Understand and Troubleshoot Route Control in Secure Firewall SD-WAN Deployments

Contents

Introduction

This document describes routing control in BGP for route-based VPNs using Cisco SD-WAN on secure firewall.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IKEv2
- Route-based VPN
- Virtual Tunnel Interfaces (VTI)
- IPsec
- BGP
- BGP attributes like community tags and route reflectors
- SD-WAN feature on secure firewall

Components Used

The information in this document is based on:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Feature Information

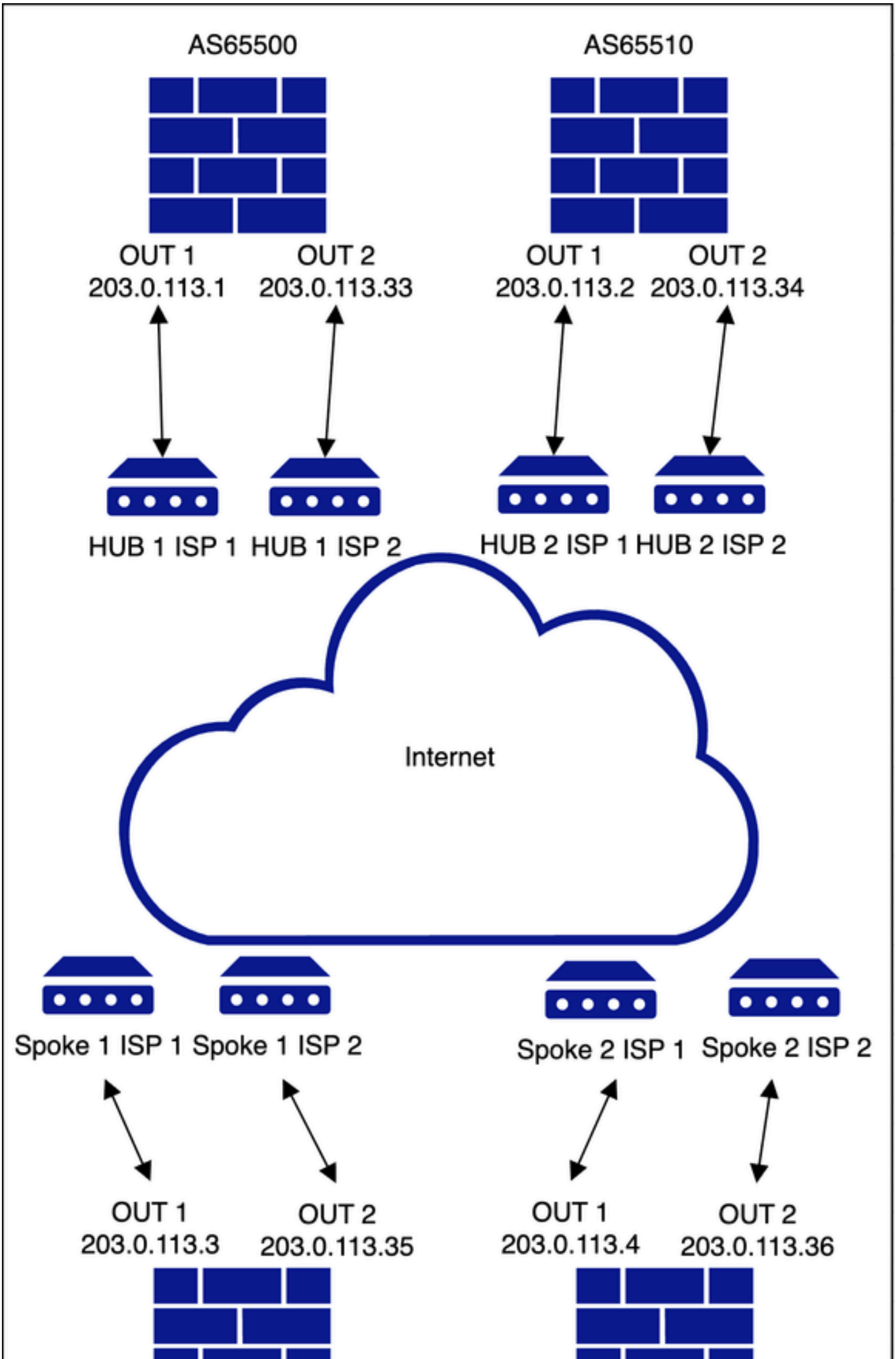
With the new SD-WAN deployment for site-to-site, route-based VPN with BGP enabled for the overlay, Cisco focuses on key BGP attributes to implement loop-free and secure overlay routing, ensuring that underlay and overlay networks remain segregated throughout the topology. This deployment also ensures that no manual intervention is required to adjust the relevant attributes.

Deployment Scenario

Select a topology that includes both iBGP and eBGP connections between the HUB and spoke. This approach provides maximum visibility into the routing controls implemented as part of the SD-WAN solution on Cisco Secure Firewalls.

Dual HUB and Spoke with Dual ISP

Underlay Topology


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

```
community-list standard FMC_VPN_COMMUNITY_101010 permit 101010

<<<<<<<<<<


community-list standard FMC_VPN_COMMUNITY_202020 permit 202020

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

Please note that there is a single pair of inbound and outbound route-maps per topology though the configurations are identical for both topologies, just the naming convention is unique per topology. In our scenario, **FMC_VPN_RMAP_COMMUNITY_IN_8589939614** and **FMC_VPN_RMAP_COMMUNITY_OUT_8589939614** are for topology 1 while **FMC_VPN_RMAP_COMMUNITY_IN_8589942200** and **FMC_VPN_RMAP_COMMUNITY_OUT_8589942200** are for topology 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
```

The BGP configuration across the devices in the topology is shown:

Spoke1 and 2 (IBGP with HUB1 and EBGP with 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 (IBGP Peering with the Spokes)

<#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 (EBGP Peering with the Spokes)

<#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
```

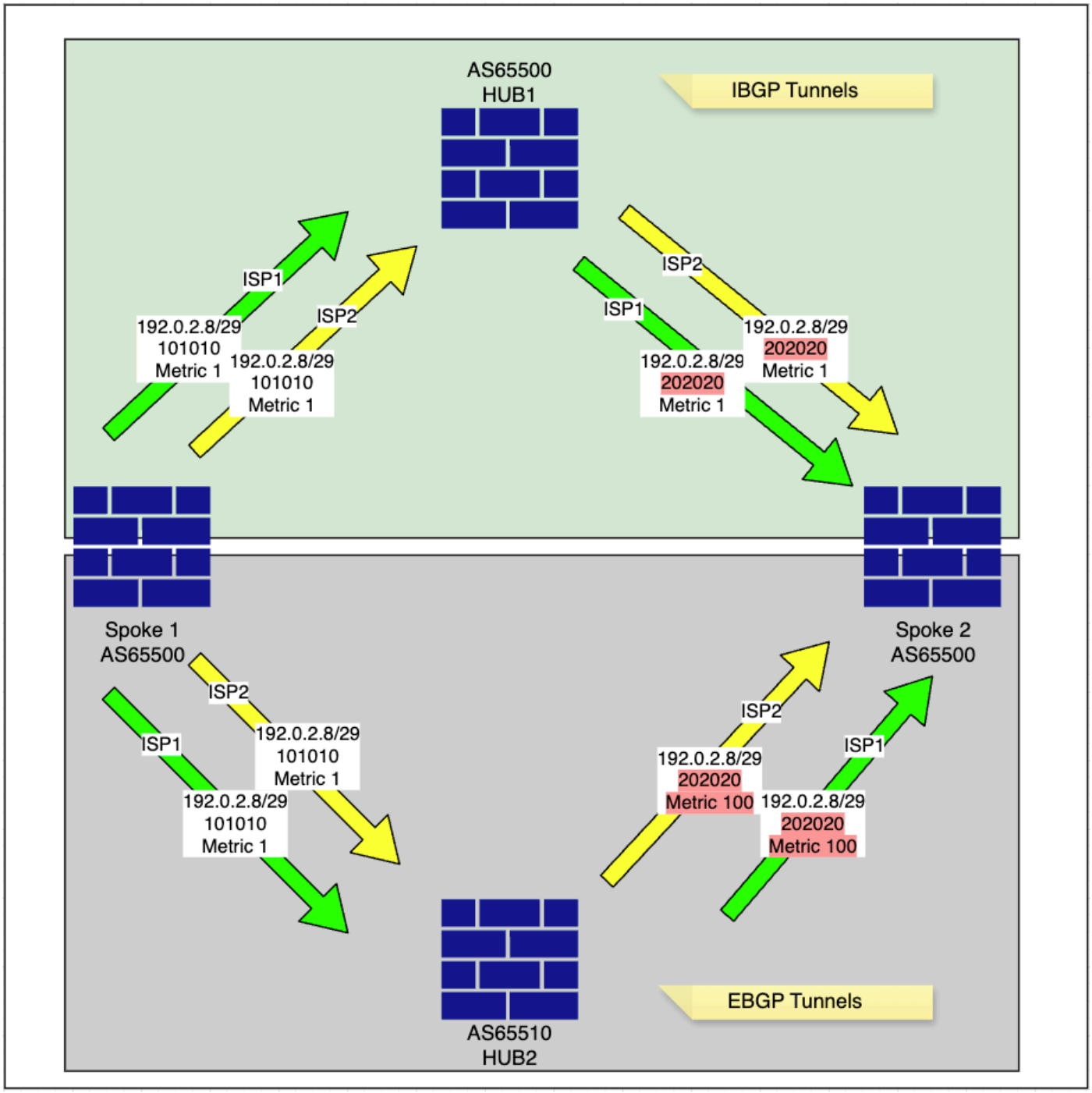
<<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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
```

Routing Topology



- The spoke advertises its internal network, 192.0.2.8/29, into BGP with a specific community tag of 101010, as configured in the route-map **FMC_VPN_CONNECTED_DIST_RMAP_101010**.

Spoke1

<#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

- The spoke modifies the metric value for its internal network, 192.0.2.8/29, and advertise it to the hubs, as configured in the route-maps **FMC_VPN_RMAP_COMMUNITY_OUT_8589939614** and **FMC_VPN_RMAP_COMMUNITY_OUT_8589942200**.

<#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 learns the Spoke 1 network 192.0.2.8/29 with the community tag 101010, and changes the community tag to 202020 while preserving the metric before forwarding it to other spokes, as defined in the configured route-maps.

HUB1

<#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 also learns the Spoke 1 network 192.0.2.8/29 with the community tag 101010, and changes the community tag to 202020 and update the metric to 100 before forwarding it to other spokes, as specified in the configured route-maps. This metric change takes effect due to eBGP peering. This is because MED (Multi-Exit Discriminator) is an optional, non-transitive BGP attribute used to influence inbound traffic by suggesting a preferred entry point into an AS. MED is generally not

propagated between iBGP peers within the same AS and instead advertised to external BGP (eBGP) peers in different autonomous systems.

HUB2

<#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
```

- Spoke 2 receives the Spoke 1 network 192.0.2.8/29 from both the HUB1 ISP1 and HUB1 ISP2 tunnels with a metric of 1, while it receives the same network from the HUB2 ISP1 and HUB2 ISP2 tunnels with an updated next-hop of HUB1.

Spoke 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
```

- Spoke 2 also advertises networks learned from HUB1 back to HUB2, as defined by the configured outbound route-map, with the updated metric.

<#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

The purpose of this document is to provide a walkthrough of the backend routing deployment, with a focus on the routing controls implemented within BGP to ensure both contingency and redundancy.

In summary, spoke 2 as well as any other spokes in the topology uses the same approach when advertising their networks into the BGP domain. The most important routing control in this scenario is community list

filtering, which ensures that only networks within this topology are advertised to other peers, preventing unintended network propagation.

Additionally, the MED Multi-exit Discriminator attribute is used to influence route selection for eBGP peers, ensuring that routes learned via the iBGP peer configured as the primary HUB are preferred over prefixes learned from the secondary HUB via eBGP.

By making topology adjustments, such as configuring iBGP for the secondary HUB, you can eliminate the need for MED manipulation and inbound route-maps that flip community tags before advertising the same network to other spokes.

Related Information

- For additional assistance, please contact TAC. A valid support contract is required:Cisco Worldwide Support Contacts.
- You can also visit the Cisco VPN Community for additional insights and trending discussions.