

Konfigurieren von Google Cloud Interconnect als Transport mit Cisco SD-WAN per Mausklick

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

[Übersicht über das Design](#)

[Lösungsdetails](#)

[Schritt 1: Vorbereitung](#)

[Schritt 2: Erstellen eines Cisco Cloud Gateway mit Cloud onRamp für Multicloud-Workflows](#)

[Schritt 3: Fügen Sie in der GCP-Konsole eine Partner Interconnect-Verbindung hinzu.](#)

[Schritt 4: Verwenden von Cloud onRamp Interconnect in Cisco vManage zum Erstellen der DC-Verbindung](#)

[Schritt 5: Konfigurieren des RZ-Routers zum Einrichten von Tunneln über das Internet und über GCP Cloud Interconnect](#)

[Überprüfung](#)

[SD-WAN-Router-Konfiguration für DC-Megaport](#)

Einleitung

Dieses Dokument beschreibt die Verwendung von Google [Cloud Interconnect](#) als Software-Defined Wide Area Network (SD-WAN)-Transport.

Hintergrundinformationen

Enterprise-Kunden mit Workloads auf der Google Cloud-Plattform (GCP) verwenden [Cloud Interconnect](#) für Rechenzentrums- oder Hub-Verbindungen. Gleichzeitig ist die öffentliche Internetverbindung auch im Rechenzentrum sehr verbreitet und dient als Basis für SD-WAN-Verbindungen mit anderen Standorten. In diesem Artikel wird beschrieben, wie GCP Cloud Interconnect als Basis für Cisco SD-WAN verwendet werden kann.

Es ist sehr ähnlich, dass die gleiche Lösung für AWS beschreibt.

Der Hauptvorteil von GCP Cloud Interconnect als ein weiteres Transportmittel für Cisco SD-WAN ist die Möglichkeit, SD-WAN-Richtlinien für alle Transporte einschließlich GCP Cloud Interconnect zu verwenden. Kunden können SD-WAN-anwendungssensitive Richtlinien erstellen und kritische Anwendungen über GCP Cloud Interconnect routen und im Falle von SLA-Verletzungen über das öffentliche Internet umleiten.

Problem

GCP Cloud Interconnect bietet keine nativen SD-WAN-Funktionen. Typische Fragen von

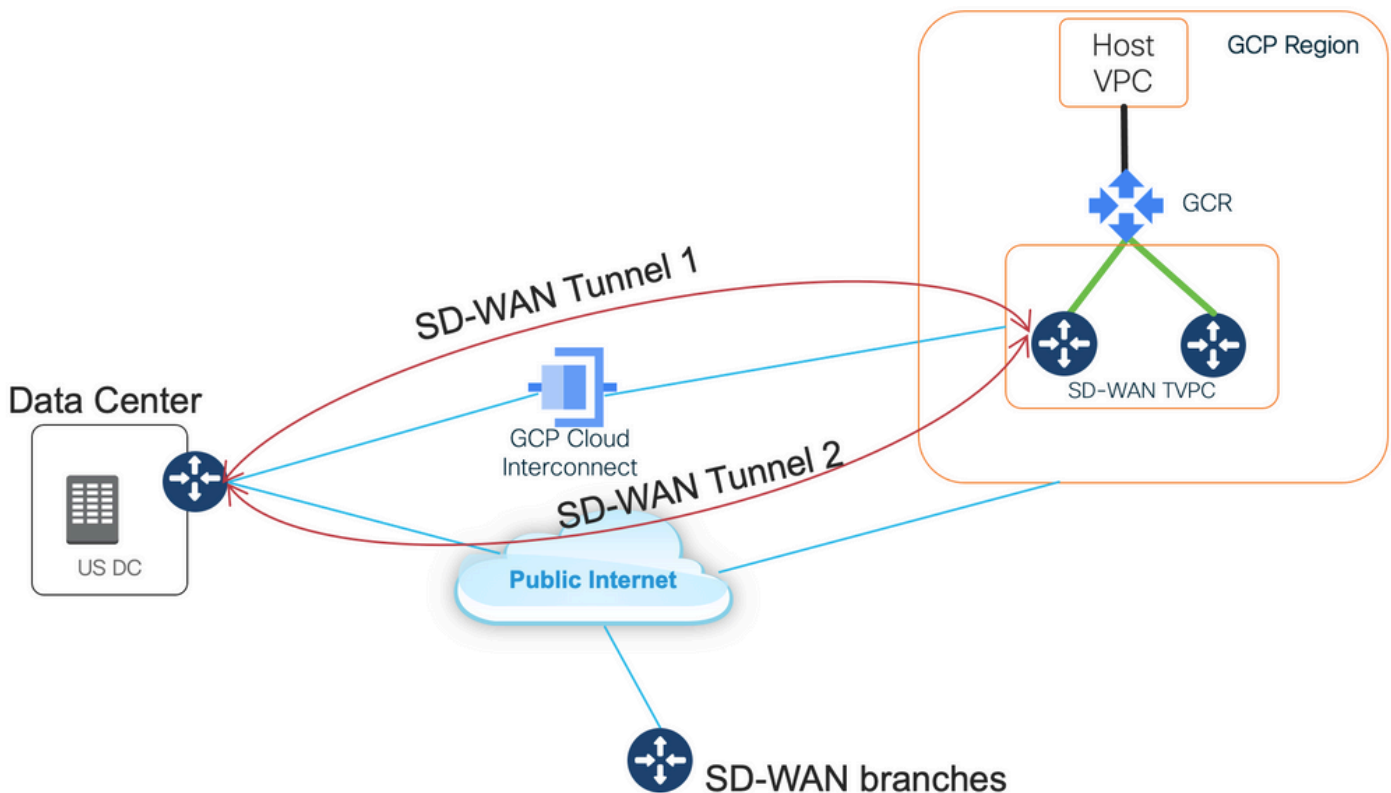
Enterprise SD-WAN-Kunden sind:

- "Kann ich GCP Cloud Interconnect als Underlay für Cisco SD-WAN verwenden?"
- "Wie kann ich GCP Cloud Interconnect mit Cisco SD-WAN verbinden?"
- "Wie kann ich eine ausfallsichere, sichere und skalierbare Lösung erstellen?"

Lösung

Übersicht über das Design

Der zentrale Designpunkt ist die Verbindung des Rechenzentrums über GCP Cloud Interconnect mit Cisco SD-Routern, die von Cloud onRamp für die Multicloud-Bereitstellung erstellt wurden, wie im Bild gezeigt.



Diese Lösung bietet folgende Vorteile:

- Vollständig automatisch: Cisco Cloud onRamp für die Automatisierung über mehrere Clouds kann für die Bereitstellung von SD-WAN-Transit-VPCs mit zwei SD-WAN-Routern verwendet werden. Host-VPCs können als Teil von Cloud onRamp erkannt und SD-WAN-Netzwerken mit nur einem Mausklick zugeordnet werden.
- Vollständiges SD-WAN über GCP Cloud Interconnect: GCP Cloud Interconnect ist nur ein weiterer SD-WAN-Transport. Alle SD-WAN-Funktionen wie anwendungssensitive Richtlinien, Verschlüsselung usw. können nativ über GCP Cloud Interconnect im SD-WAN-Tunnel verwendet werden.

Beachten Sie, dass die Skalierbarkeit dieser Lösung mit der C8000V-Leistung auf GCP einhergeht. Weitere Informationen zur C8000v-Leistung auf GCP finden Sie unter [SalesConnect](#).

Lösungsdetails

Der Hauptpunkt, um diese Lösung zu verstehen, sind SD-WAN-Farben. Bitte beachten Sie, dass GCP SD-WAN-Router **private Farbe private2** für die Internetverbindung sowie die Konnektivität über Interconnect haben, dass SD-WAN-Tunnel über das Internet unter Verwendung öffentlicher IP-Adressen gebildet werden und dass SD-WAN-Tunnel (unter Verwendung derselben Schnittstelle) über die Verbindungsstromkreise unter Verwendung privater IP-Adressen zu einem Rechenzentrum/Standort eingerichtet werden. Das bedeutet, dass der Data Center Router (biz-internet color) eine Verbindung zu GCP SD-WAN-Routern (private2 color) über das Internet mit öffentlichen IP-Adressen und über seine private Farbe über Private IP herstellen wird.

Allgemeine Informationen zu SD-WAN-Farben:

Transport Locators (TLOCs) beziehen sich auf die WAN-Transportschnittstellen (VPN 0), über die SD-WAN-Router mit dem Underlay-Netzwerk verbunden sind. Jede TLOC wird eindeutig durch eine Kombination aus der System-IP-Adresse des SD-WAN-Routers, der Farbe der WAN-Schnittstelle und der Transportkapselung (GRE oder IPsec) identifiziert. Das Cisco Overlay Management Protocol (OMP) wird zur Verteilung von TLOCs (auch als TLOC-Routen bezeichnet), SD-WAN-Overlay-Präfixen (auch als OMP-Routen bezeichnet) und weiteren Informationen zwischen SD-WAN-Routern verwendet. SD-WAN-Router können sich über TLOC-Routen gegenseitig erreichen und IPsec-VPN-Tunnel untereinander einrichten.

SD-WAN-Router und/oder Controller (vManage, vSmart oder vBond) können sich im Netzwerk hinter Network Address Translation (NAT)-Geräten befinden. Wenn sich ein SD-WAN-Router bei einem vBond-Controller authentifiziert, erkennt der vBond-Controller während des Austauschs sowohl die private IP-Adresse/Portnummer als auch die öffentliche IP-Adresse/Portnummer. vBond-Controller fungieren als Session Traversal Utilities for NAT (STUN)-Server, mit denen SD-WAN-Router zugeordnete und/oder übersetzte IP-Adressen und Portnummern ihrer WAN-Transportschnittstellen erkennen können.

Auf SD-WAN-Routern ist jeder WAN-Transport mit einem öffentlichen und privaten IP-Adresspaar verknüpft. Die private IP-Adresse gilt als die Adresse vor der NAT. Dies ist die IP-Adresse, die der WAN-Schnittstelle des SD-WAN-Routers zugewiesen wird. Obwohl dies als private IP-Adresse gilt, kann diese IP-Adresse entweder Teil des öffentlich routbaren IP-Adressbereichs oder Teil des nicht öffentlich routbaren IP-Adressbereichs IETF RFC 1918 sein. Die öffentliche IP-Adresse gilt als Post-NAT-Adresse. Dies wird vom vBond-Server erkannt, wenn der SD-WAN-Router anfänglich mit dem vBond-Server kommuniziert und sich authentifiziert. Die öffentliche IP-Adresse kann entweder Teil des öffentlich routbaren IP-Adressbereichs oder Teil des nicht öffentlich routbaren IP-Adressbereichs von IETF RFC 1918 sein. Ohne NAT sind die öffentlichen und privaten IP-Adressen der SD-WAN-Transportschnittstelle identisch.

TLOC-Farben sind statisch definierte Schlüsselwörter, die zur Identifizierung einzelner WAN-Transportnetze auf jedem SD-WAN-Router verwendet werden. Jeder WAN-Transport auf einem bestimmten SD-WAN-Router muss eine eindeutige Farbe aufweisen. Farben werden auch verwendet, um einen einzelnen WAN-Transport als öffentlich oder privat zu identifizieren. Die Farben Metro-Ethernet, MPLS und private1, private2, private3, private4, private5 und private6 gelten als private Farben. Sie sind für die Verwendung in privaten Netzwerken oder Orten ohne NAT bestimmt. Die Farben sind 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, public-internet, red und silver sind öffentliche Farben. Sie sind für die Verwendung in öffentlichen Netzwerken oder an Orten mit öffentlicher IP-Adressierung der WAN-Transportschnittstellen vorgesehen, entweder nativ oder über NAT.

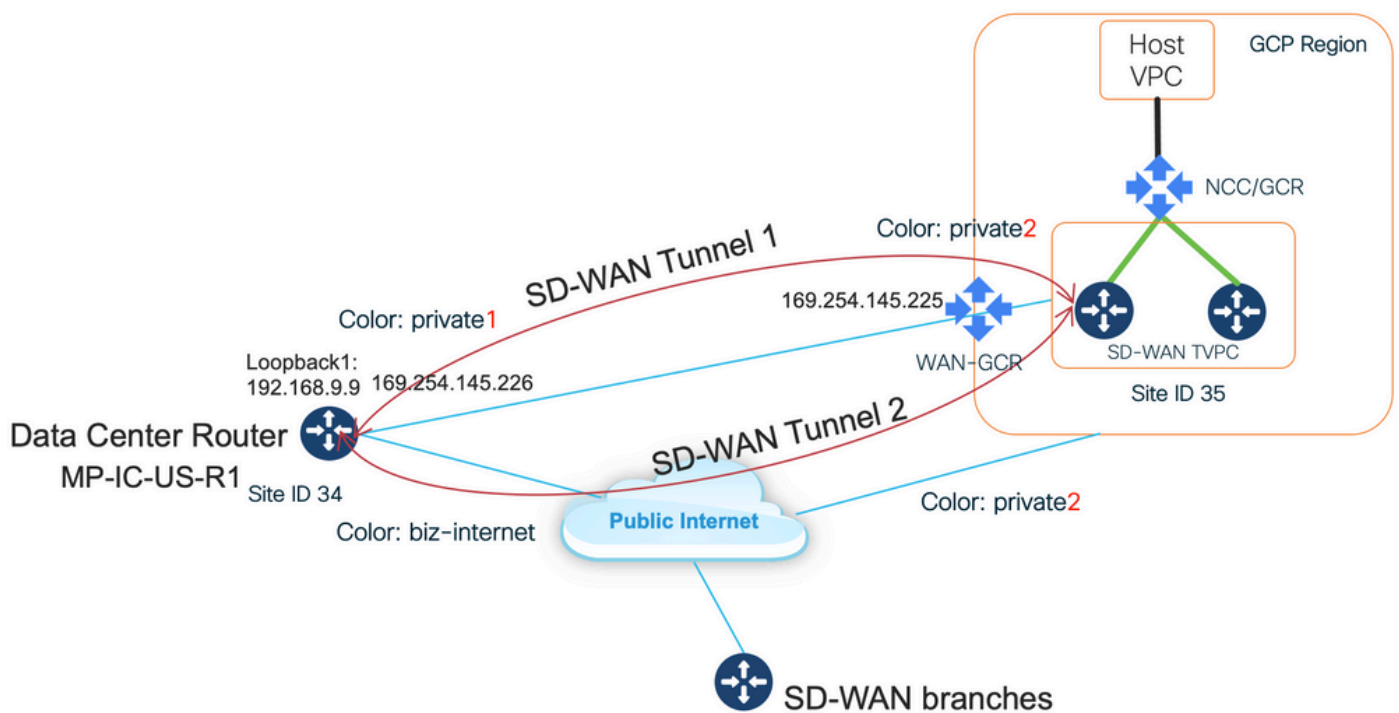
Die Farbe legt die Verwendung privater oder öffentlicher IP-Adressen für die Kommunikation über die Kontroll- und Datenebene fest. Wenn zwei SD-WAN-Router versuchen, miteinander zu kommunizieren, wobei beide WAN-Transportschnittstellen private Farben verwenden, versucht

jede Seite, eine Verbindung zur privaten IP-Adresse des Routers herzustellen. Wenn eine oder beide Seiten öffentliche Farben verwenden, versucht jede Seite, eine Verbindung zur öffentlichen IP-Adresse des Routers der Außenstelle herzustellen. Eine Ausnahme bildet, wenn die Standort-IDs von zwei Geräten identisch sind. Wenn die Standort-IDs identisch sind, die Farben jedoch öffentlich sind, werden die privaten IP-Adressen für die Kommunikation verwendet. Dies kann bei SD-WAN-Routern auftreten, die versuchen, mit einem vManage oder vSmart Controller am gleichen Standort zu kommunizieren. Beachten Sie, dass SD-WAN-Router standardmäßig keine IPsec-VPN-Tunnel untereinander erstellen, wenn sie dieselben Standort-IDs haben.

Hier sehen Sie die Ausgabe des Data Center-Routers, der zwei Tunnel via Internet (color biz-internet) und zwei Tunnel über GCP Cloud Interconnect (color private1) zu zwei SD-WAN-Routern anzeigt. Weitere Informationen finden Sie in der vollständigen Konfiguration des DC-Routers im Anhang.

```
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#
```

Dieses Bild zeigt Topologiedetails mit IP-Adressen und SD-WAN-Farben, die zur Verifizierung der Lösung verwendet werden.



Verwendete Software:

- SD-WAN-Controller mit CCO Version 20.7.1.1

- Rechenzentrums-Router, simuliert mit C8000v mit 17.06.01a, bereitgestellt über vManage Cloud onRamp für Interconnect mit Megaport
- Zwei SD-WAN-Router in GCP: C8000v mit 17.06.01a wird über vManage Cloud onRamp für Multicloud bereitgestellt

Schritt 1: Vorbereitung

Stellen Sie sicher, dass für Cisco vManage ein funktionierendes GCP-Konto definiert ist und die globalen Einstellungen für die Cloud onRamp korrekt konfiguriert sind.

Definieren Sie auch ein Interconnect-Partnerkonto in vManage. In diesem Blog wird Megaport als Interconnect-Partner verwendet, sodass Sie ein geeignetes Konto und globale Einstellungen definieren können.

Schritt 2: Erstellen eines Cisco Cloud Gateway mit Cloud onRamp für Multicloud-Workflows

Dies ist ein unkomplizierter Prozess: zwei SD-WAN-Geräte auswählen, die Standard-GCP-Vorlage anhängen und bereitstellen. Weitere Informationen finden Sie in der [Multicloud-Dokumentation zu Cloud onRamp](#).

Schritt 3: Fügen Sie in der GCP-Konsole eine Partner Interconnect-Verbindung hinzu.

Verwenden Sie den GCP-Konfigurations-Workflow (**Hybrid Connectivity > Interconnect**), um eine Partner Interconnect-Verbindung mit einem ausgewählten Partner herzustellen. Im Fall dieses Blogs - mit Megaport, wie im Bild gezeigt.

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

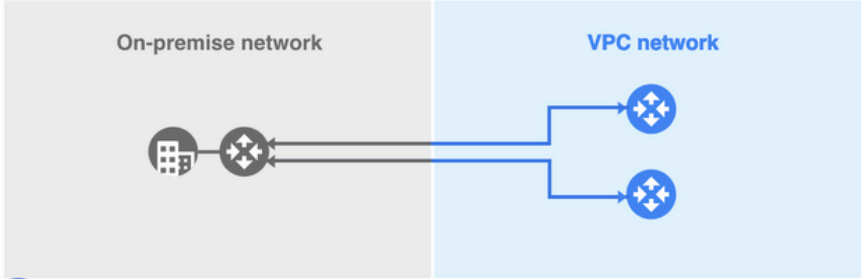
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

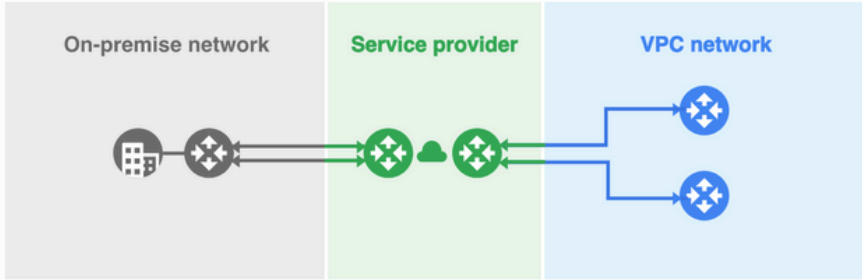
Interconnect type

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**

Wählen Sie die Option **ICH HABE BEREITS EINEN SERVICE PROVIDER**.

Zur einfachen Demonstration wird die Option **"Ein einzelnes VLAN erstellen"** ohne Redundanz verwendet.

Wählen Sie den richtigen Netzwerknamen aus, der zuvor von Cloud onRamp für Multicloud-Workflows erstellt wurde. Im Abschnitt "VLAN" (VLAN) können Sie einen neuen GCR-Router erstellen und einen Namen für das VLAN definieren, der später im Abschnitt "Cloud onRamp Interconnect" angezeigt wird.

Dieses Bild zeigt alle Punkte, die erwähnt werden.

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> <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> <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) ? <small>Region is permanent</small></p> <p>VLAN</p> <p>Cloud Router * gcp-gcr-ic-r1 ?</p> <p>VLAN attachment name * test-vlan-name ? <small>Lowercase letters, numbers, hyphens allowed</small></p> <p>Description VLAN for Megaport</p> <p>Maximum transmission unit (MTU) * 1440</p>
Cloud Routers	
Network Connectivity Center	

Im Prinzip einmal Schritt 3. ist abgeschlossen, können Sie einfach die BGP-Konfiguration abrufen und die Verbindung basierend auf dem Interconnect-Anbieter herstellen. In diesem Fall wird Megaport zum Testen verwendet. Sie können jedoch jede Art von Verbindung verwenden, die über Megaport, Equinix oder einen MSP möglich ist.

Schritt 4: Verwenden von Cloud onRamp Interconnect in Cisco vManage zum Erstellen der DC-Verbindung

Ähnlich wie beim AWS-Blog können Sie mit dem Cisco Cloud onRamp Interconnect-Workflow mit Megaport einen Rechenzentrums-Router erstellen und für GCP Cloud Interconnect verwenden. Bitte beachten Sie, dass Megaport hier nur zu Testzwecken eingesetzt wird. Wenn Sie bereits über ein Rechenzentrum verfügen, müssen Sie Megaport nicht verwenden.

Wählen Sie in Cisco vManage einen kostenlosen SD-WAN-Router aus, fügen Sie die Standard-CoR-Megaport-Vorlage hinzu, und stellen Sie diesen mithilfe des CoR Interconnect-Workflows als Cisco Cloud Gateway in Megaport bereit.

Sobald der Cisco SD-WAN-Router in Megaport aktiv ist, können Sie eine Verbindung mithilfe des CoR Interconnect-Workflows herstellen, wie im Bild gezeigt.

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

Schritt 5: Konfigurieren des RZ-Routers zum Einrichten von Tunneln über das Internet und über GCP Cloud Interconnect

Setzen Sie den SD-WAN-Megaport-Router in den CLI-Modus, und **verschieben Sie** die Konfiguration von der Service-Seite auf VPN0. Da GCP IP-Adressen der Adresse 169.254.x.y verwendet, können Sie eine Loopback1-Schnittstelle auf dem Router des Rechenzentrums erstellen und diese für die SD-WAN-Kommunikation über GCP Cloud Interconnect verwenden.

Nachfolgend sind die relevanten Teile der Konfiguration des DC-Routers aufgeführt.

```
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
!
```

Weitere Informationen finden Sie in der vollständigen Konfiguration des DC-Routers im zweiten Abschnitt des Dokuments.

Überprüfung

GCP Cloud Interconnect-Status:

The screenshot shows the Google Cloud Platform console for the project 'npitaev20-4-ef-gcp-project'. The 'Interconnect' page is active, displaying 'VLAN ATTACHMENTS' and 'PHYSICAL CONNECTIONS'. 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
gcp-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		

BGP-Verbindungen zwischen dem Rechenzentrums-Router und dem WAN-GCR implementieren 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#
```

SD-WAN-Router-Konfiguration für DC-Megaport

```
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 private1 private1 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
!
```



```
ip unnumbered Loopback1
no ip redirects
ipv6 unnumbered Loopback1
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#