Comprensión y solución de problemas del control de rutas en implementaciones de SD-WAN de firewall seguro

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
  - Información sobre la Función
- Escenario de implementación
  - HUB y radio duales con ISP duales
    - Topología subyacente
    - Topología de superposición
    - Configuración
    - Verificación y resolución de problemas
    - Configuración común para todos los dispositivos
    - Spoke 1 y 2 (IBGP con HUB1 y EBGP con HUB2)
    - HUB1 (iguales IBGP con los radios)
    - HUB2 (Peering EBGP con los Spokes)
    - Topología de routing
    - Spoke1
    - HUB1
    - HUB2
    - Spoke 2
- Conclusión
- Información Relacionada

Introducción

Este documento describe el control de ruteo en BGP para VPNs basadas en rutas que utilizan Cisco SD-WAN en un firewall seguro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IKEv2
- VPN basada en ruta
- Interfaces de túnel virtual (VTI)

- IPsec
- BGP
- Atributos BGP como etiquetas de comunidad y reflectores de ruta
- Función SD-WAN en firewall seguro

Componentes Utilizados

La información de este documento se basa en:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Información sobre la Función

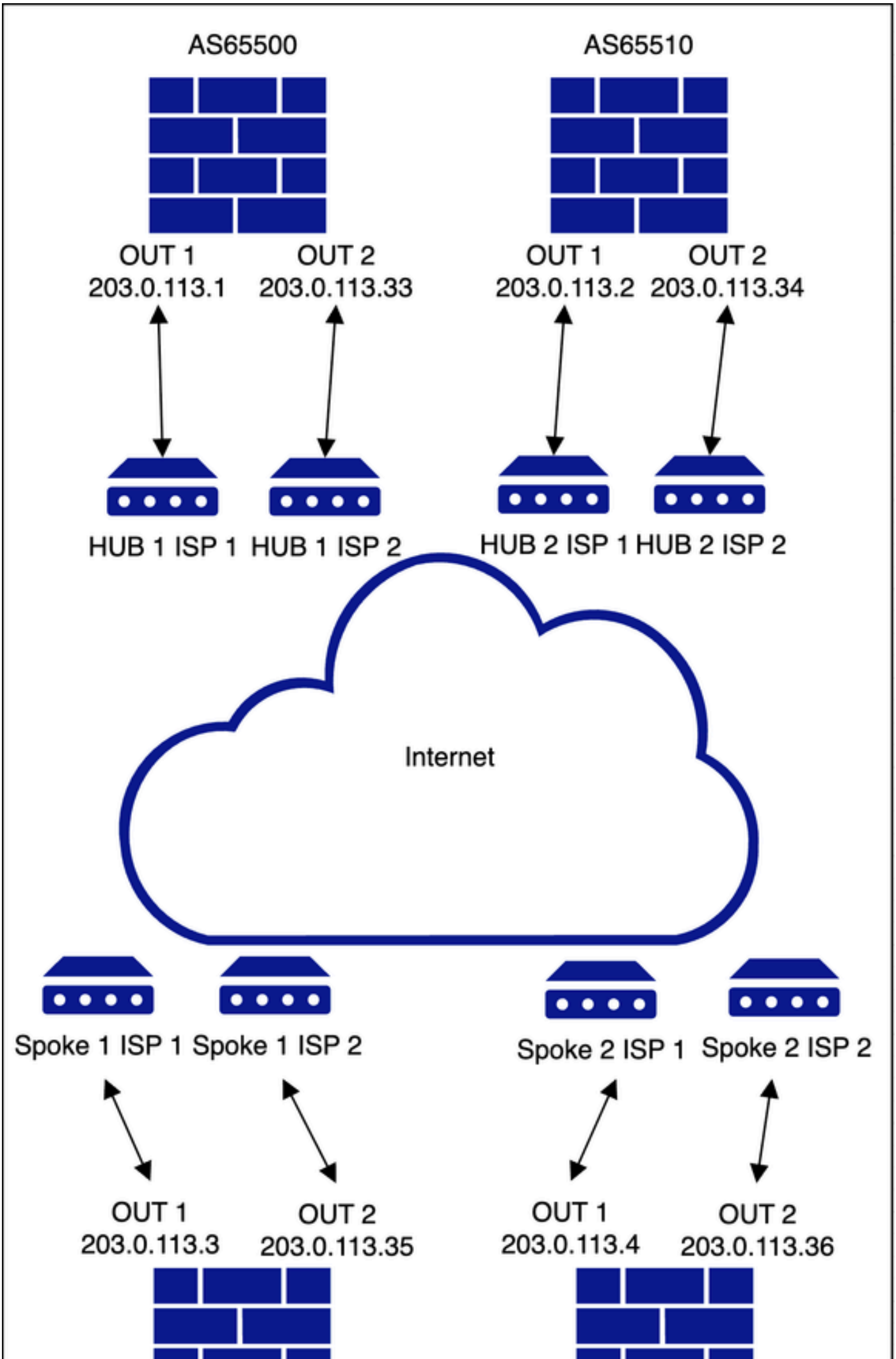
Con la nueva implementación de SD-WAN para VPN de sitio a sitio y basada en rutas con BGP habilitado para la superposición, Cisco se centra en los atributos BGP clave para implementar un routing de superposición seguro y sin bucles, lo que garantiza que las redes de superposición y superposición permanezcan separadas en toda la topología. Esta implementación también garantiza que no se requiere intervención manual para ajustar los atributos relevantes.

Escenario de implementación

Seleccione una topología que incluya conexiones iBGP y eBGP entre el HUB y el spoke. Este enfoque proporciona la máxima visibilidad de los controles de routing implementados como parte de la solución SD-WAN en Cisco Secure Firewalls.

HUB y radio duales con ISP duales

Topología subyacente


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

Tenga en cuenta que hay un solo par de mapas de ruta entrantes y salientes por topología, aunque las configuraciones son idénticas para ambas topologías, solo que la convención de nomenclatura es única por topología. En nuestro escenario, FMC_VPN_RMAP_COMMUNITY_IN_858939614 y FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 son para la topología 1 mientras que FMC_VPN_RMAP_COMMUNITY_IN_8589942200 y FMC_VPN_RMAP_COMMUNITY_OUT_8589942200 son para la topología 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

Se muestra la configuración BGP en todos los dispositivos de la topología:

Spoke1 y 2 (IBGP con HUB1 y EBGP con 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 (iguales IBGP con los radios)

<#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 (Peering EBGP con los 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
```

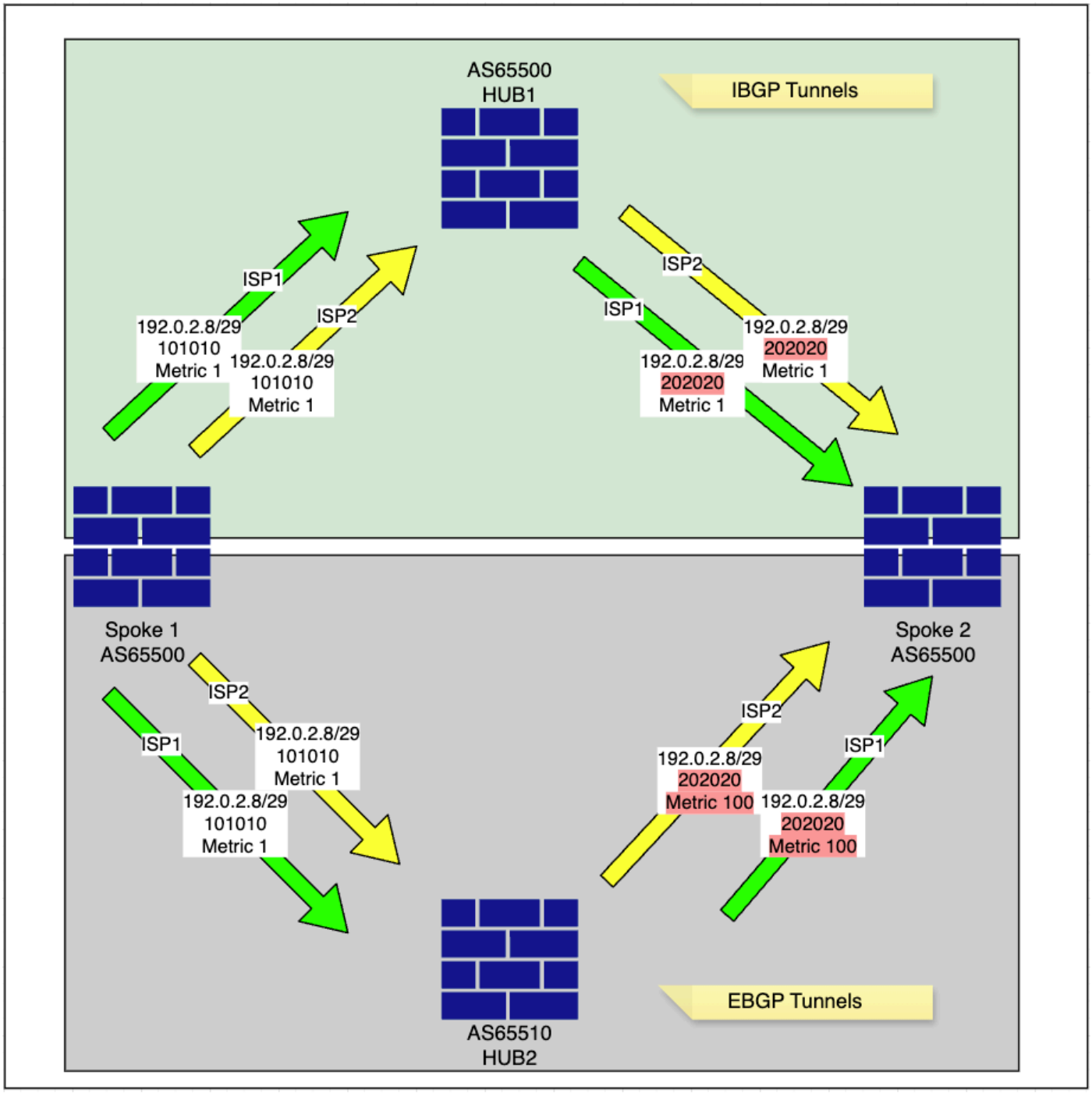
<<<<< tunnel from HUB 2 to Spoke 1 via ISP 2

```
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
```

Topología de routing



- El spoke anuncia su red interna, 192.0.2.8/29, en BGP con una etiqueta de comunidad específica de 101010, según lo configurado en el 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
```

- El spoke modifica el valor de la métrica para su red interna, 192.0.2.8/29, y lo anuncia a los hubs, según lo configurado en los route-maps FMC_VPN_RMAP_COMMUNITY_OUT_8589939614 y 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
```

- El HUB1 aprende la red Spoke 1 192.0.2.8/29 con la etiqueta de comunidad 101010 y cambia la etiqueta de comunidad a 202020 mientras conserva la métrica antes de reenviarla a otros spokes, como se define en los route-maps configurados.

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 también aprende la red Spoke 1 192.0.2.8/29 con la etiqueta de comunidad 101010, y cambia la etiqueta de comunidad a 202020 y actualiza la métrica a 100 antes de reenviarla a otros spokes, como se especifica en los route-maps configurados. Este cambio de métrica tiene efecto debido al peering eBGP. Esto se debe a que MED (Multi-Exit Discriminator) es un atributo BGP opcional no transitivo que se utiliza para influir en el tráfico entrante al sugerir un punto de entrada preferido en un AS. MED no se propaga generalmente entre los peers iBGP dentro del mismo AS y en su lugar se anuncia a peers BGP externos (eBGP) en diferentes sistemas autónomos.

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 recibe la red Spoke 1 192.0.2.8/29 de los túneles ISP1 y ISP2 del HUB1 con una métrica de 1, mientras que recibe la misma red de los túneles ISP1 y ISP2 del HUB2 con un salto siguiente actualizado del 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 también anuncia las redes aprendidas del HUB1 de vuelta al HUB2, según lo

definido por el route-map saliente configurado, con la métrica actualizada.

<#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
```

Conclusión

El propósito de este documento es proporcionar un tutorial de la implementación de ruteo backend, con un enfoque en los controles de ruteo implementados dentro de BGP para garantizar tanto la contingencia como la redundancia.

En resumen, spoke 2 así como cualquier otro spoke en la topología utiliza el mismo enfoque al anunciar sus redes en el dominio BGP. El control de routing más importante en este escenario es el filtrado de listas de comunidades, que garantiza que solo las redes de esta topología se anuncien a otros peers, lo que evita la propagación no intencionada de la red.

Además, el atributo MED Multi-exit Discriminator se utiliza para influir en la selección de rutas para los peers eBGP, asegurándose de que las rutas aprendidas a través del peer iBGP configurado como el HUB principal sean preferidas sobre los prefijos aprendidos del HUB secundario a través de eBGP.

Al realizar ajustes de topología, como la configuración de iBGP para el HUB secundario, puede eliminar la necesidad de manipulación MED y de mapas de ruta entrantes que voltean las etiquetas de comunidad antes de anunciar la misma red a otros radios.

Información Relacionada

- Para obtener ayuda adicional, póngase en contacto con el TAC. Se necesita un contrato de asistencia válido:Contactos de asistencia globales de Cisco.
- También puede visitar la Cisco VPN Community para obtener más información y conocer las tendencias.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).