

Configure o Google Cloud Interconnect como um transporte com o Cisco SD-WAN em um clique

Contents

[Introduction](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Visão geral do design](#)

[Detalhes da solução](#)

[Etapa 1. Preparação](#)

[Etapa 2. Crie o Cisco Cloud Gateway com Cloud on Ramp para fluxo de trabalho em multinuvem](#)

[Etapa 3. No console GCP, adicione uma conexão de interconexão de parceiro](#)

[Etapa 4. Use a interconexão Cloud onRamp no Cisco vManage para criar a conexão DC](#)

[Etapa 5. Configurar o roteador DC para estabelecer túneis sobre a Internet e sobre a interconexão de nuvem GCP](#)

[Verificar](#)

[Configuração do roteador DC Megaport SD-WAN](#)

Introduction

Este documento descreve como usar o Google [Cloud Interconnect](#) como transporte de rede de longa distância definida por software (SD-WAN).

Informações de Apoio

Clientes corporativos com cargas de trabalho na plataforma Google Cloud (GCP) usam a [interconexão de nuvem](#) para conectividade de data center ou hub. Ao mesmo tempo, a conexão pública com a Internet também é muito comum no data center e é usada como uma base para a conectividade SD-WAN com outros locais. Este artigo descreve como a interconexão de nuvem GCP pode ser usada como uma base para o Cisco SD-WAN.

É muito semelhante à que descreve a mesma solução para AWS.

O principal benefício de usar a interconexão de nuvem GCP como apenas outro transporte para a Cisco SD-WAN é a capacidade de usar políticas de SD-WAN em todos os transportes, incluindo a interconexão de nuvem GCP. Os clientes podem criar políticas com reconhecimento de aplicativos SD-WAN e rotear aplicativos críticos através da interconexão de nuvem GCP e redirecionar via Internet pública em caso de violações de SLA.

Problema

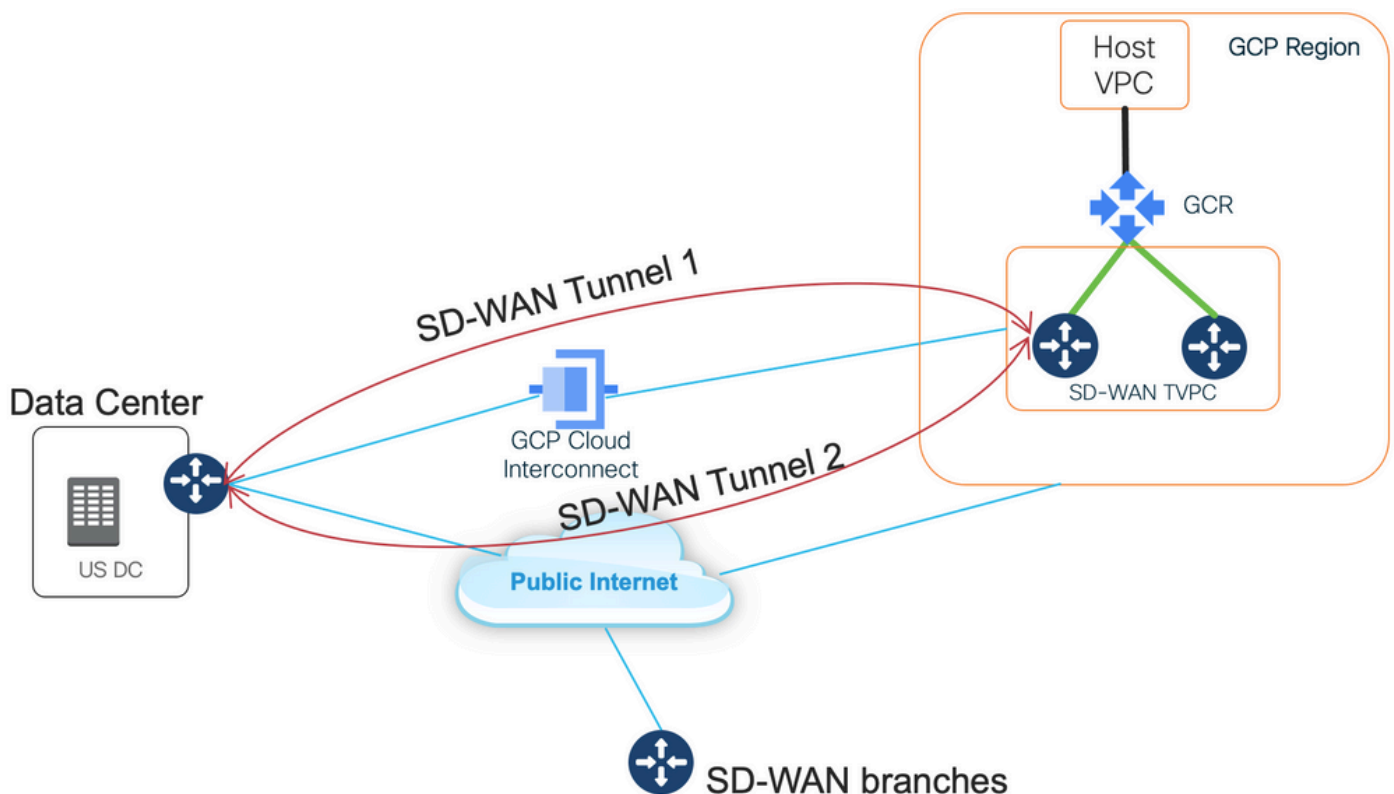
O GCP Cloud Interconnect não fornece recursos nativos de SD-WAN. As perguntas típicas dos clientes Enterprise SD-WAN são:

- "Posso usar a interconexão de nuvem GCP como uma base para o Cisco SD-WAN"?
- "Como posso interconectar o GCP Cloud Interconnect e o Cisco SD-WAN"?
- "Como posso criar uma solução resiliente, segura e escalável?"

Solução

Visão geral do design

O ponto-chave do projeto é a conexão do data center por meio da interconexão de nuvem GCP com os roteadores SD da Cisco criados pela nuvem em rack para provisionamento de multinuvem, como mostrado na imagem.



Os benefícios dessa solução são:

- **Totalmente automático:** A automação do Cisco Cloud onRamp para Multicloud pode ser usada para implantar VPC de trânsito SD-WAN com dois roteadores SD-WAN. Os VPCs de host podem ser descobertos como parte da nuvem naRamp e mapeados para redes SD-WAN com um clique.
- **Interconexão de nuvem SD-WAN sobre GCP completa:** O GCP Cloud Interconnect é apenas outro transporte SD-WAN. Todos os recursos SD-WAN, como políticas com reconhecimento de aplicativos, criptografia etc., podem ser usados nativamente no túnel SD-WAN sobre a interconexão de nuvem GCP.

Observe que a escalabilidade dessa solução acompanha o desempenho do C8000V em GCP. Consulte o [SalesConnect](#) para obter detalhes sobre o desempenho do C8000v em GCP.

Detalhes da solução

O ponto principal para entender essa solução são as cores SD-WAN. Observe que os roteadores

GCP SD-WAN terão **cor privada privada2** para a conectividade com a Internet, bem como conectividade via Interconnect, túneis SD-WAN serão formados pela Internet usando endereços IP públicos e túneis SD-WAN serão estabelecidos (usando a mesma interface) sobre os circuitos de interconexão usando endereços IP privados para um DC/Site. Isso significa que o roteador do data center (cor biz-internet) estabelecerá uma conexão com os roteadores GCP SD-WAN (cor privada2) via Internet com endereços IP públicos e via sua cor Privada sobre IP Privado.

Informações genéricas sobre as cores SD-WAN:

Os localizadores de transporte (TLOCs) se referem às interfaces de transporte de WAN (VPN 0) pelas quais os roteadores SD-WAN se conectam à rede de base. Cada TLOC é identificado exclusivamente por meio de uma combinação do endereço IP do sistema do roteador SD-WAN, da cor da interface WAN e do encapsulamento de transporte (GRE ou IPsec). O Cisco Overlay Management Protocol (OMP) é usado para distribuir TLOCs (também conhecidos como rotas TLOC), prefixos de sobreposição SD-WAN (também conhecidos como rotas OMP) e outras informações entre roteadores SD-WAN. É através de rotas TLOC que os roteadores SD-WAN sabem como alcançar um ao outro e estabelecer túneis VPN IPsec entre si.

Os roteadores e/ou controladores SD-WAN (vManage, vSmart ou vBond) podem ficar atrás dos dispositivos de Network Address Translation (NAT) dentro da rede. Quando um roteador SD-WAN se autentica em um controlador vBond, o controlador vBond aprenderá as configurações de endereço IP/número de porta privada e de endereço IP/número de porta público do roteador SD-WAN durante a troca. Os controladores vBond atuam como utilitários de passagem de sessão para servidores NAT (STUN), permitindo que os roteadores SD-WAN descubram endereços IP mapeados e/ou traduzidos e números de porta de suas interfaces de transporte de WAN.

Nos roteadores SD-WAN, cada transporte de WAN é associado a um par de endereços IP públicos e privados. O endereço IP privado é considerado o endereço pré-NAT. Esse é o endereço IP atribuído à interface WAN do roteador SD-WAN. Embora esse seja considerado o endereço IP privado, esse endereço IP pode ser parte do espaço de endereço IP roteável publicamente ou parte do espaço de endereço IP não roteável publicamente RFC 1918 da IETF. O endereço IP público é considerado o endereço pós-NAT. Isso é detectado pelo servidor vBond quando o roteador SD-WAN inicialmente se comunica e autentica com o servidor vBond. O endereço IP público também pode ser parte do espaço de endereço IP roteável publicamente ou parte do espaço de endereço IP não roteável publicamente RFC 1918 da IETF. Na ausência de NAT, os endereços IP públicos e privados da interface de transporte SD-WAN são os mesmos.

As cores da TLOC são palavras-chave definidas estaticamente usadas para identificar transportes individuais de WAN em cada roteador SD-WAN. Cada transporte de WAN em um determinado roteador SD-WAN deve ter uma cor exclusiva. As cores também são usadas para identificar um transporte de WAN individual como público ou privado. As cores metro-ethernet, Mpls e private1, private2, private3, private4, private5 e private6 são consideradas cores privadas. Eles são destinados ao uso em redes privadas ou em locais onde não há NAT. As cores são 3g, biz-internet, azul, bronze, personalizado1, personalizado2, personalizado3, padrão, ouro, verde, lte, público-internet, vermelho e prata são consideradas cores públicas. Eles devem ser usados em redes públicas ou em locais com endereçamento IP público das interfaces de transporte da WAN, seja nativamente ou através de NAT.

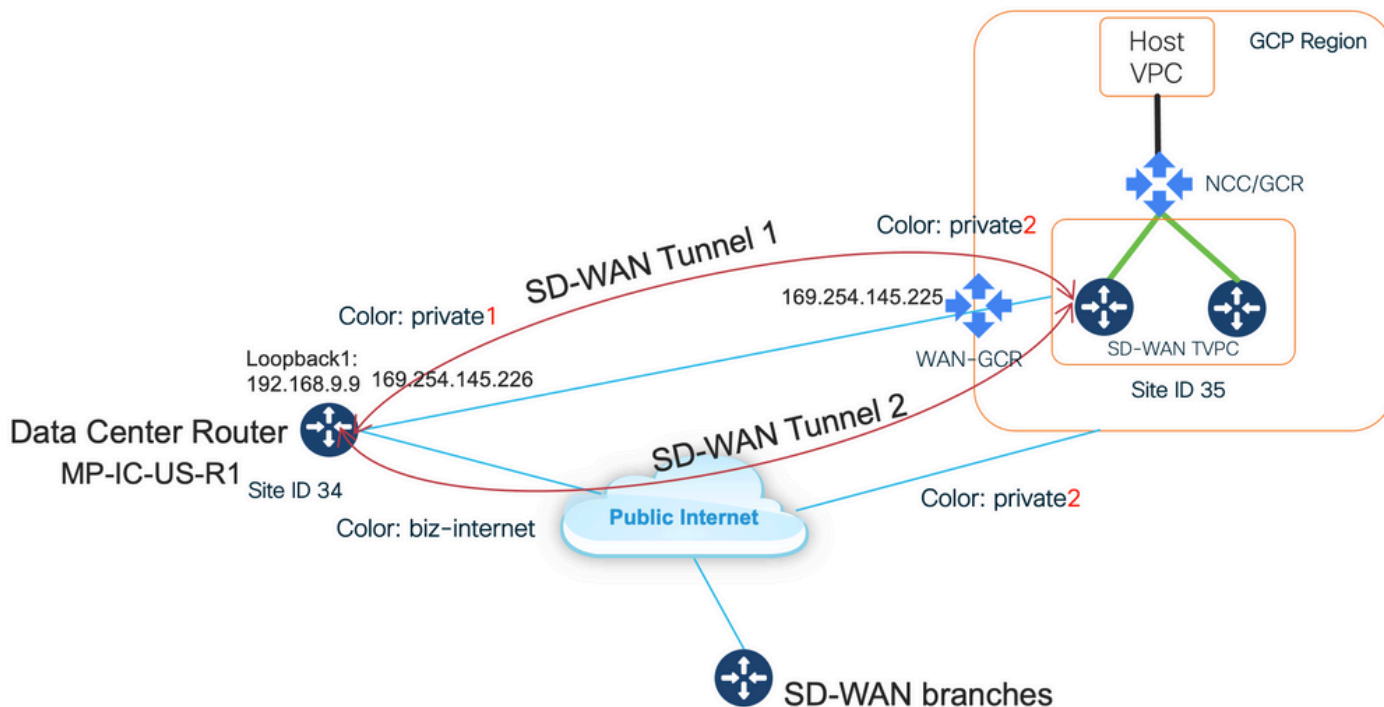
A cor determina o uso de endereços IP públicos ou privados ao se comunicar através dos planos de controle e de dados. Quando dois roteadores SD-WAN tentam se comunicar entre si, usando interfaces de transporte WAN com cores privadas, cada lado tentará se conectar ao endereço IP privado do roteador remoto. Se um ou ambos os lados estiverem usando cores públicas, cada lado tentará se conectar ao endereço IP público do roteador remoto. Uma exceção a isso é

quando as IDs de site de dois dispositivos são iguais. Quando as IDs do site são iguais, mas as cores são públicas, os endereços IP privados serão usados para comunicação. Isso pode ocorrer para roteadores SD-WAN que tentam se comunicar com um controlador vManage ou vSmart localizado no mesmo local. Observe que os roteadores SD-WAN não estabelecem, por padrão, túneis VPN IPsec entre si quando têm as mesmas IDs de site.

Aqui está a saída do roteador do data center, que mostra dois túneis através da Internet (Internet corporativa colorida) e dois túneis através da Interconexão de nuvem GCP (privada1 colorida) para dois roteadores SD-WAN. Consulte a configuração completa do roteador DC no anexo para obter mais detalhes.

```
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 privatel1 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 privatel1 private2 192.168.9.9 10.35.0.3 12347 ipsec 7 1000 10 0:00:00:16 0
...
MP-IC-US-R1#
```

Esta imagem ilustra os detalhes da topologia com endereços IP e cores SD-WAN, que são usados para verificar a solução.



Software usado:

- Controladores SD-WAN executando o CCO versão 20.7.1.1
- Roteador de data center simulado com C8000v executando 17.06.01a provisionado via vManage Cloud onRamp para interconexão com Megaport

- Dois roteadores SD-WAN no GCP: C8000v executando 17.06.01a provisionado via vManage Cloud onRamp para Multicloud

Etapa 1. Preparação

Certifique-se de que o Cisco vManage tenha uma conta GCP em funcionamento definida e que as configurações globais do Cloud onRamp estejam configuradas corretamente.

Defina também uma conta de parceiro de interconexão no vManage. Neste blog, o Megaport é usado como parceiro de interconexão, para que você possa definir uma conta apropriada e configurações globais.

Etapa 2. Crie o Cisco Cloud Gateway com Cloud on Ramp para fluxo de trabalho em multivem

Este é um processo direto: selecione dois dispositivos SD-WAN, anexe o modelo GCP padrão e implante. Consulte a [documentação Cloud onRamp for Multicloud](#) para obter detalhes.

Etapa 3. No console GCP, adicione uma conexão de interconexão de parceiro

Use o fluxo de trabalho de configuração passo a passo (**Hybrid Connectivity > Interconnect**) do GCP para criar uma conexão de interconexão de parceiros com um parceiro selecionado, no caso deste blog - com Megaport, como mostrado na imagem.

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

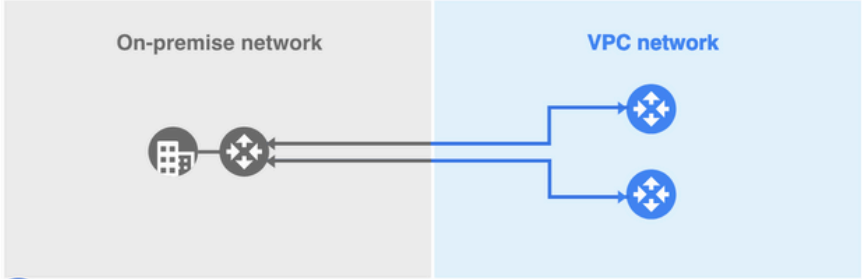
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

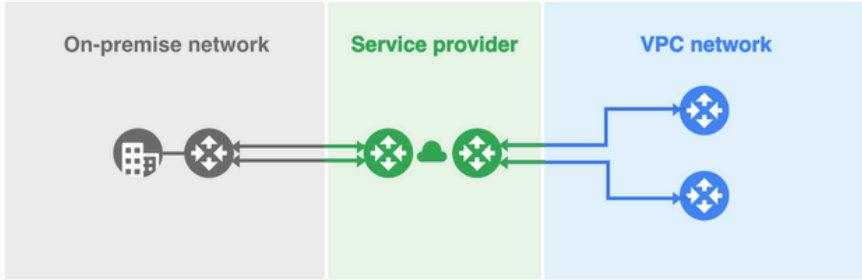
Interconnect type

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 icon and a router icon. Two blue lines representing fiber connections extend from the router to a 'VPC network' on the right, which contains two blue router icons.

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 icon and a router icon. A green line connects the router to a 'Service provider' in the middle, which contains two green router icons and a cloud icon. From the service provider, two blue lines connect to a 'VPC network' on the right, which contains two blue router icons.

CONTINUE CANCEL

Selecione a opção **JÁ TENHO UM PROVEDOR DE SERVIÇOS**.

Para facilitar a demonstração, **Crie uma única opção de VLAN** é usada sem redundância.

Selecione o nome de rede correto, que foi criado anteriormente pelo Cloud onRamp para o fluxo de trabalho da Multicloud. Na seção VLAN, você pode criar um novo roteador GCR e definir um nome para a VLAN, que será mostrado posteriormente na seção Interconexão de nuvem em rampa.

Essa imagem reflete todos os pontos mencionados.

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

Basicamente, uma vez na Etapa 3. for concluída, você pode simplesmente agarrar a configuração do BGP e fazer a conectividade com base no que o provedor de interconexão usou. Nesse caso, a Megaport é usada para testar. No entanto, você pode usar qualquer tipo de interconexão que pode ser via Megaport, Equinix ou MSP.

Etapa 4. Use a interconexão Cloud onRamp no Cisco vManage para criar a conexão DC

Semelhante ao Blog AWS, use o fluxo de trabalho do Cisco Cloud onRamp Interconnect com a Megaport para criar um roteador de data center e usá-lo para o GCP Cloud Interconnect. Observe que a Megaport é usada aqui apenas para fins de teste. Se você já tiver uma configuração de data center, não há necessidade de usar a Megaport.

No Cisco vManage, selecione um roteador SD-WAN gratuito, anexe o modelo CoR Megaport padrão e implante-o como Cisco Cloud Gateway em Megaport usando o fluxo de trabalho de interconexão de CoR.

Quando o roteador Cisco SD-WAN em Megaport estiver ativo, use o fluxo de trabalho de interconexão de CoR para criar uma conexão como mostrado na imagem.

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

Etapa 5. Configurar o roteador DC para estabelecer túneis sobre a Internet e sobre a interconexão de nuvem GCP

Traga o roteador SD-WAN Megaport para o modo CLI e **mova** a configuração do lado do serviço para VPN0. Como o GCP usa endereços IP 169.254.x.y, você pode criar a Interface Loopback1 no roteador DC e usá-la para comunicação SD-WAN sobre interconexão de nuvem GCP.

Aqui estão as partes relevantes da configuração do roteador 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 a configuração completa do roteador DC na última seção do documento.

Verificar

Status da interconexão de nuvem 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'. 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		

Conectividade BGP entre o roteador de data center e o GCR da WAN implementando a interconexão de nuvem:

```

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#

```

Configuração do roteador DC Megaport SD-WAN

```

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 tcptopt 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#