

Google Cloud Interconnect als een transport met Cisco SD-WAN in een klik configureren

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Overzicht van ontwerpen](#)

[Details oplossing](#)

[Stap 1. Voorbereiding](#)

[Stap 2. Maak Cisco Cloud Gateway met Cloud onRamp voor Multicloud](#)

[Stap 3. In GCP-console Voeg een partner-interconnect verbinding toe](#)

[Stap 4. Gebruik Cloud onRamp Interconnect in Cisco vManager om de DC-verbinding te maken](#)

[Stap 5. Configuratie van DC-router om tunnels via internet en via GCP Cloud Interconnect in te stellen](#)

[Verifiëren](#)

[Configuratie van DC-Megaport SD-WAN router](#)

Inleiding

Dit document beschrijft hoe u Google [Cloud Interconnect](#) kunt gebruiken als softwaregedefinieerde Wide Area Network (SD-WAN) transport.

Achtergrondinformatie

Enterprise-klienten met werkloads op Google Cloud Platform (GCP) gebruiken [Cloud Interconnect](#) voor datacenter of hubconnectiviteit. Tegelijkertijd is de openbare internetverbinding ook heel gebruikelijk in het datacenter en wordt deze gebruikt als basis voor SD-WAN connectiviteit met andere locaties. Dit artikel beschrijft hoe GCP Cloud Interconnect kan worden gebruikt als basis voor Cisco SD-WAN.

Het lijkt sterk op dat wat dezelfde oplossing voor AWS beschrijft.

Het belangrijkste voordeel van het gebruik van GCP Cloud Interconnect als gewoon een ander transport voor Cisco SD-WAN is de mogelijkheid om SD-WAN beleid te gebruiken voor alle transport inclusief GCP Cloud Interconnect. Klanten kunnen SD-WAN toepassingsgericht beleid maken en cruciale toepassingen routeren via GCP Cloud Interconnect en eroute via het openbare internet in geval van SLA-schendingen.

Probleem

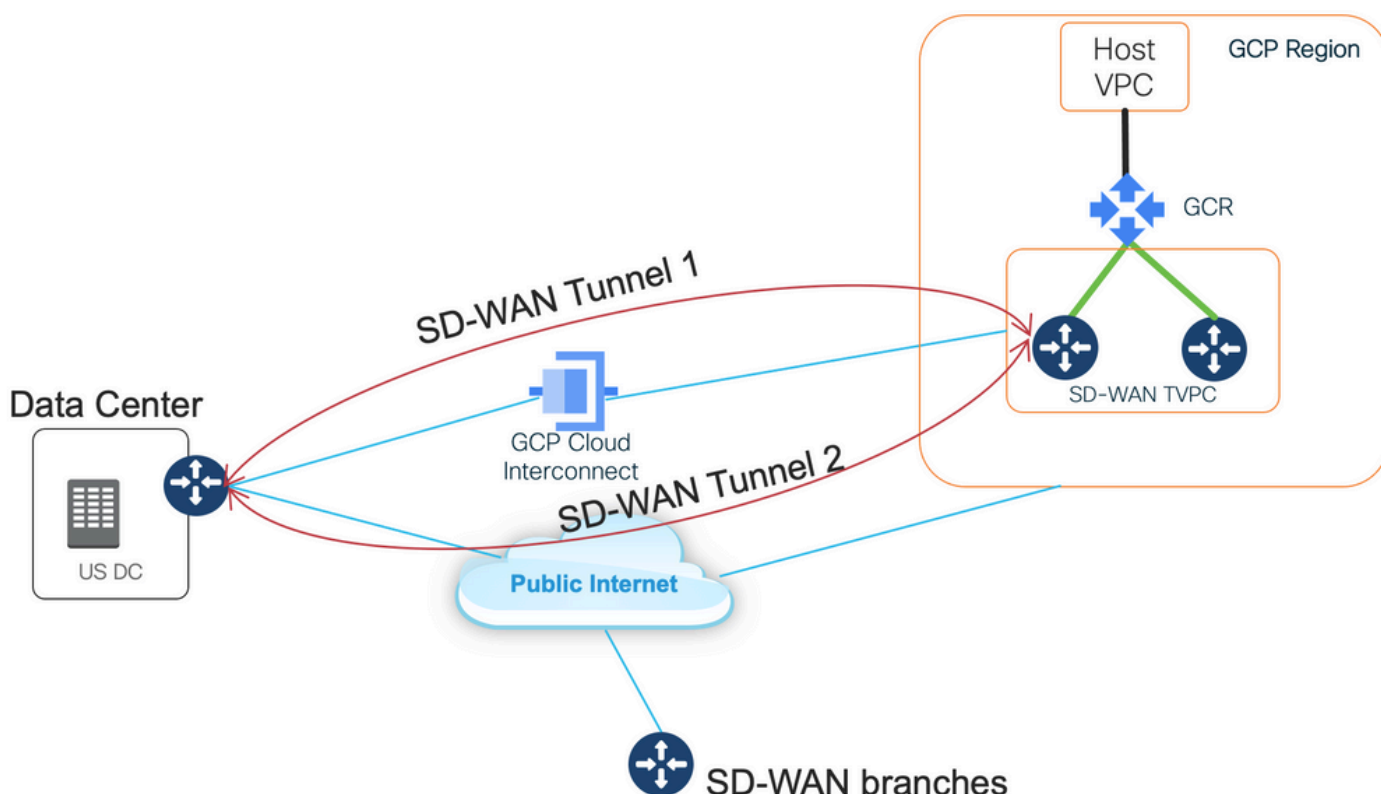
GCP Cloud Interconnect biedt geen native SD-WAN mogelijkheden. Typische vragen van ondernemingen SD-WAN klanten zijn:

- "Kan ik GCP Cloud Interconnect als basis gebruiken voor Cisco SD-WAN"?
- "Hoe kan ik GCP Cloud Interconnect en Cisco SD-WAN onderling verbinden"?
- "Hoe kan ik een veerkrachtige, veilige en schaalbare oplossing creëren"?

Oplossing

Overzicht van ontwerpen

Het belangrijkste ontwerppunt is de verbinding van het datacenter via GCP Cloud Interconnect met Cisco SD-routers die door Cloud onRamp zijn gemaakt voor multicast levering zoals in de afbeelding wordt getoond.



De voordelen van deze oplossing zijn:

- Volledig automatisch: Cisco Cloud onRamp voor multicast automatisering kan worden gebruikt om SD-WAN doorvoerVPC met twee SD-WAN routers in te zetten. VPC's op host kunnen worden ontdekt als deel van Cloud onRamp en met één klik worden toegewezen aan SD-WAN netwerken.
- Full SD-WAN via GCP Cloud Interconnect: GCP Cloud Interconnect is gewoon een ander SD-WAN transport. Alle SD-WAN functies zoals toepassingsbewust beleid, encryptie, enz. kunnen ook anders worden gebruikt in de SD-WAN tunnel via GCP Cloud Interconnect.

Houd er rekening mee dat de schaalbaarheid van deze oplossing overeenkomt met de prestaties van C8000V op de GCP. Raadpleeg [SalesConnect](#) voor meer informatie over de C8000v-prestaties op GCP.

Details oplossing

Het belangrijkste punt om deze oplossing te begrijpen is SD-WAN Kleuren. Merk op dat GCP SD-

WAN routers **privé-kleur** zullen hebben² voor de internetconnectiviteit en connectiviteit via Interconnect, SD-WAN-tunnels via het internet zullen worden gevormd via het internet met openbare IP-adressen en SD-WAN-tunnels zullen worden gerealiseerd (dezelfde interface gebruiken) via de interconnect-circuits met privé IP-adressen naar een DC/Site. Dit betekent dat de router van het datacenter (biz-internet kleur) een verbinding met GCP SD-WAN routers (private²-kleur) via het internet zal opzetten met openbare IP-adressen en via zijn privé-kleur via Private IP.

Algemene informatie over SD-WAN kleuren:

Transport Locators (TLOCs) verwijzen naar de WAN-transport (VPN 0) interfaces waardoor SD-WAN routers verbinding maken met het basisnetwerk. Elke TLOC wordt uniek geïdentificeerd door een combinatie van het systeem IP-adres van de SD-WAN router, de kleur van de WAN-interface en de transportinsluiting (GRE of IPsec). Cisco Overlay Management Protocol (OMP) wordt gebruikt om TLOCs (ook bekend als TLOC-routes), SD-WAN overlay prefixes (ook bekend als OMP-routes) en andere informatie tussen SD-WAN routers te distribueren. Het is via TLOC-routes dat SD-WAN routers elkaar weten te bereiken en IPsec VPN-tunnels met elkaar inrichten.

SD-WAN routers en/of controllers (vManager, vSmart of vBond) kunnen achter NAT-apparaten voor netwerkadresomzetting (NAT) in het netwerk zitten. Wanneer een SD-WAN router voor verificatie naar een vBond-controller zorgt, zal de vBond-controller tijdens de uitwisseling zowel het privé IP-adres/poortnummer als de openbare IP-adres/poortinstellingen van de SD-WAN router leren. vBond controllers fungeren als Session Traversal Utilities voor NAT (STUN) servers, waardoor SD-WAN routers in staat zijn ingedeelde en/of vertaalde IP-adressen en poortnummers van hun WAN-transportinterfaces te ontdekken.

Op SD-WAN routers wordt elk WAN-transport gekoppeld aan een openbaar en privé IP-adrespaar. Het particuliere IP-adres wordt beschouwd als het pre-NAT-adres. Dit is IP-adres dat is toegewezen aan de WAN-interface van de SD-WAN router. Hoewel dit als het privé IP-adres wordt beschouwd, kan dit IP-adres ofwel een deel van de openbare routeerbare IP-adresruimte of een deel van de IETF RFC 1918 niet-publiekelijk routeerbare IP-adresruimte zijn. Het openbare IP-adres wordt beschouwd als het post-NAT-adres. Dit wordt gedetecteerd door de vBond server wanneer de SD-WAN router aanvankelijk communiceert en authentiek verklaard met de vBond server. Het openbare IP-adres kan ook een deel van de publiekelijk routeerbare IP-adresruimte of een deel van de IETF RFC 1918 niet-publiekelijk routeerbare IP-adresruimte zijn. Bij gebrek aan NAT zijn zowel de openbare als de particuliere IP-adressen van de SD-WAN transportinterface hetzelfde.

De kleuren van TLOC zijn statistisch gedefinieerde sleutelwoorden die gebruikt worden om individuele WAN-transporten op elke SD-WAN router te identificeren. Elk WAN-transport op een bepaalde SD-WAN router moet een unieke kleur hebben. Kleuren worden ook gebruikt om een individueel WAN-transport aan te duiden als publiek of privaat. De kleuren metro-Ethernet, Mpls, en privé¹, private², private³, private⁴, private⁵, en private⁶ worden beschouwd als privé kleuren. Ze zijn bedoeld voor gebruik op particuliere netwerken of plaatsen waar geen NAT is. De kleuren zijn 3g, biz-internet, blauw, bronze, op maat¹, op maat², op maat³, standaard, goud, groen, lte, publiek-internet, rood en zilver worden gezien als openbare kleuren. Ze zijn bedoeld om te worden gebruikt op openbare netwerken of op plaatsen met openbare IP-adressering van de WAN-transportinterfaces, hetzij op nationaal niveau, hetzij via NAT.

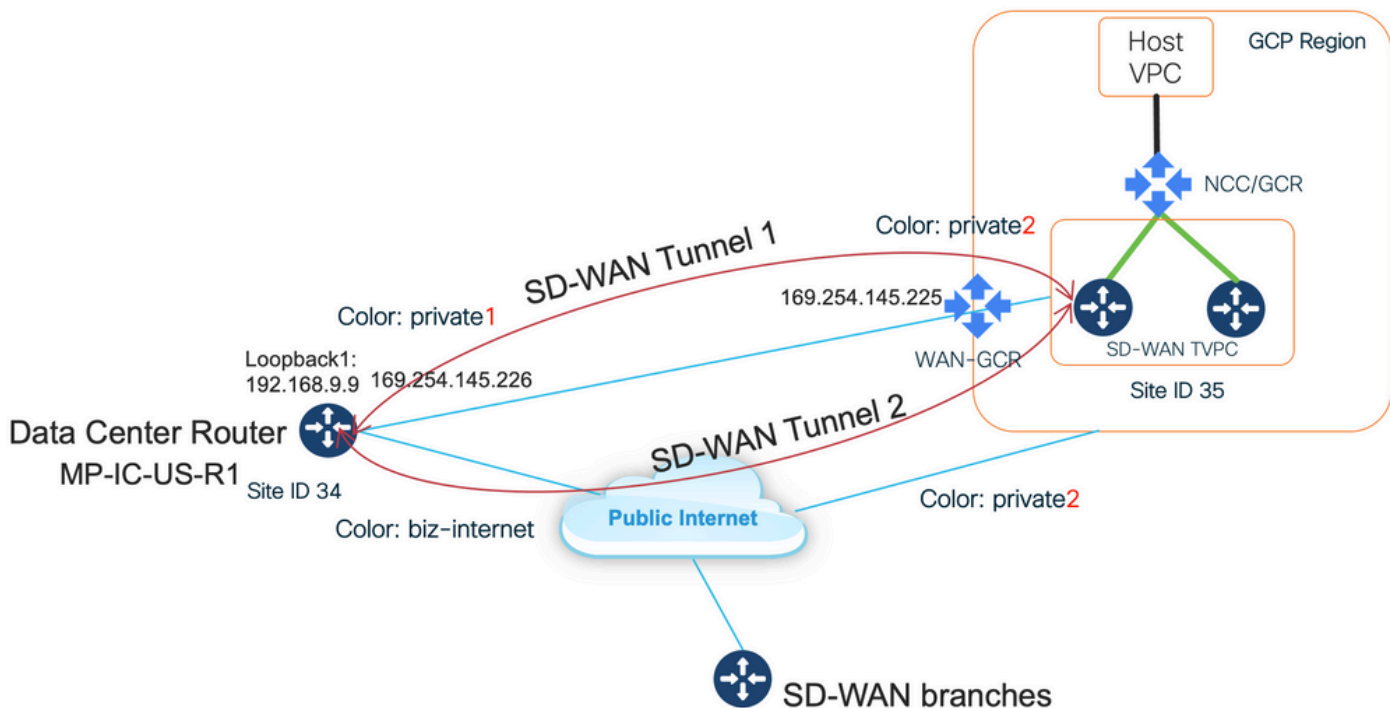
De kleur dicteert het gebruik van of privé of openbare IP adressen wanneer het door de controle en gegevensvliegtuigen communiceert. Wanneer twee SD-WAN routers met elkaar proberen te communiceren, allebei WAN-transportinterfaces met privé-kleuren gebruiken, zal elke kant proberen verbinding te maken met het privé IP-adres van de externe router. Als één of beide

partijen openbare kleuren gebruiken, zal elke kant proberen om aan te sluiten op het openbare IP-adres van de afstandsrouter. Een uitzondering hierop is wanneer de site-ID's van twee apparaten hetzelfde zijn. Wanneer de Site ID's hetzelfde zijn maar de kleuren publiek zijn, dan worden de privé IP-adressen gebruikt voor communicatie. Dit kan voorkomen voor SD-WAN routers die proberen te communiceren met een vManager of vSmart controller op dezelfde locatie. Merk op dat SD-WAN routers standaard geen IPsec VPN-tunnels tussen elkaar realiseren wanneer ze dezelfde Site-ID's hebben.

Hier is de uitvoer van de router van het datacenter, die twee tunnels via internet (gekleurd biz-internet) en twee tunnels via GCP Cloud Interconnect (gekleurd privé1) toont aan twee SD-WAN routers. Raadpleeg de volledige DC-routerconfiguratie in de bijlage voor meer informatie.

```
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#
```

Dit beeld illustreert topologiedetails met IP adressen en SD-WAN kleuren, die worden gebruikt om de oplossing te verifiëren.



Gebruikte software:

- SD-WAN controllers voor gebruik van CCO versie 20.7.1.1
- Datacenterrouter gesimuleerd met C8000v die 17.06.01a draait en via vManager Cloud

onRamp wordt geprovisioneerd voor interconnect met Megaport

- Twee SD-WAN routers in GCP: C8000v-versie met 17.06.01a, provisioneerd via vManager Cloud onRamp voor multicast

Stap 1. Voorbereiding

Zorg ervoor dat Cisco vManager een werkende GCP-account heeft gedefinieerd en dat Cloud onRamp Global Settings correct worden ingesteld.

Maak ook een Interconnect-partneraccount in vManager. In deze blog Megaport wordt gebruikt als Interconnect-partner, zodat u een geschikt account- en wereldwijde instellingen kunt definiëren.

Stap 2. Maak Cisco Cloud Gateway met Cloud onRamp voor Multicloud

Dit is een eenvoudig proces: Selecteer twee SD-WAN apparaten, bevestig de standaard GCP-sjabloon en stel in. Raadpleeg [Cloud onRamp voor](#) meer informatie [over](#) Cloud-documentatie.

Stap 3. In GCP-console Voeg een partner-interconnect verbinding toe

Gebruik GCP stap-voor-stap configuratie werkschema (**Hybrid Connectivity > Interconnect**) om een partner interconnect verbinding te maken met een geselecteerde partner, in het geval van deze blog - met Megaport zoals in de afbeelding getoond.

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

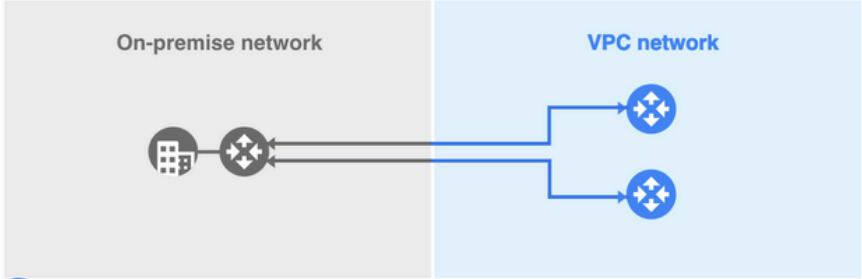
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

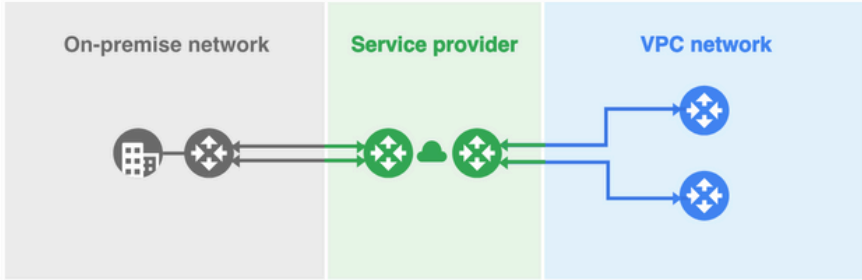
Interconnect type

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. From the service provider, two blue lines connect to a 'VPC network' on the right, which contains two blue router icons.

CONTINUE CANCEL

Selecteer de optie **DIE IK REEDS EEN SERVICEPROVIDER HEB**.

Voor gemak van demonstratie, **creëert u één VLAN**-optie zonder redundantie.

Selecteer de juiste netwerknnaam, die eerder door Cloud onRamp werd gemaakt voor Cloud Cloud onRamp voor MulticCloud. Onder de sectie VLAN kunt u een nieuwe GCR-router maken en een naam voor het VLAN definiëren, die later in de sectie Cloud onRamp Interconnect zal worden weergegeven.

Deze afbeelding weerspiegelt alle genoemde punten.

Hybrid Connectivity	← Add Partner VLAN attachment
VPN	✓ Check your connection — 2 Add VLAN attachments — 3 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. Learn more</p>
Cloud Routers	<p>Redundancy</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). Learn more about redundancy</p>
Network Connectivity Center	<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) ?</p> <p>Region is permanent</p>	
<p>VLAN</p>	
<p>Cloud Router * gcp-gcr-ic-r1 ?</p>	
<p>VLAN attachment name * test-vlan-name ?</p> <p>Lowercase letters, numbers, hyphens allowed</p>	
<p>Description VLAN for Megaport</p>	
<p>Maximum transmission unit (MTU) * 1440</p>	

Na voltooiing van Stap 3 kunt u eenvoudig de BGP-configuratie grijpen en de connectiviteit maken op basis van wat de Interconnect-provider heeft gebruikt. In dit geval wordt Megaport gebruikt om te testen. U kunt echter elk type onderlinge verbinding gebruiken dat via Megaport, Equinix of een MSP kan worden gegenereerd.

Stap 4. Gebruik Cloud onRamp Interconnect in Cisco vManager om de DC-verbinding te maken

Overeenkomstig met het AWS-blog dient u het Cisco Cloud onRamp Interconnect-werkschema met Megaport te gebruiken om een datacenter-router te maken en het te gebruiken voor GCP Cloud Interconnect. Houd er rekening mee dat Megaport hier alleen voor testdoeleinden wordt gebruikt. Als u al een installatie voor datacenters hebt, hoeft u Megaport niet te gebruiken.

In Cisco vManager selecteert u één vrije SD-WAN router en voegt u de standaardjabloon van het CoR-type toe en implementeert u deze als Cisco Cloud Gateway in Megaport met behulp van CoR Interconnect-werkstromen.

Zodra de Cisco SD-WAN router in Megaport actief is, gebruikt u de CoR Interconnect-oplossing om een verbinding te maken zoals in de afbeelding wordt weergegeven.

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-ripitsev
 Redundancy: Disable
 Google Cloud Interconnect Attachment: us-west1:gcp-gw-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

Step 5. Configuratie van DC-router om tunnels via internet en via GCP Cloud Interconnect in te stellen

Breng SD-WAN Megaport router naar CLI-modus en **verplaats** de configuratie van de serviceskant naar VPN0. Omdat GCP 169.254.x.y IP-adressen gebruikt, kunt u Loopback1-interface op de DC-router maken en gebruiken voor SD-WAN-communicatie via GCP Cloud Interconnect.

Hier zijn de relevante onderdelen van de DC-routerconfiguratie.

```
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
!

```

Raadpleeg de volledige DC-routerconfiguratie in het laatste gedeelte van het document.

Verifiëren

GCP Cloud Interconnect-status:

BGP-connectiviteit tussen datacenterrouter en WAN GCR voor implementatie van Cloud Interconnect:

```

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#

```

Configuratie van DC-Megaport SD-WAN router

```

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.

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#