Begrijpen en oplossen van routebeheer in Secure Firewall SD-WAN-implementaties

Inhoud

Inleiding

Dit document beschrijft routeringscontrole in BGP voor routegebaseerde VPN's die Cisco SD-WAN gebruiken op een beveiligde firewall.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IKEv2
- Routegebaseerde VPN
- Virtual Tunnel Interfaces (VTI)
- IPSEC
- BGP

- BGP attributen zoals community tags en route reflectoren
- SD-WAN-functie op beveiligde firewall

Gebruikte componenten

De informatie in dit document is gebaseerd op:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Informatie over functies

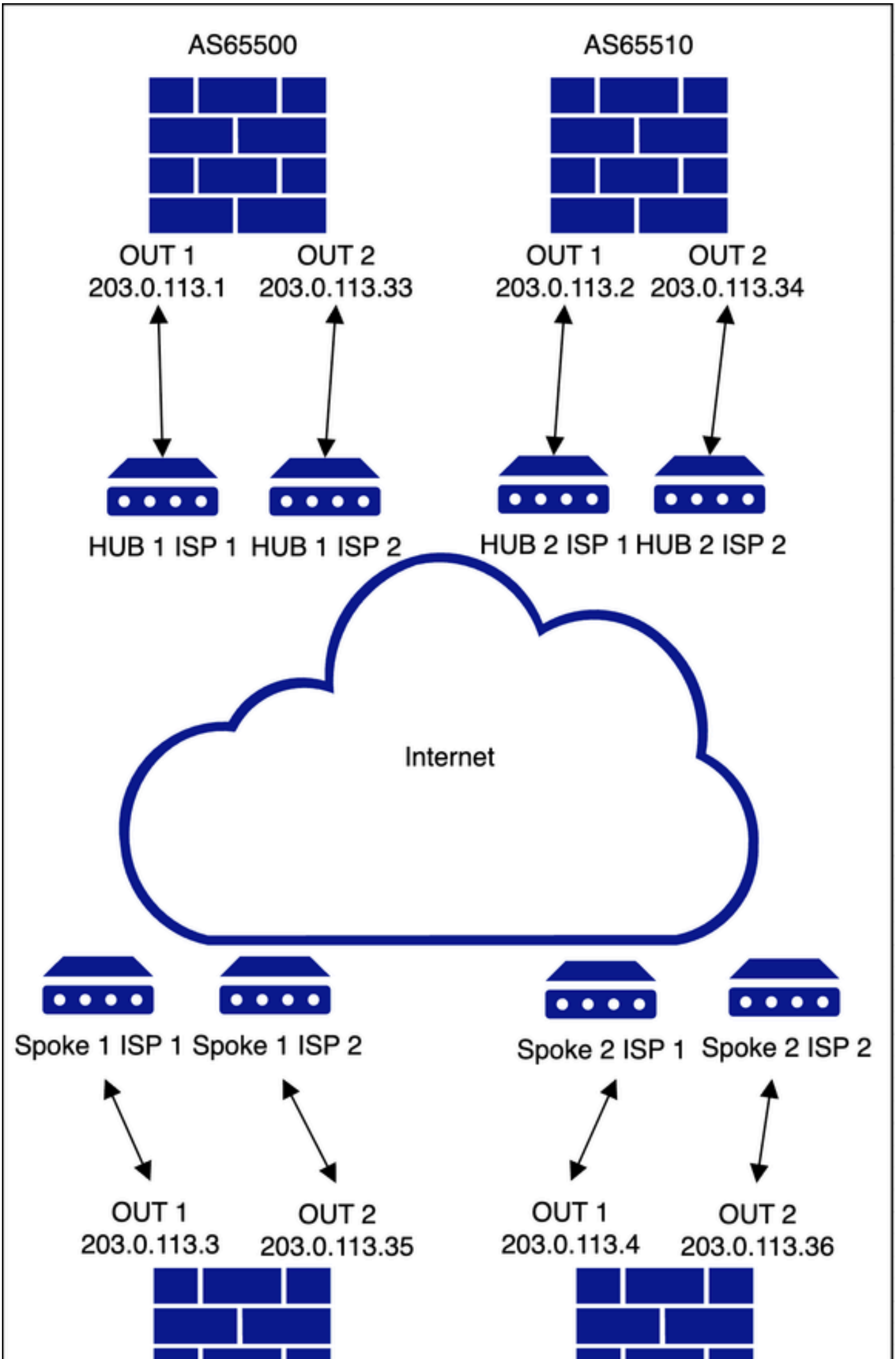
Met de nieuwe SD-WAN-implementatie voor site-to-site, routegebaseerde VPN met BGP ingeschakeld voor de overlay, richt Cisco zich op de belangrijkste BGP-kenmerken om loop-free en veilige overlay-routering te implementeren, zodat onderlay- en overlay-netwerken gescheiden blijven in de topologie. Deze implementatie zorgt er ook voor dat er geen handmatige interventie nodig is om de relevante attributen aan te passen.

Implementatiescenario

Selecteer een topologie die zowel iBGP- als eBGP-verbindingen tussen de HUB en de spaak bevat. Deze aanpak biedt maximale zichtbaarheid in de routeringscontroles die zijn geïmplementeerd als onderdeel van de SD-WAN-oplossing op Cisco Secure Firewalls.

Dual HUB en Spoke met Dual ISP

onderliggende topologie


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

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

Houd er rekening mee dat er één paar inkomende en uitgaande routekaarten per topologie is, hoewel de configuraties voor beide topologieën identiek zijn, alleen de naamgevingsconventie is uniek per topologie. In ons scenario zijn FMC_VPN_RMAP_COMMUNITY_IN_8589939614 en FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 voor topologie 1, terwijl FMC_VPN_RMAP_COMMUNITY_IN_8589942200 en FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 voor topologie 2 zijn.

<#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

De BGP-configuratie voor alle apparaten in de topologie wordt weergegeven:

Spoke1 en 2 (IBGP met HUB1 en EBGP met 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
```

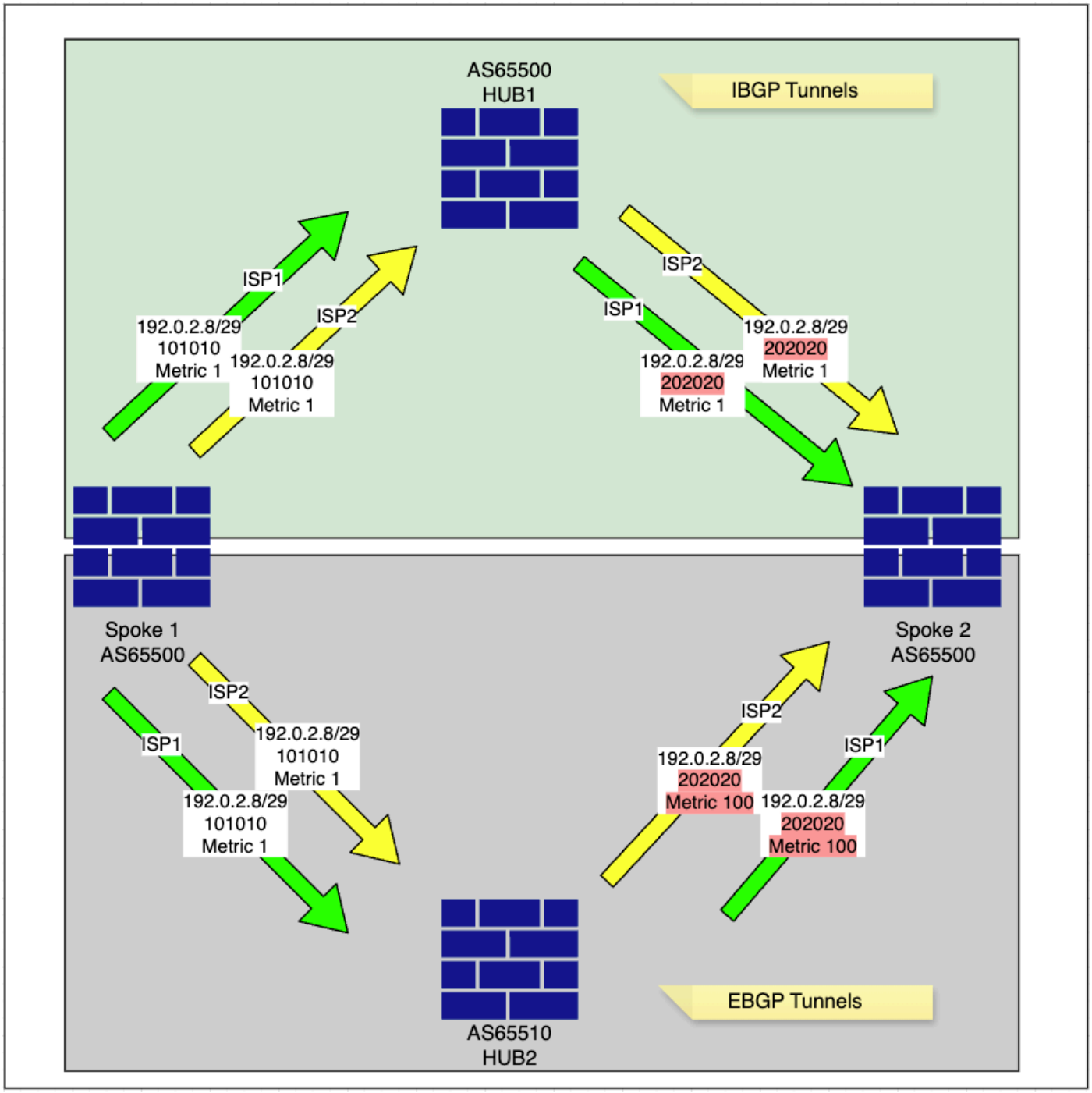
<<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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
```

routingtopologie



- De spoke adverteert zijn interne netwerk, 192.0.2.8/29, in BGP met een specifieke community-tag van 101010, zoals geconfigureerd in de routekaart 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
```

- De spoke wijzigt de metrische waarde voor zijn interne netwerk, 192.0.2.8/29, en adverteert deze aan de hubs, zoals geconfigureerd in de routekaarten FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 en 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 leert het Spoke 1-netwerk 192.0.2.8/29 met de community-tag 101010 en wijzigt de community-tag naar 202020 met behoud van de metric voordat deze wordt doorgestuurd naar andere spokes, zoals gedefinieerd in de geconfigureerde routekaarten.

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 leert ook het Spoke 1-netwerk 192.0.2.8/29 met de community-tag 101010 en wijzigt de community-tag naar 202020 en update de metric naar 100 voordat u deze doorstuurt naar andere spokes, zoals gespecificeerd in de geconfigureerde routekaarten. Deze metrische verandering treedt in werking als gevolg van eBGP-peering. Dit komt omdat MED (Multi-Exit Discriminator) een optioneel, niet-transitief BGP-attribuut is dat wordt gebruikt om inkomend verkeer te beïnvloeden door een voorkeursinvoerpunt in een AS voor te stellen. MED wordt over het algemeen niet verspreid tussen iBGP-peers binnen dezelfde AS en in plaats daarvan geadverteerd aan externe BGP-peers (eBGP) in verschillende autonome systemen.

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 ontvangt het Spoke 1-netwerk [192.0.2.8/29](192.0.2.8/29) van zowel de HUB1 ISP1- als HUB1 ISP2-tunnels met een metriek van 1, terwijl het hetzelfde netwerk ontvangt van de HUB2 ISP1- en HUB2 ISP2-tunnels met een bijgewerkte next-hop van HUB1.

Spreker 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 adverteert ook netwerken die zijn geleerd van HUB1 terug naar HUB2, zoals gedefinieerd door de geconfigureerde uitgaande routekaart, met de bijgewerkte metriek.

<#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
```

Conclusie

Het doel van dit document is om een walkthrough te bieden van de back-end routing-implementatie, met een focus op de routeringscontroles die binnen BGP worden geïmplementeerd om zowel contingentie als redundantie te garanderen.

Samenvattend, sprak 2 en alle andere sprekers in de topologie gebruiken dezelfde aanpak bij het adverteren van hun netwerken in het BGP-domein. De belangrijkste routeringscontrole in dit scenario is het filteren van de communitylijst, wat ervoor zorgt dat alleen netwerken binnen deze topologie worden geadverteerd aan andere peers, waardoor onbedoelde netwerkverspreiding wordt voorkomen.

Daarnaast wordt het attribuut MED Multi-exit Discriminator gebruikt om de routeselectie voor eBGP-peers te beïnvloeden, zodat routes die via de iBGP-peer zijn geleerd en die als primaire HUB zijn geconfigureerd, de voorkeur krijgen boven voorvoegsels die via eBGP van de secundaire HUB zijn geleerd.

Door topologische aanpassingen te maken, zoals het configureren van iBGP voor de secundaire HUB, kunt u de noodzaak voor MED-manipulatie en inkomende routekaarten elimineren die community-tags omdraaien voordat u hetzelfde netwerk naar andere spaken adverteert.

Gerelateerde informatie

- Voor aanvullende hulp kunt u contact opnemen met TAC. Een geldig supportcontract is vereist: Cisco Worldwide Support Contacts.
- U kunt ook de Cisco VPN Community bezoeken voor meer inzichten en trending discussies.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.