、この導入により、関連する属性を調整するために手動による介入が必要なくなります。

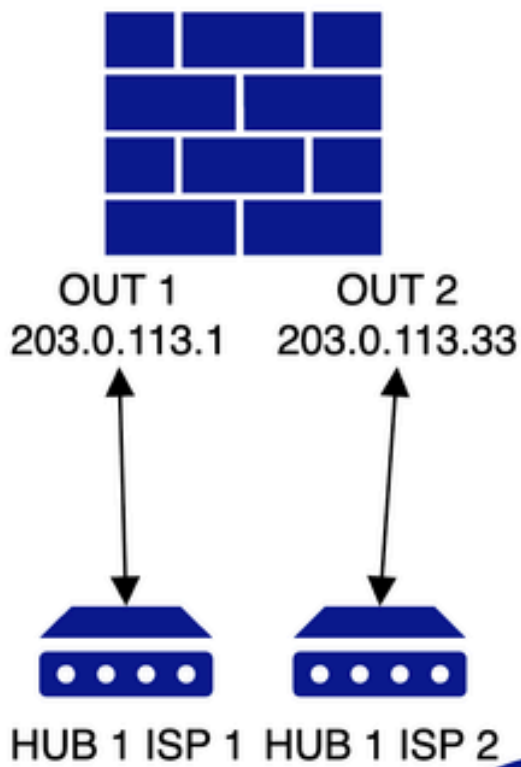
導入シナリオ

ハブとスポークの間のiBGP接続とeBGP接続の両方を含むトポロジを選択します。このアプローチにより、Cisco Secure Firewalls上のSD-WANソリューションの一部として実装されているルーティング制御を最大限に可視化できます。

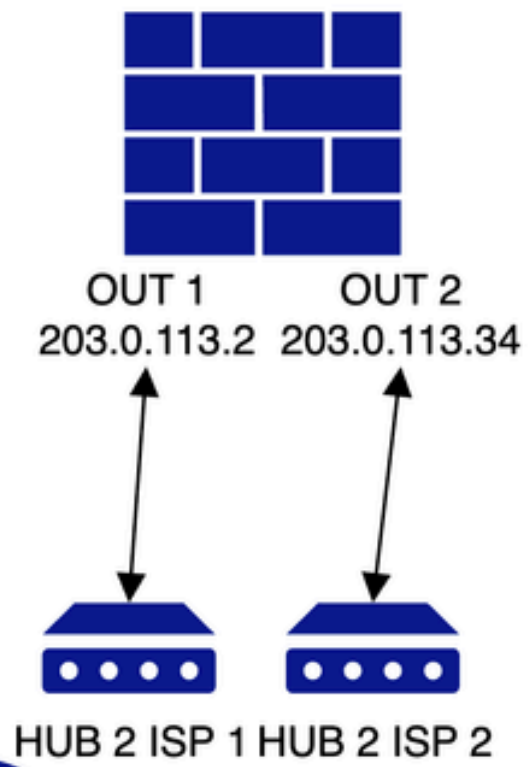
デュアルISPを使用したデュアルハブアンドスポーク

アンダーレイトポロジ

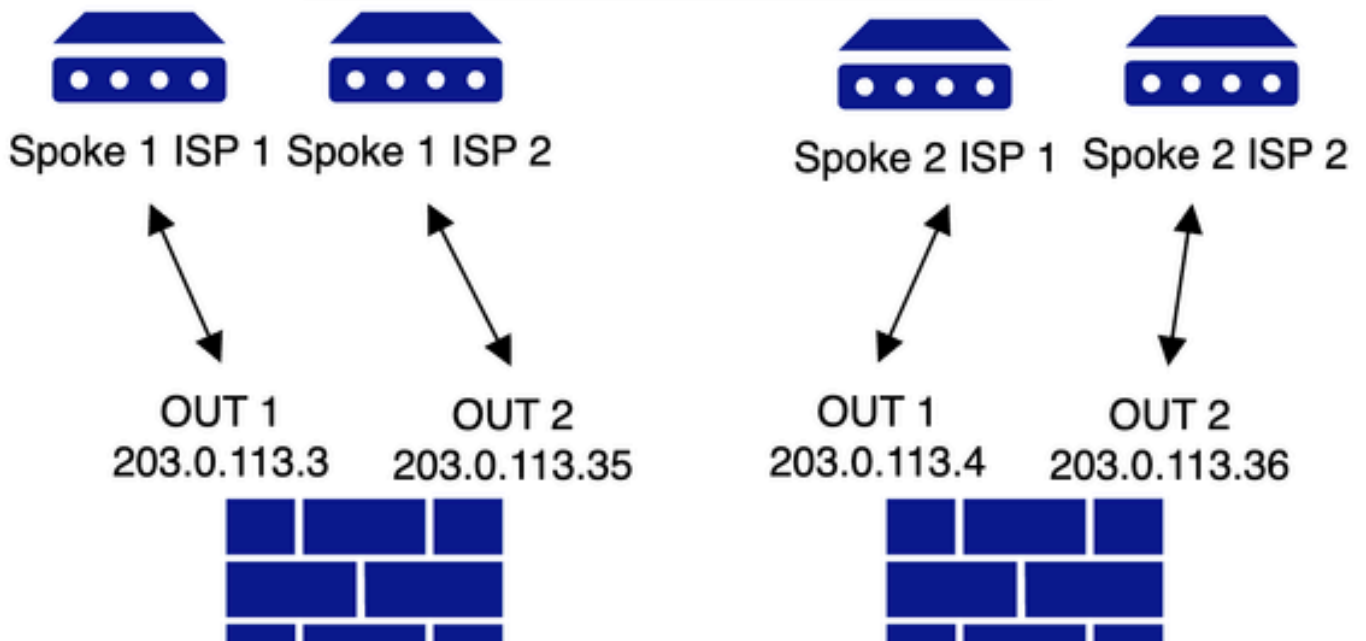
AS65500



AS65510



Internet



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

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

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

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

トポロジごとに着信ルートマップと発信ルートマップのペアが1つずつあることに注意してください。ただし、設定は両方のトポロジで同一であり、命名規則だけがトポロジごとに一意です。このシナリオでは、FMC_VPN_RMAP_COMMUNITY_IN_8589939614とFMC_VPN_RMAP_COMMUNITY_OUT_858939614はトポロジ1用で、FMC_VPN_RMAP_COMMUNITY_IN_85894200とFMC_VPN_RMAP_COMMUNITY_OUT_858942200はトポロジ2用です。

```
<#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

トポロジ内のデバイス間のBGP設定を次に示します。

スポーク1および2 (HUB1を使用するIBGPおよびHUB2を使用する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 (スポークとのIBGPピアリング)

```
<#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 (スポークとのEBGPピアリング)

<#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
```

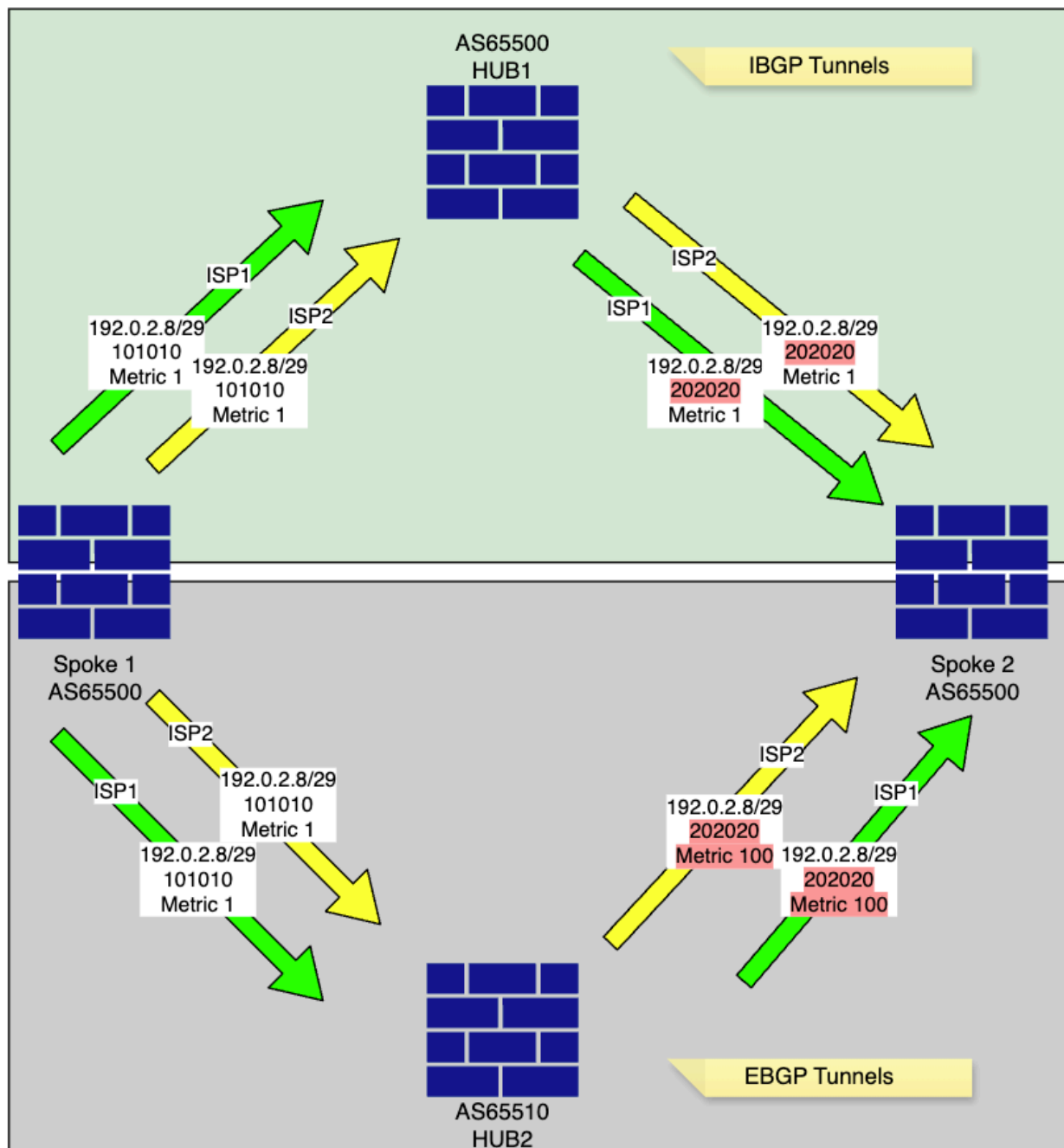
<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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
```

ルーティングトポロジ



- スポークは、ルートマップ [FMC VPN CONNECTED DIST RMAP 101010](#) で設定されているように、特定のコミュニティタグ101010を使用してBGPに内部ネットワーク [192.0.2.8/29](#) をアドバタイズします。

スポーク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

- スポークは、内部ネットワーク[192.0.2.8/29](https://www.ietf.org/rfc/rfc192.0.2.8/29)のメトリック値を変更し、ルートマップ FMC_VPN_RMAP_COMMUNITY_OUT_858939614および FMC_VPN_RMAP_COMMUNITY_OUT_85894200で設定されているように、ハブにアドバタイズします。

<#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は、コミュニティタグ101010を使用してスポーク1ネットワーク[192.0.2.8/29](https://www.ietf.org/rfc/rfc192.0.2.8/29)を学習し、設定されたルートマップの定義に従って、メトリックを他のスポークに転送する前にメトリックを保持したまま、コミュニティタグを202020に変更します。

ハブ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

- また、HUB2は、コミュニティタグ101010を使用してスポーク1ネットワーク [192.0.2.8/29](#)を学習し、設定されたルートマップに指定されているとおり、他のスポークに転送する前に、コミュニティタグを202020に変更し、メトリックを100に更新します。このメトリックの変更は、eBGPピアリングにより有効になります。これは、MED(Multi-Exit Discriminator)はオプションの非経過的なBGP属性であり、ASへの優先エン트리ポイントを提案することで着信トラフィックに影響を与えるために使用されるためです。通常、MEDは同じAS内のiBGPピア間では伝搬されず、異なる自律システム内の外部BGP(eBGP)ピアにアドバタイズされます。

ハブ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

- スポーク2は、メトリック1でHUB1 ISP1とHUB1 ISP2の両方のトンネルからスポーク1のネットワーク[192.0.2.8/29](#)を受信し、更新されたネクストホップHUB1を持つHUB2 ISP1とHUB2 ISP2のトンネルから同じネットワークを受信します。

スポーク 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

- また、スポーク2は、設定された発信ルートマップで定義されているように、更新されたメ

トリックでHUB1から学習したネットワークをHUB2にアドバタイズします。

<#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

このドキュメントの目的は、不測の事態と冗長性の両方を確保するためにBGP内で実装されたルーティング制御に重点を置いて、バックエンドルーティング導入の段階的検証を行うことです。

要約すると、スポーク2およびトポロジ内の他のスポークは、BGPドメインにネットワークをアドバタイズするときに同じアプローチを使用します。このシナリオで最も重要なルーティング制御は、コミュニティリストフィルタリングです。これにより、このトポロジ内のネットワークのみが他のピアにアドバタイズされ、意図しないネットワークの伝搬が防止されます。

また、[MED Multi-exit Discriminator](#) (MED)アトリビュートは、eBGPピアのルート選択に影響を与えるために使用され、プライマリHUBとして設定されたiBGPピアを通じて学習されたルートが、eBGPを通じてセカンダリHUBから学習されたプレフィックスよりも優先されるようになります。

セカンダリHUBのiBGPの設定などのトポロジ調整を行うことで、同じネットワークを他のスポークにアドバタイズする前にコミュニティタグを反転させるMED操作と着信ルートマップの必要性を排除できます。

関連情報

- 詳細については、TACにお問い合わせください。有効なサポート契約が必要です。シス[コ](#)[ワ](#)[ー](#)[ル](#)[ド](#)[ワ](#)[イ](#)[ド](#)[サ](#)[ポ](#)[ー](#)[ト](#)[の](#)[連](#)[絡](#)[先](#)[を](#)[参](#)[照](#)[し](#)[て](#)[く](#)[だ](#)[さ](#)[い](#)[。](#)
- また、[Cisco VPN Community](#)にもアクセスして、さまざまな考察やトレンドについて議論することができます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。