

# Configure Google Cloud Interconnect como transporte con Cisco SD-WAN en un solo clic

## Contenido

[Introducción](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Descripción general del diseño](#)

[Detalles de la solución](#)

[Paso 1. Preparación](#)

[Paso 2. Creación de Cisco Cloud Gateway con Cloud OnRamp para flujos de trabajo en varias nubes](#)

[Paso 3. En la consola GCP, agregue una conexión de interconexión de partners](#)

[Paso 4. Utilice Cloud onRamp Interconnect en Cisco vManage para crear la conexión de DC](#)

[Paso 5. Configuración del router DC para establecer túneles a través de Internet y a través de la interconexión en la nube GCP](#)

[Verificación](#)

[Configuración del router SD-WAN Megaport de DC](#)

## Introducción

Este documento describe cómo utilizar Google [Cloud Interconnect](#) como transporte de red de área extensa (SD-WAN) definido por software.

## Antecedentes

Los clientes empresariales con cargas de trabajo en la plataforma de nube de Google (GCP) utilizan [Cloud Interconnect](#) para la conectividad de Data Center o Hub. Al mismo tiempo, la conexión pública a Internet también es muy común en el Data Center y se utiliza como base para la conectividad SD-WAN con otras ubicaciones. En este artículo se describe cómo se puede utilizar GCP Cloud Interconnect como elemento subyacente para la SD-WAN de Cisco.

Es muy similar a lo que describe la misma solución para AWS.

La ventaja clave del uso de GCP Cloud Interconnect como otro transporte para Cisco SD-WAN es la capacidad de utilizar políticas SD-WAN en todos los transportes, incluido GCP Cloud Interconnect. Los clientes pueden crear políticas de reconocimiento de aplicaciones SD-WAN y enrutar aplicaciones críticas a través de GCP Cloud Interconnect y volver a enrutar a través de Internet pública en caso de infracciones de SLA.

## Problema

GCP Cloud Interconnect no proporciona capacidades SD-WAN nativas. Las preguntas típicas de

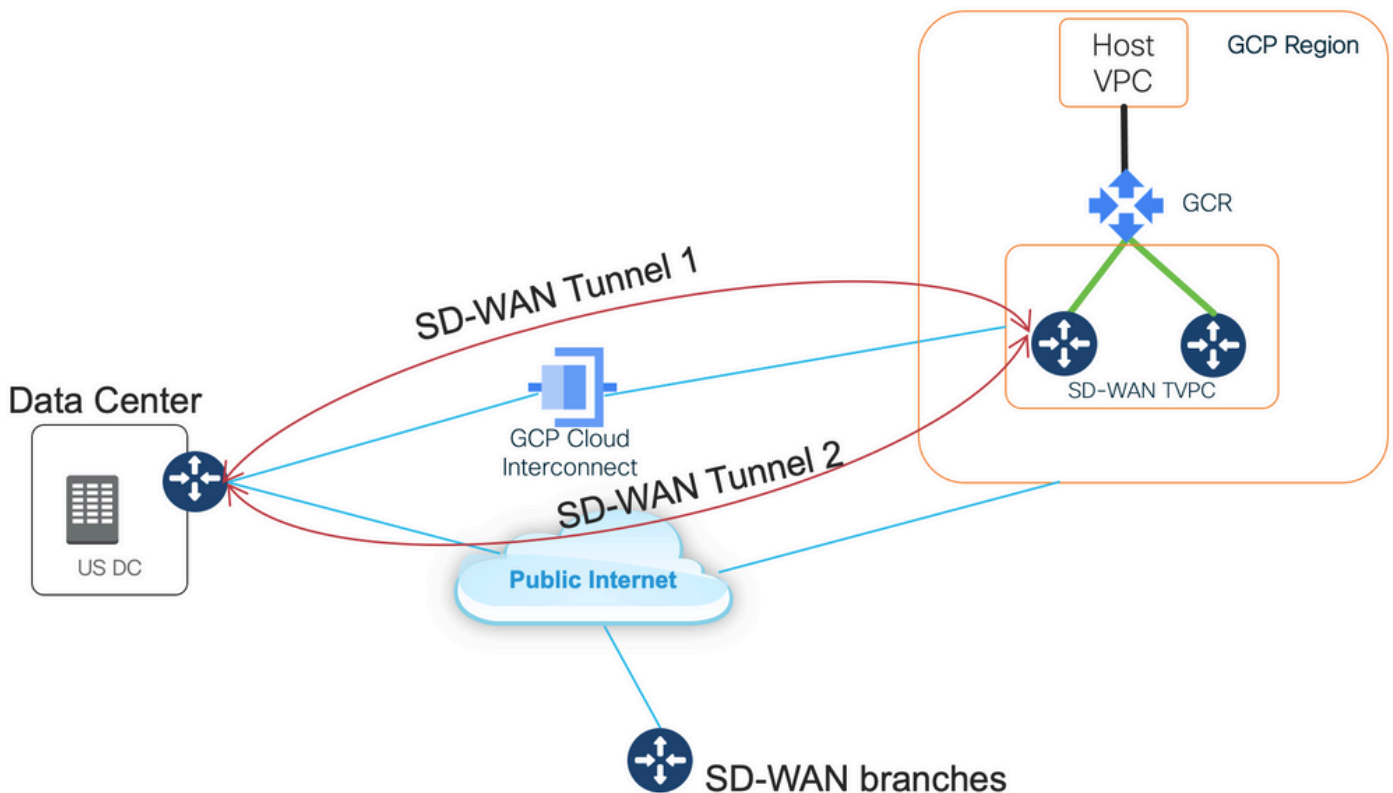
los clientes de la SD-WAN empresarial son:

- "¿Puedo utilizar GCP Cloud Interconnect como elemento subyacente para Cisco SD-WAN?"
- "¿Cómo puedo interconectar GCP Cloud Interconnect y Cisco SD-WAN?"
- "¿Cómo puedo crear una solución flexible, segura y escalable?"

## Solución

### Descripción general del diseño

El punto de diseño clave es la conexión del Data Center a través de GCP Cloud Interconnect a los routers SD de Cisco creados por Cloud onRamp para el aprovisionamiento de varias nubes, como se muestra en la imagen.



Las ventajas de esta solución son las siguientes:

- Totalmente automático: Cisco Cloud onRamp para la automatización de la nube múltiple se puede utilizar para implementar VPC de tránsito SD-WAN con dos routers SD-WAN. Los VPC host se pueden detectar como parte de la nube en rampa y se asignan a redes SD-WAN con un solo clic.
- SD-WAN completo sobre interconexión en la nube GCP: GCP Cloud Interconnect es sólo otro transporte SD-WAN. Todas las funciones de SD-WAN, como las políticas con reconocimiento de aplicaciones, el cifrado, etc., se pueden utilizar de forma nativa en el túnel SD-WAN a través de GCP Cloud Interconnect.

Tenga en cuenta que la escalabilidad de esta solución va a la par con el rendimiento de C8000V en GCP. Consulte [SalesConnect](#) para obtener detalles sobre el rendimiento de C8000v en GCP.

### Detalles de la solución

El punto clave para comprender esta solución son los colores SD-WAN. Tenga en cuenta que los routers GCP SD-WAN tendrán **color privado2** para la conectividad a Internet, así como conectividad a través de Interconnect, los túneles SD-WAN se formarán a través de Internet utilizando direcciones IP públicas y túneles SD-WAN (utilizando la misma interfaz) a través de los circuitos de interconexión utilizando direcciones IP privadas a un DC/sitio. Esto significa que el router del Data Center (biz-internet color) establecerá una conexión a los routers GCP SD-WAN (privado2 color) a través de Internet con direcciones IP públicas y a través de Su color privado sobre IP privada.

Información genérica sobre los colores SD-WAN:

Los localizadores de transporte (TLOC) hacen referencia a las interfaces de transporte WAN (VPN 0) mediante las cuales los routers SD-WAN se conectan a la red subyacente. Cada TLOC se identifica de forma única mediante una combinación de la dirección IP del sistema del router SD-WAN, el color de la interfaz WAN y la encapsulación de transporte (GRE o IPsec). Cisco Overlay Management Protocol (OMP) se utiliza para distribuir las TLOC (también conocidas como rutas TLOC), prefijos de superposición SD-WAN (también conocidos como rutas OMP) y otra información entre routers SD-WAN. Es a través de las rutas TLOC que los routers SD-WAN saben cómo llegar entre sí y establecer túneles VPN IPsec entre sí.

Los routers y/o controladores SD-WAN (vManage, vSmart o vBond) pueden estar detrás de los dispositivos de traducción de direcciones de red (NAT) dentro de la red. Cuando un router SD-WAN se autentica en un controlador vBond, el controlador vBond aprenderá tanto la dirección IP privada/número de puerto como la dirección IP pública/número de puerto del router SD-WAN durante el intercambio. Los controladores de vBond actúan como Utilidades transversales de sesión para servidores NAT (STUN), lo que permite a los routers SD-WAN detectar direcciones IP asignadas o traducidas y números de puerto de sus interfaces de transporte WAN.

En los routers SD-WAN, cada transporte WAN se asocia a un par de direcciones IP públicas y privadas. La dirección IP privada se considera la dirección NAT previa. Se trata de una dirección IP asignada a la interfaz WAN del router SD-WAN. Aunque se considera que esta es la dirección IP privada, esta dirección IP puede ser parte del espacio de direcciones IP enrutables públicamente o parte del espacio de direcciones IP no enrutables públicamente RFC 1918 de IETF. La dirección IP pública se considera la dirección posterior a NAT. El servidor vBond detecta esto cuando el router SD-WAN se comunica y autentica inicialmente con el servidor vBond. La dirección IP pública también puede ser parte del espacio de dirección IP enrutable públicamente o parte del espacio de dirección IP no enrutable públicamente RFC 1918 de IETF. En ausencia de NAT, las direcciones IP públicas y privadas de la interfaz de transporte SD-WAN son iguales.

Los colores TLOC son palabras clave definidas estáticamente que se utilizan para identificar los transportes WAN individuales en cada router SD-WAN. Cada transporte WAN en un router SD-WAN determinado debe tener un color único. Los colores también se utilizan para identificar un transporte WAN individual como público o privado. Los colores metro-ethernet, Mpls y private1, private2, private3, private4, private5 y private6 se consideran colores privados. Están pensados para su uso en redes privadas o lugares donde no hay NAT. Los colores son 3g, internet biz, azul, bronce, personalizado1, personalizado2, personalizado3, predeterminado, oro, verde, lte, internet público, rojo y plateado se consideran colores públicos. Se pretende que se utilicen en redes públicas o en lugares con direcciones IP públicas de las interfaces de transporte WAN, ya sea de forma nativa o a través de NAT.

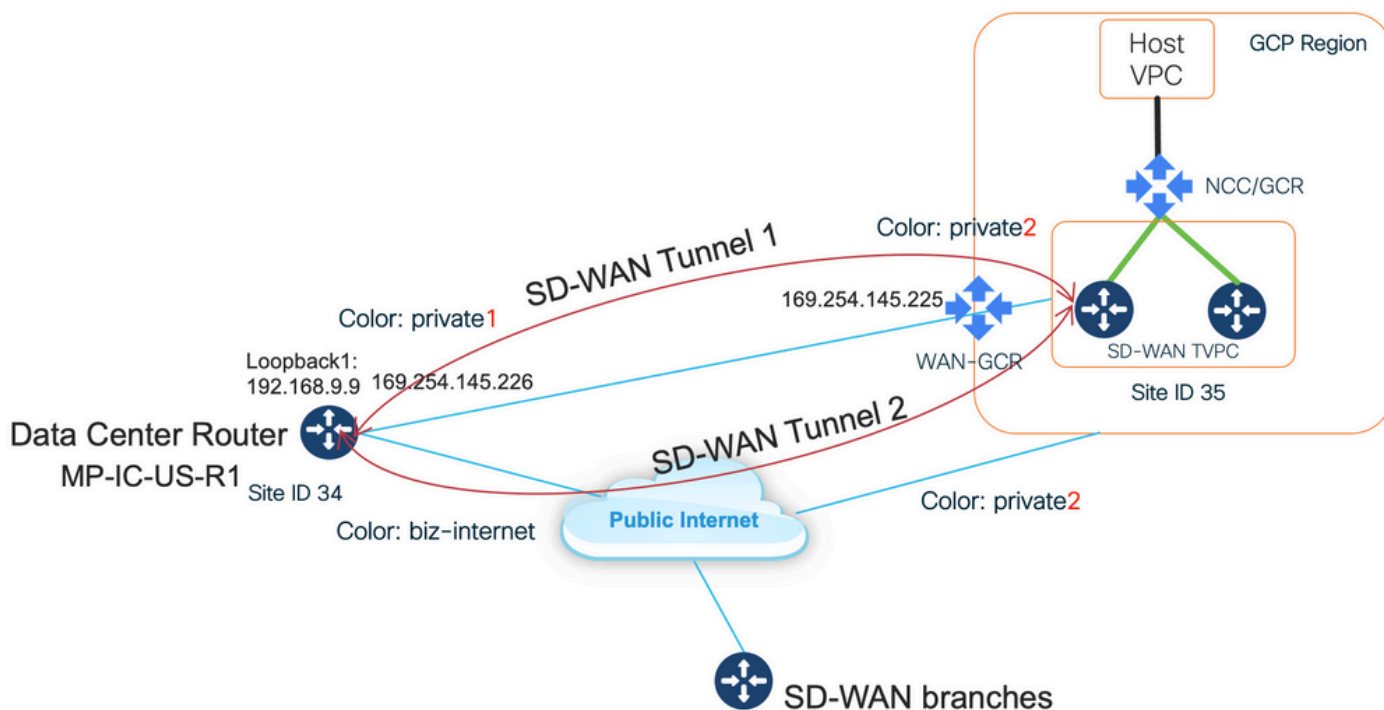
El color indica el uso de direcciones IP privadas o públicas al comunicarse a través de los planos de control y datos. Cuando dos routers SD-WAN intentan comunicarse entre sí, ambos utilizando interfaces de transporte WAN con colores privados, cada lado intentará conectarse a la dirección

IP privada del router remoto. Si uno o ambos lados utilizan colores públicos, cada lado intentará conectarse a la dirección IP pública del router remoto. Una excepción es cuando los ID de sitio de dos dispositivos son iguales. Cuando los ID del sitio son iguales, pero los colores son públicos, las direcciones IP privadas se utilizarán para la comunicación. Esto puede ocurrir para los routers SD-WAN que intentan comunicarse con un controlador vManage o vSmart ubicado dentro del mismo sitio. Tenga en cuenta que los routers SD-WAN no establecen túneles VPN IPsec entre sí cuando tienen los mismos ID de sitio.

Esta es la salida del router del Data Center, que muestra dos túneles a través de Internet (color biz-internet) y dos túneles a través de GCP Cloud Interconnect (color privado1) a dos routers SD-WAN. Consulte la configuración completa del router DC en el archivo adjunto para obtener más detalles.

```
MP-IC-US-R1#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec UPTIME
TRANSITIONS
-----
-----
-----
35.35.35.2 35 up biz-internet private2 162.43.150.15 35.212.162.72 12347 ipsec 7 1000 10
4:02:55:32 0
35.35.35.1 35 up biz-internet private2 162.43.150.15 35.212.232.51 12347 ipsec 7 1000 10
4:02:55:32 0
35.35.35.1 35 up private1 private2 192.168.9.9 10.35.0.2 12347 ipsec 7 1000 10 0:00:00:16 0
35.35.35.2 35 up private1 private2 192.168.9.9 10.35.0.3 12347 ipsec 7 1000 10 0:00:00:16 0
...
MP-IC-US-R1#
```

Esta imagen ilustra los detalles de la topología con direcciones IP y colores SD-WAN, que se utilizan para verificar la solución.



Software utilizado:

- Controladores SD-WAN que ejecutan CCO versión 20.7.1.1
- Router de Data Center simulado con C8000v con 17.06.01a provisionado a través de

vManage Cloud onRamp para la interconexión con Megaport

- Dos routers SD-WAN en GCP: C8000v con 17.06.01a aprovisionado mediante vManage Cloud onRamp para varias nubes

## **Paso 1. Preparación**

Asegúrese de que Cisco vManage tenga una cuenta GCP en funcionamiento definida y que los valores globales de Cloud onRamp estén configurados correctamente.

También defina una cuenta de partner de interconexión en vManage. En este blog Megaport se utiliza como partner de Interconnect, por lo que puede definir una cuenta adecuada y una configuración global.

## **Paso 2. Creación de Cisco Cloud Gateway con Cloud OnRamp para flujos de trabajo en varias nubes**

Este es un proceso sencillo: seleccione dos dispositivos SD-WAN, adjunte la plantilla GCP predeterminada e implemente. Consulte la [documentación sobre la nube en ramp para la nube múltiple](#) para obtener más detalles.

## **Paso 3. En la consola GCP, agregue una conexión de interconexión de partners**

Utilice el flujo de trabajo de configuración paso a paso de GCP (**Conectividad híbrida > Interconexión**) para crear una conexión de interconexión de partners con un partner seleccionado, en el caso de este blog - con Megaport como se muestra en la imagen.

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

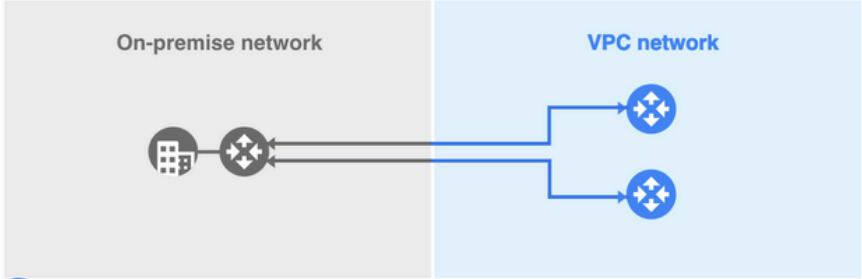
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

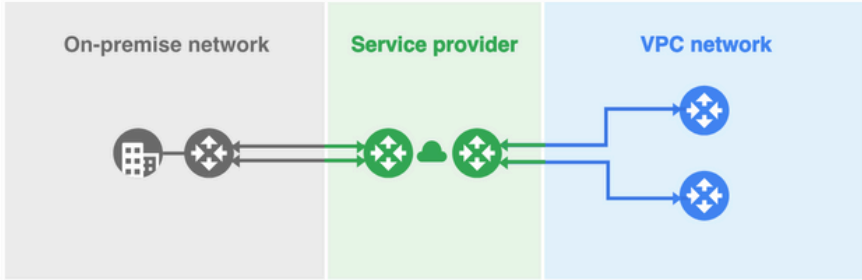
**Interconnect type**

**Dedicated Interconnect connection** Connect your on-premises network to your Google Cloud VPC network by connecting a new fiber to your equipment. [Learn more](#)



The diagram shows an 'On-premise network' on the left with a server and a router icon. Two blue lines connect this router to two blue router icons in the 'VPC network' on the right.

**Partner Interconnect connection** Connect your on-premises network to your Google Cloud VPC network through a connection from a supported service provider. [Learn more](#) or [check supported service providers](#)



The diagram shows an 'On-premise network' on the left with a server and a router icon. A green line connects this router to a green router icon in the 'Service provider' section. Another green line connects this service provider router to a second green router icon, which is then connected to two blue router icons in the 'VPC network' on the right.

**CONTINUE** CANCEL

Seleccione la opción **YA TENGO UN PROVEEDOR DE SERVICIOS**.

Para facilitar la demostración, se utiliza **Create a single VLAN** option without redundancy.

Seleccione el nombre de red correcto, creado anteriormente por Cloud onRamp para el flujo de trabajo de varias nubes. En la sección VLAN, puede crear un nuevo router GCR y definir un nombre para la VLAN, que luego se mostrará en la sección Cloud onRamp Interconnect.

Esta imagen refleja todos los puntos mencionados.

Hybrid Connectivity	<a href="#">←</a> Add Partner VLAN attachment
VPN	<span>✓</span> Check your connection — <b>2</b> Add VLAN attachments — <span>3</span> Connect to your VPC networks
Interconnect	<p>A VLAN attachment allows you to access your VPC network by adding a VLAN to your existing service provider connection. <a href="#">Learn more</a></p> <p><b>Redundancy</b></p> <p>Creating a redundant pair of VLANs is recommended to increase availability. If you don't need redundancy or an SLA, you can create a single VLAN attachment (and make it redundant later). <a href="#">Learn more about redundancy</a></p> <p> <input type="radio"/> Create a redundant pair of VLAN attachments (recommended)  <input type="radio"/> Add a redundant VLAN to an existing VLAN  <input checked="" type="radio"/> Create a single VLAN (no redundancy)       </p> <p>Network * wan-mc-demo-npitaev</p> <p>Region * us-west1 (Oregon) <span>?</span> Region is permanent</p> <p><b>VLAN</b></p> <p>Cloud Router * gcp-gcr-ic-r1 <span>?</span></p> <p>VLAN attachment name * test-vlan-name <span>?</span> Lowercase letters, numbers, hyphens allowed</p> <p>Description VLAN for Megaport</p> <p>Maximum transmission unit (MTU) * 1440</p>
Cloud Routers	
Network Connectivity Center	

Básicamente, una vez Paso 3. se completa, simplemente puede tomar la configuración de BGP y hacer que la conectividad se base en lo que el proveedor de Interconnect ha utilizado. En este caso, Megaport se utiliza para la prueba. Sin embargo, puede utilizar cualquier tipo de interconexión que puede ser a través de Megaport, Equinix o un MSP.

#### Paso 4. Utilice Cloud onRamp Interconnect en Cisco vManage para crear la conexión de DC

Al igual que el blog de AWS, utilice el flujo de trabajo de Cisco Cloud onRamp Interconnect con Megaport para crear un router de Data Center y utilizarlo para GCP Cloud Interconnect. Tenga en cuenta que Megaport se utiliza aquí sólo para realizar pruebas, si ya dispone de una configuración de Data Center, no es necesario utilizar Megaport.

En Cisco vManage, seleccione un router SD-WAN gratuito, adjunte la plantilla de megaport de CoR predeterminada e implétela como Cisco Cloud Gateway en Megaport mediante el flujo de trabajo de CoR Interconnect.

Una vez que el router SD-WAN de Cisco en Megaport esté activo, utilice el flujo de trabajo de la interconexión CoR para crear una conexión como se muestra en la imagen.

Cisco vManage Select Resource Group Configuration · Cloud onRamp for Multicloud

Cloud OnRamp For Multicloud > Interconnect Connectivity > Add Connection

Interconnect Gateway MP-IC-GW-US1 1 Destination 2 Primary MP-IC-GW-US1 3 Details 4 Summary

**DESTINATION**

Destination Type: Cloud  
 Cloud Service Provider: Google Cloud  
 Google Account: GCP-rpitsev  
 Redundancy: Disable  
 Google Cloud Interconnect Attachment: us-west1:gcp-gcrlc-r1:gcr-megaport-vlan

**DETAILS**

Settings: Auto-generated  
 Segment: 10

**PRIMARY**

Peering Location: San Jose (sjc-zone2-6) - San Jose - CA - USA  
 Connection Name: MP-GCP-SJ-Peering  
 Bandwidth(Mbps): 50

Connection Name : MP-GCP-SJ-Peering

Cancel Back Save

## Paso 5. Configuración del router DC para establecer túneles a través de Internet y a través de la interconexión en la nube GCP

Ponga el router megaport SD-WAN en modo CLI y **mueva** la configuración del lado del servicio a VPN0. Debido a que GCP utiliza direcciones IP 169.254.x.y, puede crear la interfaz Loopback1 en el router DC y utilizarla para la comunicación SD-WAN sobre la interconexión en la nube GCP.

Estas son las partes relevantes de la configuración del router DC.

```
interface Loopback1
no shutdown
ip address 192.168.9.9 255.255.255.255
!
!
interface Tunnel2
ip unnumbered Loopback1
tunnel source Loopback1
tunnel mode sdwan
!
!
interface GigabitEthernet1.215
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
ip mtu 1440
!
!
router bgp 64513
bgp log-neighbor-changes
neighbor 169.254.145.225 remote-as 16550
neighbor 169.254.145.225 description MP-GCP-SJ-Peering
neighbor 169.254.145.225 ebgp-multihop 4
!
address-family ipv4
network 192.168.9.9 mask 255.255.255.255
neighbor 169.254.145.225 activate
neighbor 169.254.145.225 send-community both
exit-address-family
```



```

!
!
sdwan
interface Loopback1
tunnel-interface
encapsulation ipsec preference 100 weight 1
color privatel
max-control-connections 0
allow-service all
!

```

Consulte la configuración completa del router DC en la última sección del documento.

## Verificación

Estado de interconexión de la nube de GCP:

The screenshot shows the Google Cloud Platform console for the project 'npitaev-20-4-efg-gcp-project'. The 'Interconnect' page is active, showing 'VLAN ATTACHMENTS' for a Dedicated Interconnect connection. A table lists the following attachment:

Name	Region	Status	Type	Bandwidth	Cloud Router	VLAN ID	Cloud Router IP	On-premises router IP	Interconnect	Des	Actions
gcr-megaport-vlan	us-west1	Up	Partner	50 Mb/s	gcp-gcr-ic-r1	1205	169.254.145.225/29	169.254.145.226/29	San Jose (sjc-zone2-6) Partner: Megaport		

Conectividad BGP entre el router del Data Center y el GCR WAN que implementa la interconexión de la nube:

```

MP-IC-US-R1#sh ip ro bgp
...
10.0.0.0/27 is subnetted, 1 subnets
B 10.35.0.0 [20/100] via 169.254.145.225, 01:25:26
MP-IC-US-R1#

```

## Configuración del router SD-WAN Megaport de DC

```

MP-IC-US-R1#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec UPTIME
TRANSITIONS
-----
-----
-----
10.12.1.11 12 up biz-internet public-internet 162.43.150.15 13.55.49.253 12426 ipsec 7 1000 10
4:02:55:32 0
35.35.35.2 35 up biz-internet private2 162.43.150.15 35.212.162.72 12347 ipsec 7 1000 10
4:02:55:32 0
35.35.35.1 35 up biz-internet private2 162.43.150.15 35.212.232.51 12347 ipsec 7 1000 10
4:02:55:32 0
61.61.61.61 61 down biz-internet biz-internet 162.43.150.15 162.43.145.3 12427 ipsec 7 1000 NA 0
61.61.61.61 61 down biz-internet privatel 162.43.150.15 198.18.0.5 12367 ipsec 7 1000 NA 0
35.35.35.1 35 up privatel private2 192.168.9.9 10.35.0.2 12347 ipsec 7 1000 10 0:00:00:16 0
35.35.35.2 35 up privatel private2 192.168.9.9 10.35.0.3 12347 ipsec 7 1000 10 0:00:00:16 0
10.12.1.11 12 down privatel public-internet 192.168.9.9 13.55.49.253 12426 ipsec 7 1000 NA 0
61.61.61.61 61 down privatel biz-internet 192.168.9.9 162.43.145.3 12427 ipsec 7 1000 NA 0

```

61.61.61.61 61 down privatel privatel 192.168.9.9 198.18.0.5 12367 ipsec 7 1000 NA 0

MP-IC-US-R1#sh ip ro bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP  
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
H - NHRP, G - NHRP registered, g - NHRP registration summary  
o - ODR, P - periodic downloaded static route, l - LISP  
a - application route  
+ - replicated route, % - next hop override, p - overrides from PFR  
&- replicated local route overrides by connected

Gateway of last resort is 162.43.150.14 to network 0.0.0.0

10.0.0.0/27 is subnetted, 1 subnets

B 10.35.0.0 [20/100] via 169.254.145.225, 00:03:17

MP-IC-US-R1#

MP-IC-US-R1#sh sdwa

MP-IC-US-R1#sh sdwan runn

MP-IC-US-R1#sh sdwan running-config

system

location "55 South Market Street, San Jose, CA -95113, USA"

gps-location latitude 37.33413

gps-location longitude -121.8916

system-ip 34.34.34.1

overlay-id 1

site-id 34

port-offset 1

control-session-pps 300

admin-tech-on-failure

sp-organization-name MC-Demo-npitaev

organization-name MC-Demo-npitaev

port-hop

track-transport

track-default-gateway

console-baud-rate 19200

no on-demand enable

on-demand idle-timeout 10

vbond 54.188.241.123 port 12346

!

service tcp-keepalives-in

service tcp-keepalives-out

no service tcp-small-servers

no service udp-small-servers

hostname MP-IC-US-R1

username admin privilege 15 secret 9

\$9\$3V6L3V6L2VUI2k\$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo

vrf definition 10

rd 1:10

address-family ipv4

route-target export 64513:10

route-target import 64513:10

exit-address-family

!

address-family ipv6

exit-address-family

!

!

ip arp proxy disable

no ip finger

```
no ip rcmd rcp-enable
no ip rcmd rsh-enable
no ip dhcp use class
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
no shutdown
arp timeout 1200
ip address dhcp client-id GigabitEthernet1
no ip redirects
ip dhcp client default-router distance 1
ip mtu 1500
load-interval 30
mtu 1500
negotiation auto
exit
interface GigabitEthernet1.215
no shutdown
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
no ip redirects
ip mtu 1440
exit
interface Loopback1
no shutdown
ip address 192.168.9.9 255.255.255.255
exit
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet1
no ip redirects
ipv6 unnumbered GigabitEthernet1
no ipv6 redirects
tunnel source GigabitEthernet1
tunnel mode sdwan
exit
interface Tunnel2
no shutdown
ip unnumbered Loopback1
no ip redirects
ipv6 unnumbered Loopback1
no ipv6 redirects
tunnel source Loopback1
tunnel mode sdwan
exit
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
no logging monitor
logging buffered 512000
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
!
router bgp 64513
bgp log-neighbor-changes
neighbor 169.254.145.225 remote-as 16550
neighbor 169.254.145.225 description MP-GCP-SJ-Peering
neighbor 169.254.145.225 ebgp-multihop 4
address-family ipv4 unicast
```

```
neighbor 169.254.145.225 activate
neighbor 169.254.145.225 send-community both
network 192.168.9.9 mask 255.255.255.255
exit-address-family
!
timers bgp 60 180
!
snmp-server ifindex persist
line aux 0
stopbits 1
!
line con 0
speed 19200
stopbits 1
!
line vty 0 4
transport input ssh
!
line vty 5 80
transport input ssh
!
lldp run
nat64 translation timeout tcp 3600
nat64 translation timeout udp 300
sdwan
interface GigabitEthernet1
tunnel-interface
encapsulation ipsec weight 1
no border
color biz-internet
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
hello-tolerance 12
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
interface Loopback1
tunnel-interface
encapsulation ipsec preference 100 weight 1
color privatel
max-control-connections 0
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
```

```
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
appqoe
no tcpopt enable
no dreopt enable
!
omp
no shutdown
send-path-limit 4
ecmp-limit 4
graceful-restart
no as-dot-notation
timers
holdtime 60
advertisement-interval 1
graceful-restart-timer 43200
eor-timer 300
exit
address-family ipv4
advertise bgp
advertise connected
advertise static
!
address-family ipv6
advertise bgp
advertise connected
advertise static
!
!
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
hello-interval 1000
no pmtu-discovery
multiplier 1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
ipsec
rekey 86400
replay-window 512
!
!
sslproxy
no enable
rsa-key-modulus 2048
certificate-lifetime 730
eckey-type P256
ca-tp-label PROXY-SIGNING-CA
settings expired-certificate drop
settings untrusted-certificate drop
```

```
settings unknown-status drop
settings certificate-revocation-check none
settings unsupported-protocol-versions drop
settings unsupported-cipher-suites drop
settings failure-mode close
settings minimum-tls-ver TLSv1
dual-side optimization enable
!
```

```
MP-IC-US-R1#
MP-IC-US-R1#
MP-IC-US-R1#
MP-IC-US-R1#sh run
Building configuration...
```

```
Current configuration : 4628 bytes
!
! Last configuration change at 19:42:11 UTC Tue Jan 25 2022 by admin
!
version 17.6
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname MP-IC-US-R1
!
boot-start-marker
boot-end-marker
!
!
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 64513:10
route-target import 64513:10
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition 65528
!
address-family ipv4
exit-address-family
!
logging buffered 512000
logging persistent size 104857600 filesize 10485760
no logging monitor
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
```

```
!  
!  
!  
aaa server radius dynamic-author  
!  
aaa session-id common  
fhrp version vrrp v3  
ip arp proxy disable  
!  
!  
!  
!  
!  
!  
ip bootp server  
no ip dhcp use class  
!  
!  
no login on-success log  
ipv6 unicast-routing  
!  
!  
!  
!  
!  
!  
subscriber templating  
!  
!  
!  
!  
!  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
crypto pki trustpoint TP-self-signed-1238782368  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-1238782368  
revocation-check none  
rsa-keypair TP-self-signed-1238782368  
!  
crypto pki trustpoint SLA-TrustPoint  
enrollment pkcs12  
revocation-check crl  
!  
!  
crypto pki certificate chain TP-self-signed-1238782368  
crypto pki certificate chain SLA-TrustPoint  
!  
!  
!  
!
```





```
no ipv6 redirects
tunnel source Loopback1
tunnel mode sdwan
!
interface GigabitEthernet1
ip dhcp client default-router distance 1
ip address dhcp client-id GigabitEthernet1
no ip redirects
load-interval 30
negotiation auto
arp timeout 1200
!
interface GigabitEthernet1.215
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
no ip redirects
ip mtu 1440
arp timeout 1200
!
router omp
!
router bgp 64513
bgp log-neighbor-changes
neighbor 169.254.145.225 remote-as 16550
neighbor 169.254.145.225 description MP-GCP-SJ-Peering
neighbor 169.254.145.225 ebgp-multihop 4
!
address-family ipv4
network 192.168.9.9 mask 255.255.255.255
neighbor 169.254.145.225 activate
neighbor 169.254.145.225 send-community both
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat settings central-policy
ip nat route vrf 65528 0.0.0.0 0.0.0.0 global
no ip nat service H225
no ip nat service ras
no ip nat service rtsp udp
no ip nat service rtsp tcp
no ip nat service netbios-ns tcp
no ip nat service netbios-ns udp
no ip nat service netbios-ssn
no ip nat service netbios-dgm
no ip nat service ldap
no ip nat service sunrpc udp
no ip nat service sunrpc tcp
no ip nat service msrpc tcp
no ip nat service tftp
no ip nat service rcmd
no ip nat service pptp
no ip ftp passive
ip scp server enable
!
!
!
!
!
!
!
```

```
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
stopbits 1
speed 19200
line aux 0
line vty 0 4
transport input ssh
line vty 5 80
transport input ssh
!
nat64 translation timeout udp 300
nat64 translation timeout tcp 3600
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
!
!
!
!
!
!
netconf-yang
netconf-yang feature candidate-datastore
end

MP-IC-US-R1#
MP-IC-US-R1#
MP-IC-US-R1#sh ver
Cisco IOS XE Software, Version 17.06.01a
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
17.6.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sat 21-Aug-21 03:20 by mcpre
```

Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.  
All rights reserved. Certain components of Cisco IOS-XE software are  
licensed under the GNU General Public License ("GPL") Version 2.0. The  
software code licensed under GPL Version 2.0 is free software that comes  
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such  
GPL code under the terms of GPL Version 2.0. For more details, see the  
documentation or "License Notice" file accompanying the IOS-XE software,  
or the applicable URL provided on the flyer accompanying the IOS-XE  
software.

ROM: IOS-XE ROMMON

MP-IC-US-R1 uptime is 4 days, 3 hours, 2 minutes  
Uptime for this control processor is 4 days, 3 hours, 3 minutes  
System returned to ROM by reload  
System image file is "bootflash:packages.conf"  
Last reload reason: factory-reset

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Technology Package License Information:  
Controller-managed

The current throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C8000V (VXE) processor (revision VXE) with 2028465K/3075K bytes of memory.  
Processor board ID 9SRWHHH66II  
Router operating mode: Controller-Managed  
1 Gigabit Ethernet interface  
32768K bytes of non-volatile configuration memory.  
3965112K bytes of physical memory.  
11526144K bytes of virtual hard disk at bootflash:.

Configuration register is 0x2102

MP-IC-US-R1#