Routenkontrolle in SD-WAN-Bereitstellungen mit sicheren Firewalls verstehen und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

In diesem Dokument wird die Routing-Kontrolle in BGP für routenbasierte VPNs beschrieben, die Cisco SD-WAN in einer sicheren Firewall verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IKEv2
- Routenbasiertes VPN
- Virtuelle Tunnelschnittstellen (VTI)

- IPsec
- BGP
- BGP-Attribute wie Community-Tags und Routen-Reflektoren
- SD-WAN-Funktion in einer sicheren Firewall

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Informationen zu Funktionen

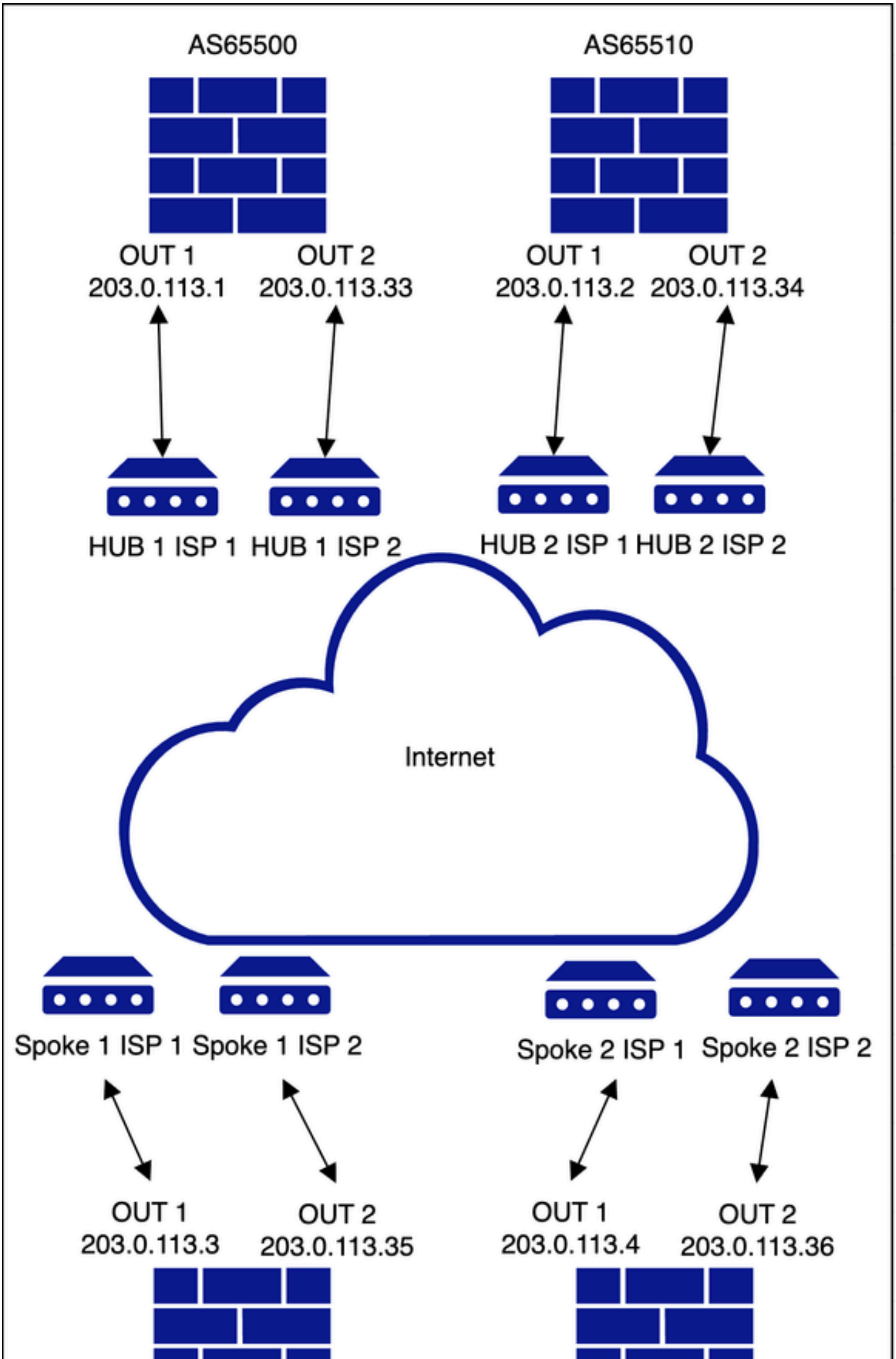
Mit der neuen SD-WAN-Bereitstellung für ein standortübergreifendes, routenbasiertes VPN mit aktiviertem BGP für das Overlay legt Cisco den Schwerpunkt auf wichtige BGP-Attribute zur Implementierung eines schleifenfreien und sicheren Overlay-Routings, wodurch sichergestellt wird, dass die Underlay- und Overlay-Netzwerke in der Topologie voneinander getrennt bleiben. Diese Bereitstellung stellt außerdem sicher, dass kein manueller Eingriff erforderlich ist, um die relevanten Attribute anzupassen.

Bereitstellungsszenario

Wählen Sie eine Topologie aus, die sowohl iBGP- als auch eBGP-Verbindungen zwischen HUB und Spoke umfasst. Dieser Ansatz bietet eine maximale Transparenz der Routing-Kontrollen, die als Teil der SD-WAN-Lösung in den Cisco Secure Firewalls implementiert sind.

Zwei HUBs und Spokes mit zwei ISPs

Underlay-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
<<<<<<<<<<
```

Beachten Sie, dass es für jede Topologie ein Paar von eingehenden und ausgehenden Routing-Maps gibt, obwohl die Konfigurationen für beide Topologien identisch sind. Die Namenskonvention ist jedoch für jede Topologie eindeutig. In unserem Szenario sind FMC_VPN_RMAP_COMMUNITY_IN_858.99.39.614 und FMC_VPN_RMAP_COMMUNITY_OUT_85.89.99.39.614 für Topologie 1 während FMC_VPN_RMAP_COMMUNITY_IN_858942200 und FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 sind für Topologie 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

Die BGP-Konfiguration für alle Geräte in der Topologie wird angezeigt:

Spoke1 und 2 (IBGP mit HUB1 und EBGP mit 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 mit den 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 mit den 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
```

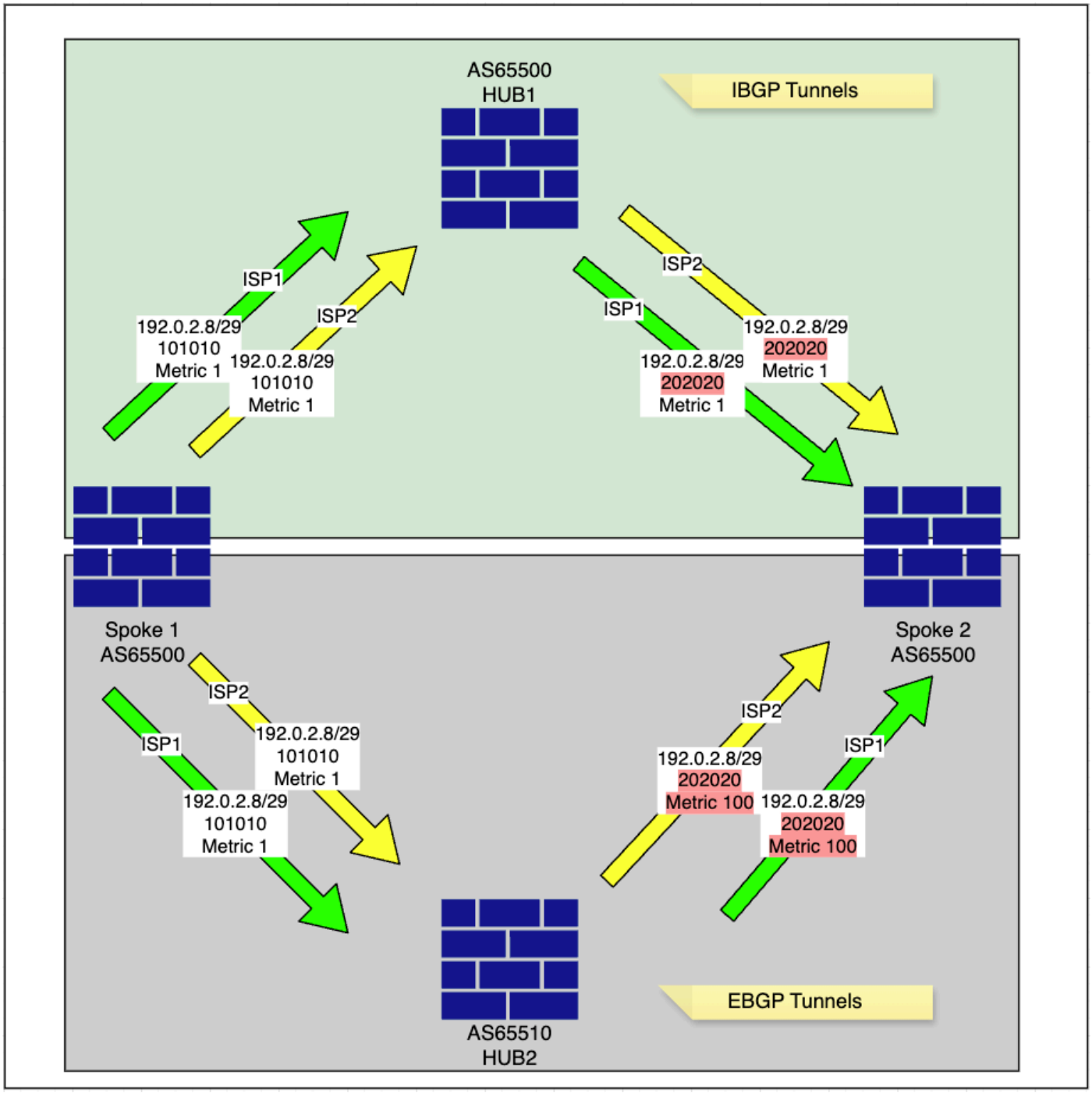
<<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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-Topologie



- Der Spoke meldet sein internes Netzwerk 192.0.2.8/29 an BGP mit einem spezifischen Community-Tag von 101010, wie in der Routing-Map FMC_VPN_CONNECTED_DIST_RMAP_1010 konfiguriert.

Speiche 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

- Der Spoke ändert den Metrikwert für sein internes Netzwerk 192.0.2.8/29 und kündigt ihn den Hubs an, wie in den Routenzuordnungen FMC_VPN_RMAP_COMMUNITY_OUT_858.993.9614 konfiguriert und FMC_VPN_RMAP_COMMUNITY_OUT_858.994.2200.

<#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 lernt das Spoke 1-Netzwerk 192.0.2.8/29 mit dem Community-Tag 101010 und ändert das Community-Tag auf 202020, wobei die Metrik beibehalten wird, bevor sie an andere Stationen weitergeleitet wird, wie in den konfigurierten Routen-Maps definiert.

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 lernt auch das Spoke 1-Netzwerk 192.0.2.8/29 mit dem Community-Tag 101010, ändert das Community-Tag auf 202020 und aktualisiert die Metrik auf 100, bevor es an andere Stationen weitergeleitet wird, wie in den konfigurierten Routen-Maps angegeben. Diese Metrikänderung wird durch eBGP-Peering wirksam. MED (Multi-Exit Discriminator) ist ein optionales, nicht transitives BGP-Attribut, das zur Beeinflussung des eingehenden Datenverkehrs verwendet wird, indem ein bevorzugter Eintrittspunkt in ein AS vorgeschlagen wird. MED wird im Allgemeinen nicht zwischen iBGP-Peers innerhalb desselben AS propagiert und stattdessen externen BGP (eBGP)-Peers in verschiedenen autonomen Systemen angekündigt.

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 empfängt das Spoke 1-Netzwerk 192.0.2.8/29 von den beiden HUB1-ISP1- und HUB1-ISP2-Tunneln mit einer Metrik von 1, während es dasselbe Netzwerk von den HUB2-ISP1- und HUB2-ISP2-Tunneln mit einem aktualisierten Next-Hop von HUB1 empfängt.

Speiche 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 kündigt außerdem die von HUB1 bezogenen Netzwerke gemäß der konfigurierten Outbound-Routing-Map mit der aktualisierten Metrik an HUB2 an.

<#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
```

Schlussfolgerung

In diesem Dokument wird eine exemplarische Vorgehensweise für die Bereitstellung des Backend-Routings beschrieben. Der Schwerpunkt liegt dabei auf den im BGP implementierten Routingkontrollen, um sowohl Kontingenz als auch Redundanz sicherzustellen.

Zusammenfassend lässt sich sagen, dass Spoke 2 und alle anderen Spokes in der Topologie denselben Ansatz verwenden, wenn sie ihre Netzwerke in der BGP-Domäne ankündigen. Die wichtigste Routing-Kontrolle in diesem Szenario ist die Community-Listenfilterung, die sicherstellt, dass nur Netzwerke in dieser Topologie anderen Peers angekündigt werden, um eine unbeabsichtigte Netzwerkausbreitung zu verhindern.

Darüber hinaus wird das Attribut MED Multi-exit Discriminator verwendet, um die Routenauswahl für eBGP-Peers zu beeinflussen und sicherzustellen, dass Routen, die über den als primäres HUB konfigurierten iBGP-Peer bezogen werden, gegenüber Präfixen, die vom sekundären HUB über eBGP bezogen werden, bevorzugt werden.

Durch Topologieanpassungen, z. B. durch die Konfiguration von iBGP für den sekundären HUB, können Sie MED-Manipulation und eingehende Routing-Maps, die Community-Tags umdrehen, bevor Sie dasselbe Netzwerk an andere Stationen weitergeben, überflüssig machen.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie beim TAC. Ein gültiger Support-Vertrag ist erforderlich:Cisco Worldwide Support Contacts
- Weitere Einblicke und Gespräche zu Trends finden Sie außerdem in der Cisco VPN Community.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.