

Configurazione di Google Cloud Interconnect come trasporto con Cisco SD-WAN in un clic

Sommario

[Introduzione](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Panoramica della progettazione](#)

[Dettagli della soluzione](#)

[Passaggio 1. Preparazione](#)

[Passaggio 2. Creare Cisco Cloud Gateway con Cloud onRamp per flusso di lavoro multicast](#)

[Passaggio 3. Nella console GCP aggiungere una connessione di interconnessione partner](#)

[Passaggio 4. Utilizzare Cloud onRamp Interconnect in Cisco vManage per creare la connessione DC](#)

[Passaggio 5. Configurare il router DC per stabilire i tunnel su Internet e su GCP Cloud Interconnect](#)

[Verifica](#)

[Configurazione router SD-WAN Megaport DC](#)

Introduzione

Questo documento descrive come usare Google [Cloud Interconnect](#) come trasporto SD-WAN (Wide Area Network) definito dal software.

Premesse

I clienti aziendali con carichi di lavoro su Google Cloud Platform (GCP) utilizzano [Cloud Interconnect](#) per la connettività di centri dati o hub. Allo stesso tempo, la connessione Internet pubblica è molto comune nei centri dati e viene utilizzata come base per la connettività SD-WAN con altre postazioni. Questo articolo descrive come GCP Cloud Interconnect può essere usato come underlay per Cisco SD-WAN.

È molto simile a quello che descrive la stessa soluzione per AWS.

Il vantaggio principale dell'uso di GCP Cloud Interconnect come un altro trasporto per Cisco SD-WAN è la possibilità di utilizzare le policy SD-WAN su tutti i trasporti, compresa l'interconnessione cloud GCP. I clienti possono creare policy compatibili con le applicazioni SD-WAN e instradare le applicazioni critiche attraverso l'interconnessione cloud GCP e reindirizzarle tramite Internet pubblico in caso di violazione degli SLA.

Problema

GCP Cloud Interconnect non fornisce funzionalità SD-WAN native. Le domande tipiche dei clienti

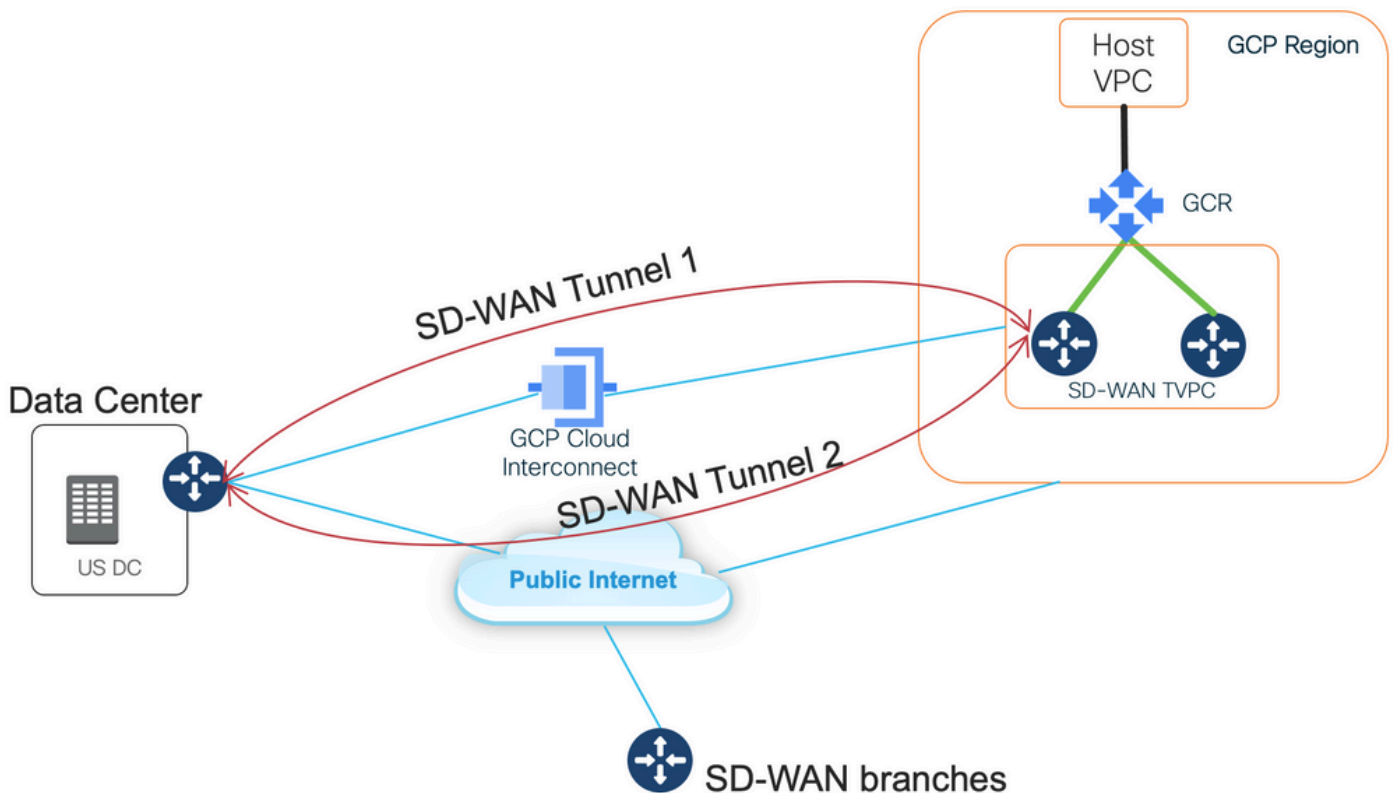
aziendali SD-WAN sono:

- "Posso utilizzare GCP Cloud Interconnect come base per Cisco SD-WAN"?
- "Come posso interconnettere GCP Cloud Interconnect e Cisco SD-WAN"?
- "Come posso creare una soluzione resiliente, sicura e scalabile?"

Soluzione

Panoramica della progettazione

Il punto di progettazione chiave è la connessione del data center tramite GCP Cloud Interconnect ai router SD Cisco creati da Cloud onRamp per il provisioning multicast, come mostrato nell'immagine.



I vantaggi di questa soluzione sono:

- Completamente automatico: Cisco Cloud onRamp per automazione multicolore può essere utilizzato per installare VPC di transito SD-WAN con due router SD-WAN. I VPC host possono essere rilevati come parte di Cloud onRamp e mappati su reti SD-WAN con un solo clic.
- Piena SD-WAN over GCP Cloud Interconnect: GCP Cloud Interconnect è solo un altro trasporto SD-WAN. Tutte le funzioni SD-WAN, come le policy compatibili con le applicazioni, la crittografia, ecc., possono essere utilizzate in modo nativo sul tunnel SD-WAN su GCP Cloud Interconnect.

La scalabilità di questa soluzione si accompagna alle prestazioni di C8000V su GCP. Per ulteriori informazioni sulle prestazioni del server C8000v su GCP, fare riferimento a [SalesConnect](#).

Dettagli della soluzione

Il punto chiave per comprendere questa soluzione è la tecnologia SD-WAN Colors. Notare che i router GCP SD-WAN avranno il **colore privato2** per la connettività Internet, così come la connettività tramite Interconnect, i tunnel SD-WAN saranno formati su Internet utilizzando indirizzi IP pubblici e i tunnel SD-WAN saranno stabiliti (utilizzando la stessa interfaccia) sui circuiti di interconnessione utilizzando indirizzi IP privati a un DC/Sito. Ciò significa che il router del data center (colore biz-internet) stabilirà una connessione ai router GCP SD-WAN (colore private2) via Internet con indirizzi IP pubblici e tramite il suo colore privato su IP privato.

Informazioni generiche sui colori SD-WAN:

I Transport Locator (TLOC) si riferiscono alle interfacce di trasporto WAN (VPN 0) tramite le quali i router SD-WAN si connettono alla rete sottostante. Ogni TLOC viene identificato univocamente tramite una combinazione dell'indirizzo IP di sistema del router SD-WAN, del colore dell'interfaccia WAN e dell'incapsulamento del trasporto (GRE o IPsec). Il protocollo OMP (Cisco Overlay Management Protocol) viene utilizzato per distribuire TLOC (noti anche come route TLOC), prefissi di overlay SD-WAN (noti anche come route OMP) e altre informazioni tra router SD-WAN. È attraverso le route TLOC che i router SD-WAN sanno come raggiungere gli altri router e stabilire i tunnel VPN IPsec tra loro.

I router e/o i controller SD-WAN (vManage, vSmart o vBond) possono essere posizionati dietro i dispositivi NAT (Network Address Translation) all'interno della rete. Quando un router SD-WAN esegue l'autenticazione a un controller vBond, durante lo scambio il controller vBond apprenderà sia l'indirizzo IP privato/numero di porta che l'indirizzo IP pubblico/numero di porta del router SD-WAN. I controller vBond fungono da utility di attraversamento delle sessioni per i server NAT (STUN), consentendo ai router SD-WAN di rilevare gli indirizzi IP e i numeri di porta delle interfacce di trasporto WAN mappati e/o tradotti.

Sui router SD-WAN, ogni trasporto WAN è associato a una coppia di indirizzi IP pubblici e privati. L'indirizzo IP privato viene considerato l'indirizzo precedente al NAT. Questo è l'indirizzo IP assegnato all'interfaccia WAN del router SD-WAN. Sebbene questo sia considerato l'indirizzo IP privato, può essere parte dello spazio di indirizzi IP instradabile pubblicamente o parte dello spazio di indirizzi IP instradabile non pubblicamente dell'IETF RFC 1918. L'indirizzo IP pubblico viene considerato l'indirizzo post-NAT. Questo viene rilevato dal server vBond quando il router SD-WAN inizialmente comunica e si autentica con il server vBond. L'indirizzo IP pubblico può anche far parte dello spazio degli indirizzi IP instradabile pubblicamente o dello spazio degli indirizzi IP non instradabile pubblicamente della RFC 1918 dell'IETF. In assenza di NAT, gli indirizzi IP pubblici e privati dell'interfaccia di trasporto SD-WAN sono gli stessi.

I colori TLOC sono parole chiave definite in modo statico usate per identificare i singoli trasporti WAN su ciascun router SD-WAN. Ogni trasporto WAN su un router SD-WAN specificato deve avere un colore univoco. I colori vengono inoltre utilizzati per identificare un singolo trasporto WAN come pubblico o privato. I colori metro-ethernet, Mpls e private1, private2, private3, private4, private5 e private6 sono considerati colori privati. Sono destinati all'utilizzo in reti private o in luoghi in cui non esiste un NAT. I colori sono 3g, biz-internet, blu, bronzo, custom1, custom2, custom3, default, oro, verde, lte, public-internet, rosso e argento sono considerati colori pubblici. Sono destinati ad essere utilizzati in reti pubbliche o in luoghi con indirizzamento IP pubblico delle interfacce di trasporto WAN, in modo nativo o tramite NAT.

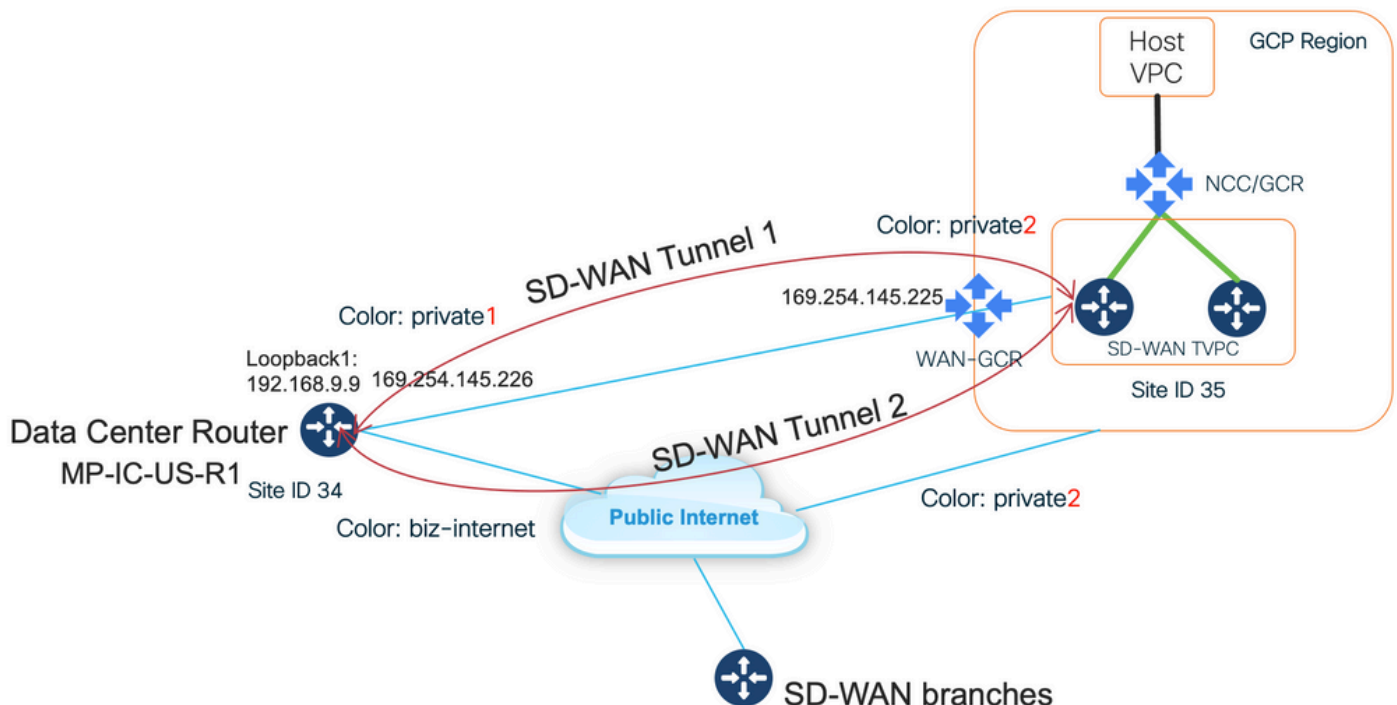
Il colore determina l'uso di indirizzi IP pubblici o privati quando si comunica attraverso i piani dati e di controllo. Quando due router SD-WAN tentano di comunicare tra loro, entrambi utilizzando interfacce di trasporto WAN con colori privati, ciascun lato tenterà di connettersi all'indirizzo IP privato del router remoto. Se uno o entrambi i lati utilizzano colori pubblici, ciascun lato tenterà di connettersi all'indirizzo IP pubblico del router remoto. Un'eccezione a questa regola è costituita dal

fatto che gli ID sito di due dispositivi sono gli stessi. Se gli ID del sito sono uguali, ma i colori sono pubblici, per la comunicazione verranno utilizzati gli indirizzi IP privati. Ciò può verificarsi per i router SD-WAN che tentano di comunicare con un controller vManage o vSmart situato nello stesso sito. Si noti che per impostazione predefinita i router SD-WAN non stabiliscono tunnel VPN IPsec tra loro quando hanno gli stessi ID sito.

Di seguito viene riportato l'output del router del data center, che mostra due tunnel tramite Internet (color biz-internet) e due tunnel tramite GCP Cloud Interconnect (color private1) a due router SD-WAN. Fare riferimento alla configurazione completa del router CC nell'allegato per ulteriori dettagli.

```
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#
```

Questa immagine mostra i dettagli della topologia con gli indirizzi IP e i colori SD-WAN utilizzati per verificare la soluzione.



Software utilizzato:

- Controller SD-WAN con CCO versione 20.7.1.1
- Router per data center simulato con C800v con 17.06.01a con provisioning tramite vManage Cloud onRamp per l'interconnessione con Megaport

- Due router SD-WAN in GCP: C800v con 17.06.01a con provisioning tramite vManage Cloud onRamp per Multicast

Passaggio 1. Preparazione

Verificare che Cisco vManage abbia un account GCP funzionante definito e che le impostazioni globali di Cloud onRamp siano configurate correttamente.

Definire anche un account partner di interconnessione in vManage. In questo blog Megaport è usato come partner di interconnessione, in modo da poter definire un account appropriato e le impostazioni globali.

Passaggio 2. Creare Cisco Cloud Gateway con Cloud onRamp per flusso di lavoro multicast

Si tratta di un processo semplice: selezionare due dispositivi SD-WAN, collegare il modello GCP predefinito, distribuire. Per ulteriori informazioni, fare riferimento a [Cloud onRamp](#) per la [documentazione](#) di [Multicast](#).

Passaggio 3. Nella console GCP aggiungere una connessione di interconnessione partner

Utilizzare il flusso di lavoro di configurazione passo-passo di GCP (**Connettività ibrida > Interconnessione**) per creare una connessione di interconnessione partner con un partner selezionato, nel caso di questo blog - con Megaport come mostrato nell'immagine.

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

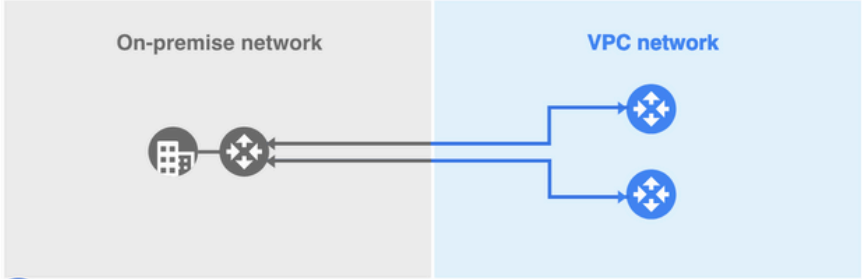
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

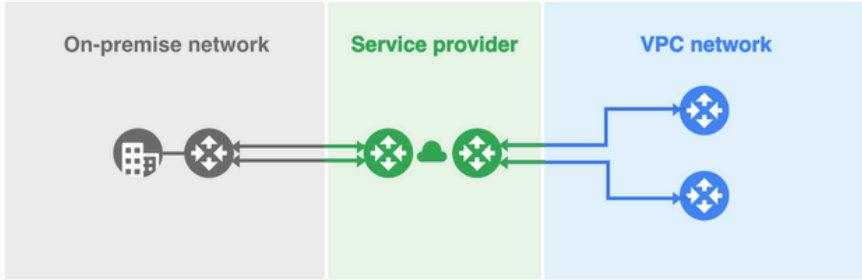
Interconnect type

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 a '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 a 'Service provider' box in the middle. Another green line connects the service provider router to a green router icon in a 'VPC network' on the right. Two blue lines then connect the VPC network router to two blue router icons in the VPC network.

CONTINUE CANCEL

Selezionare l'opzione **SI DISPONE GIÀ DI UN PROVIDER DI SERVIZI**.

Per semplificare la dimostrazione, **creare una singola VLAN** è un'opzione usata senza ridondanza.

Selezionare il nome di rete corretto, precedentemente creato da Cloud onRamp per il flusso di lavoro Multicast. Nella sezione VLAN, è possibile creare un nuovo router GCR e definire un nome per la VLAN, che verrà mostrato in seguito nella sezione Cloud onRamp Interconnect.

Questa immagine riflette tutti i punti menzionati.

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

Network Connectivity Center

← Add Partner VLAN attachment

✓ Check your connection — 2 Add VLAN attachments — 3 Connect to your VPC networks

A VLAN attachment allows you to access your VPC network by adding a VLAN to your existing service provider connection. [Learn more](#)

Redundancy

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). [Learn more about redundancy](#)

Create a redundant pair of VLAN attachments (recommended)

Add a redundant VLAN to an existing VLAN

Create a single VLAN (no redundancy)

Network *
wan-mc-demo-npitaev

Region *
us-west1 (Oregon) ?
Region is permanent

VLAN

Cloud Router *
gcp-gcr-ic-r1 ?

VLAN attachment name *
test-vlan-name ?
Lowercase letters, numbers, hyphens allowed

Description
VLAN for Megaport

Maximum transmission unit (MTU) *
1440

In pratica, una volta completato il passaggio 3., è possibile acquisire semplicemente la configurazione BGP e creare la connettività in base a ciò che il provider di interconnessione ha utilizzato. In questo caso, Megaport viene usata per il test. Tuttavia, è possibile utilizzare qualsiasi tipo di interconnessione che può essere eseguita tramite Megaport, Equinix o MSP.

Passaggio 4. Utilizzare Cloud onRamp Interconnect in Cisco vManage per creare la connessione DC

Come per il blog di AWS, usare il flusso di lavoro Cisco Cloud onRamp Interconnect con Megaport per creare un router per data center e usarlo per l'interconnessione cloud GCP. Si tenga presente che Megaport viene utilizzato solo a scopo di test; se si dispone già di una configurazione per il data center, non è necessario utilizzare Megaport.

In Cisco vManage selezionare un router SD-WAN libero, collegare il modello predefinito CoR Megaport e distribuirlo come Cisco Cloud Gateway in Megaport utilizzando il flusso di lavoro CoR Interconnect.

Quando il router Cisco SD-WAN in Megaport sarà attivo, usare il flusso di lavoro CoR Interconnect per creare una connessione, come mostrato nell'immagine.

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-gcr-ic-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

Passaggio 5. Configurare il router DC per stabilire i tunnel su Internet e su GCP Cloud Interconnect

Mettere il router Megaport SD-WAN in modalità CLI e **spostare** la configurazione dal lato servizio alla VPN0. Poiché GCP usa 169.254.x.y indirizzi IP, è possibile creare l'interfaccia Loopback1 sul router DC e usarla per la comunicazione SD-WAN su GCP Cloud Interconnect.

Ecco le parti interessate della configurazione 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 private1
max-control-connections 0
allow-service all
!

```

Consultare la configurazione completa del router CC nell'ultima sezione del documento.

Verifica

Stato interconnessione cloud GCP:

The screenshot shows the Google Cloud Platform Hybrid Connectivity Interconnect page. The left sidebar contains navigation options: VPN, Interconnect (selected), Cloud Routers, and Network Connectivity Center. The main content area is titled 'Interconnect' and has a 'REFRESH' button. Below the title, there are two tabs: 'VLAN ATTACHMENTS' (active) and 'PHYSICAL CONNECTIONS'. A description states: 'VLAN attachments are connections between your local routers and Google Cloud routers for your Dedicated or Partner Interconnect connections'. There is an 'ADD VLAN ATTACHMENT' button. Below this is a filter input field. A table lists the VLAN attachments with the following columns: Name, Region, Status, Type, Bandwidth, Cloud Router, VLAN ID, Cloud Router IP, On-premises router IP, Interconnect, Des, and Actions.

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		

Connettività BGP tra router del data center e WAN GCR per l'implementazione dell'interconnessione cloud:

```

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#

```

Configurazione router SD-WAN Megaport 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 private1 162.43.150.15 198.18.0.5 12367 ipsec 7 1000 NA 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
10.12.1.11 12 down private1 public-internet 192.168.9.9 13.55.49.253 12426 ipsec 7 1000 NA 0
61.61.61.61 61 down private1 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.

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#