보안 방화벽 SD-WAN 구축의 경로 제어 이해 및 트러블슈팅

목차

- 소개
- 사전 요구 사항
  - 요구 사항
  - 사용되는 구성 요소
  - 기능 정보
- 구축 시나리오
  - 듀얼 ISP를 통한 듀얼 허브 및 스포크
    - 언더레이 토폴로지
    - 오버레이 토폴로지
    - 설정
    - 확인 및 문제 해결
    - 모든 디바이스의 공통 컨피그레이션
    - Spoke1 및 2(HUB1의 IBGP 및 HUB2의 EBGP)
    - HUB1(스포크를 사용한 IBGP 피어링)
    - HUB2(스포크를 사용한 EBGP 피어링)
    - 라우팅 토폴로지
    - 스포크1
    - 허브1
    - 허브2
    - 스포크 2
- 결론
- 관련 정보

소개

이 문서에서는 보안 방화벽에서 Cisco SD-WAN을 사용하는 경로 기반 VPN에 대한 BGP의 라우팅 제어에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IKEv2
- 경로 기반 VPN
- VTI(Virtual Tunnel Interface)
- IPSec
- BGP

- 커뮤니티 태그 및 경로 리플렉터와 같은 BGP 특성
- 보안 방화벽의 SD-WAN 기능

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 정보

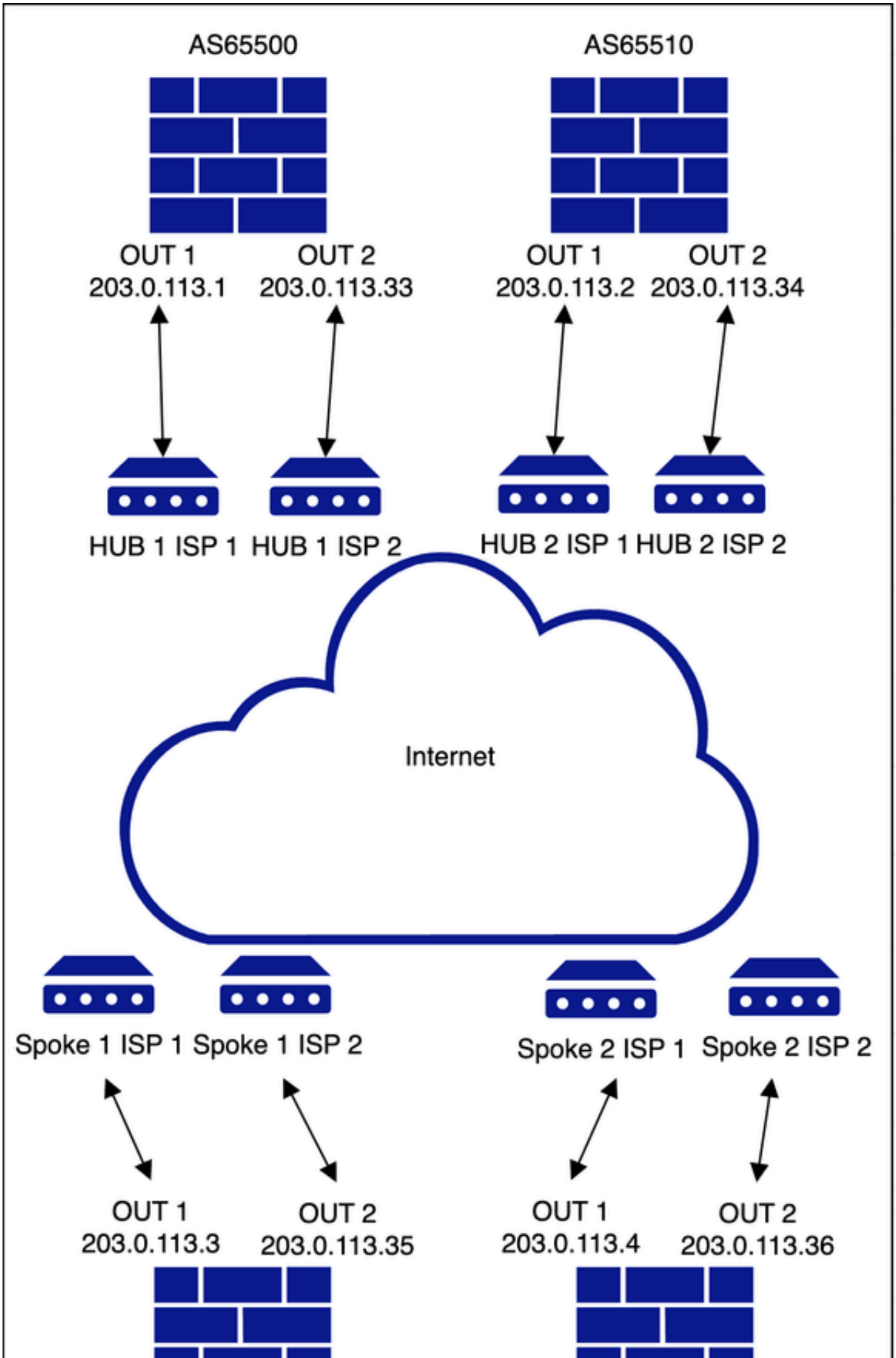
오버레이에 대해 BGP가 활성화된 사이트 대 사이트 경로 기반 VPN을 위한 새로운 SD-WAN 구축을 통해 Cisco는 주요 BGP 특성에 초점을 맞추어 루프 프리(loop-free) 및 보안 오버레이 라우팅을 구현함으로써 언더레이와 오버레이 네트워크가 토폴로지 전체에서 분리된 상태를 유지하도록 합니다. 또한 이러한 구축을 통해 관련 특성을 조정하는 데 수동 개입이 필요하지 않습니다.

구축 시나리오

HUB와 스포크 간의 iBGP 및 eBGP 연결을 모두 포함하는 토폴로지를 선택합니다. 이 접근 방식은 Cisco Secure Firewalls에서 SD-WAN 솔루션의 일부로 구현된 라우팅 제어에 대한 최대 가시성을 제공합니다.

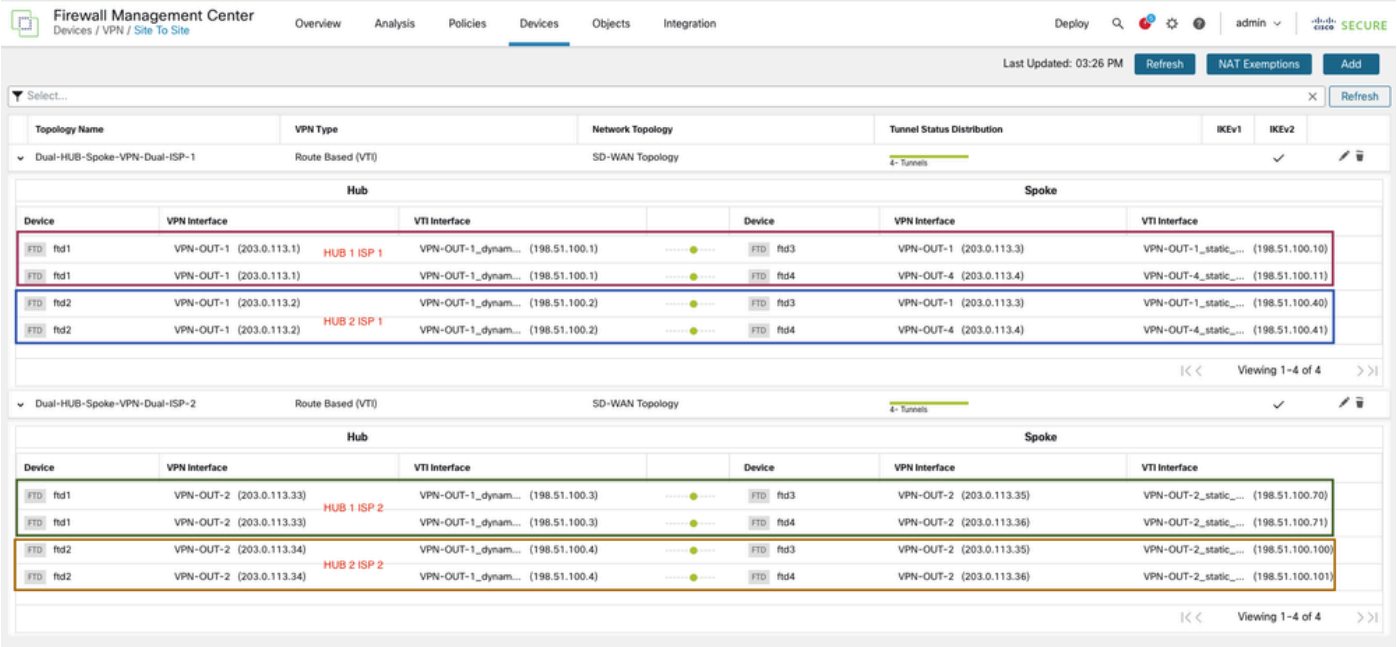
듀얼 ISP를 통한 듀얼 허브 및 스포크

언더레이 토폴로지


AS65500
AS65510
OUT 1
203.0.113.1
OUT 2
203.0.113.33
OUT 1
203.0.113.2
OUT 2
203.0.113.34
HUB 1 ISP 1
HUB 1 ISP 2
HUB 2 ISP 1
HUB 2 ISP 2
Internet
Spoke 1 ISP 1
Spoke 1 ISP 2
Spoke 2 ISP 1
Spoke 2 ISP 2
OUT 1
203.0.113.3
OUT 2
203.0.113.35
OUT 1
203.0.113.4
OUT 2
203.0.113.36

구축의 일부로 구현된 라우팅 제어에 대한 명확한 이해를 제공하는 것이므로 토폴로지 구축에 필요한 기본 컨피그레이션 단계는 다시 검토되지 않습니다. 초기 설정에 대한 자세한 지침은 이전에 게시된 문서 Configure [SD-WAN for Site-to-Site VPN over Secure Firewall을 참조하십시오](#).

CLI 섹션의 모든 컨피그레이션은 SD-WAN 컨피그레이션 마법사를 통해 적용됩니다. BGP 컨피그레이션 또는 경로 맵 컨피그레이션을 개별적으로 변경하거나 수정하지 않습니다.



확인 및 문제 해결

커뮤니티 목록은 수신 및 발신 접두사를 모두 필터링합니다. 자세한 설명은 Cisco [Secure Firewall Management Center Device Configuration Guide](#)의 Community List [섹션](#)에서 [확인할](#) 수 [있습니다](#).

모든 디바이스의 공통 컨피그레이션

<#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
<<<<<<<<<<
```

두 토폴로지의 컨피그레이션은 동일하지만 토폴로지당 하나의 인바운드 및 아웃바운드 경로 맵 쌍이 있습니다. 명명 규칙만 토폴로지당 고유합니다. 이 시나리오에서 FMC_VPN_RMAP_COMMUNITY_IN_8589939614 및 FMC_VPN_RMAP_COMMUNITY_OUT_8589939614는 토폴로지 1을 위한 것이며,

FMC_VPN_RMAP_COMMUNITY_IN_858942200 및
FMC_VPN_RMAP_COMMUNITY_OUT_85894200는 토폴로지 2를 위한 것입니다.

<#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
```

토폴로지의 디바이스 전반에서 BGP 컨피그레이션이 표시됩니다.

Spoke1 및 2(HUB1의 IBGP 및 HUB2의 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(스포크를 사용한 IBGP 피어링)

<#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(스포크를 사용한 EBGP 피어링)

<#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
```

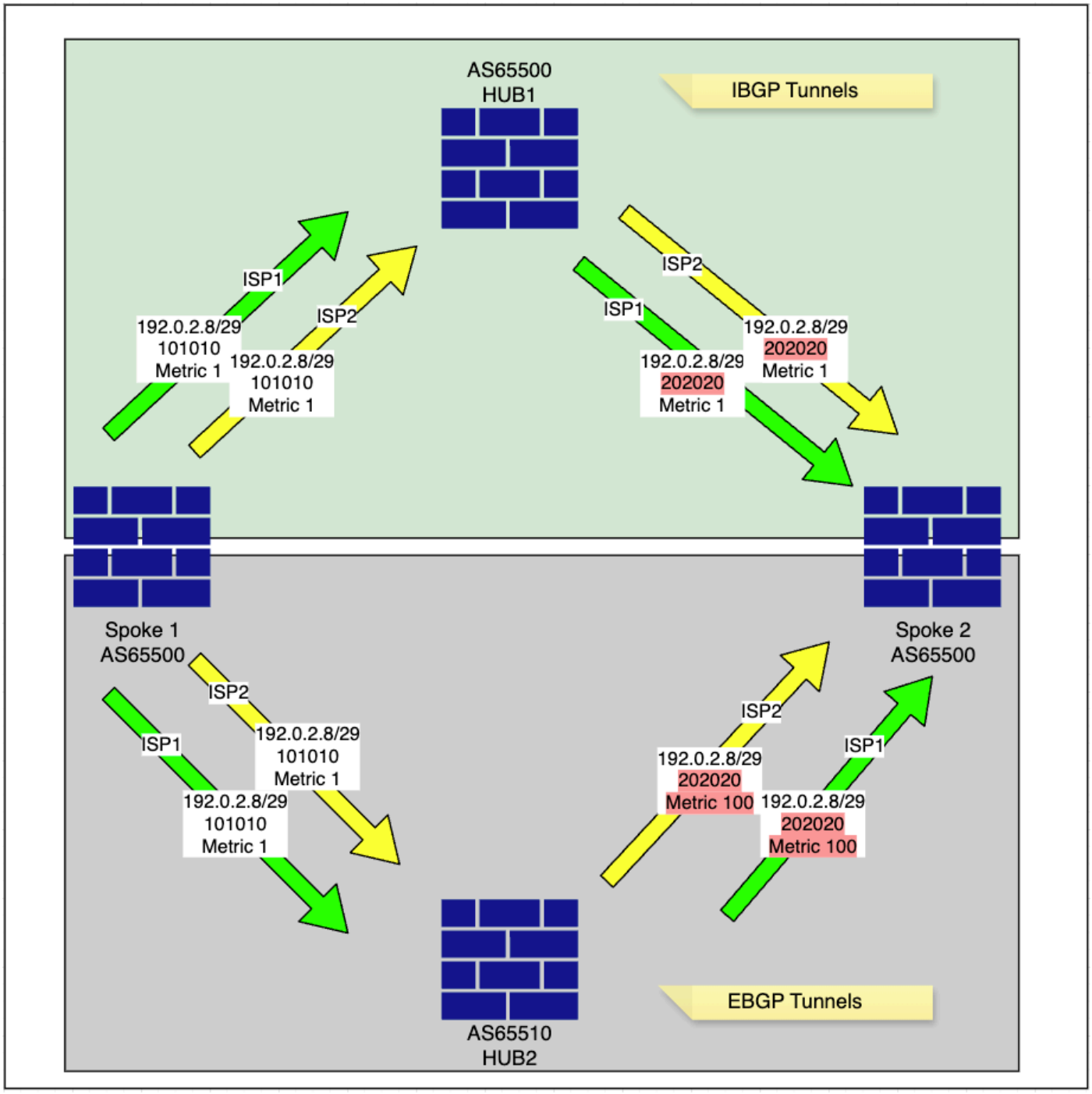
<<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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
```

라우팅 토폴로지



- 스포크는 내부 네트워크 192.0.2.8/29를 경로 맵 FMC_VPN_CONNECTED_DIST_RMAP_1010에 구성된 대로 특정 커뮤니티 태그가 101010인 BGP에 광고합니다.

스포크1

<#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

- 스포크는 내부 네트워크 192.0.2.8/29에 대한 메트릭 값을 수정하고, 경로 맵 FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 및 FMC_VPN_RMAP_COMMUNITY_OUT_858942200에 구성된 대로 허브에 알립니다.

<#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
```

- HUB1은 커뮤니티 태그 101010을 사용하여 스포크 1 네트워크 192.0.2.8/29를 학습하고, 구성된 경로 맵에 정의된 대로 메트릭을 다른 스포크에 전달하기 전에 보존하면서 커뮤니티 태그를 202020으로 변경합니다.

허브1

<#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
```

- 또한 HUB2는 커뮤니티 태그 101010을 사용하여 스포크 1 네트워크 192.0.2.8/29를 학습하며, 구성된 경로 맵에 지정된 대로 커뮤니티 태그를 202020으로 변경하고 메트릭을 100으로 업데이트한 다음 다른 스포크에 전달합니다. 이 메트릭 변경은 eBGP 피어링으로 인해 적용됩니다. 이는 MED(Multi-Exit Discriminator)가 AS에 기본 설정 진입점을 제안하여 인바운드 트래픽에 영향을 주는 데 사용되는 선택적 비전이적 BGP 특성이기 때문입니다. MED는 일반적으로 동일한 AS 내의 iBGP 피어 간에 전파되지 않고 다른 자율 시스템의 eBGP(external BGP) 피어로 광고됩니다.

허브2

<#root>

```
HUB2# show bgp community 202020 exact-match <<<< this will confirm if receieved 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
```

- 스포크 2는 메트릭이 1인 HUB1 ISP1 및 HUB1 ISP2 터널에서 스포크 1 네트워크 192.0.2.8/29를 수신하고, HUB1의 업데이트된 next-hop이 있는 HUB2 ISP1 및 HUB2 ISP2 터널에서 동일한 네트워크를 수신합니다.

스포크 2

<#root>

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


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
```

- 스포크 2는 또한 구성된 아웃바운드 route-map에 정의된 대로 업데이트된 메트릭과 함께 HUB1에서 학습한 네트워크를 HUB2로 다시 광고합니다.

<#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
```

결론

이 문서의 목적은 비상 및 이중화를 보장하기 위해 BGP 내에 구현된 라우팅 제어에 초점을 맞추어 백엔드 라우팅 구축을 살펴보는 것입니다.

요약하면, 스포크 2는 물론 토폴로지의 다른 스포크에서도 BGP 도메인으로 네트워크를 광고할 때 동일한 접근 방식을 사용합니다. 이 시나리오에서 가장 중요한 라우팅 제어는 커뮤니티 목록 필터링이며, 이렇게 하면 이 토폴로지 내의 네트워크만 다른 피어에 광고되어 의도하지 않은 네트워크 전파를 방지할 수 있습니다.

또한 MED Multi-exit Discriminator 특성은 eBGP 피어에 대한 경로 선택에 영향을 주므로 기본 허브로 구성된 iBGP 피어를 통해 학습된 경로가 eBGP를 통해 보조 허브에서 학습된 접두사보다 우선합니다.

보조 HUB에 대해 iBGP를 구성하는 것과 같은 토폴로지 조정을 수행하면 동일한 네트워크를 다른 스포크에 광고하기 전에 커뮤니티 태그를 전환하는 MED 조작 및 인바운드 경로 맵의 필요성을 제거할 수 있습니다.

관련 정보

- 추가 지원이 필요한 경우 TAC에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco Worldwide Support 연락처.
- 또한 Cisco VPN 커뮤니티를 방문하여 추가적인 통찰력 및 트렌드 논의를 할 수 있습니다.

이 번역에 관하여
Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.