

Google Cloud Interconnectをトランスポートとして設定し、Cisco SD-WANをクリックで使用

内容

[概要](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[設計の概要](#)

[ソリューションの詳細](#)

[ステップ1：準備](#)

[ステップ2：マルチクラウドワークフロー用のクラウドオンランプを使用したCisco Cloud Gatewayの作成](#)

[ステップ3:GCPコンソールでのパートナーインターコネクト接続の追加](#)

[ステップ4:Cisco vManageでCloud onRamp Interconnectを使用してDC接続を作成する](#)

[手順5：インターネットおよびGCPクラウド相互接続を介してトンネルを確立するようにDCルータを設定する](#)

[確認](#)

[DCメガポートSD-WANルータの設定](#)

概要

このドキュメントでは、ソフトウェア定義のワイドエ**ア**ネットワーク(SD-WAN)トランスポートとしてGoogleクラウド相互接続を使用する方法について説明します。

背景説明

Google Cloud Platform(GCP)のワークロードを持つ企業のお客様は、データセンターまたはハブの接続に**クラウド**インターコネクトを使用します。同時に、パブリックインターネット接続はデータセンターでも非常に一般的であり、他の場所とのSD-WAN接続のアンダーレイとして使用されます。この記事では、GCPクラウドインターコネクトをCisco SD-WANのアンダーレイとして使用する方法について説明します。

これは、AWSの同じソリューションを説明する方法とよく似ています。

GCPクラウドインターコネクトをCisco SD-WANのもう1つのトランスポートとして使用する主な利点は、GCPクラウドインターコネクトを含むすべてのトランスポートでSD-WANポリシーを使用できることです。SD-WANアプリケーション対応ポリシーを作成し、GCPクラウドインターコネクト経由で重要なアプリケーションをルーティングし、SLA違反の場合はパブリックインターネット経由で再ルーティングできます。

問題

GCPクラウドインターコネクトは、ネイティブのSD-WAN機能を提供しません。エンタープライ

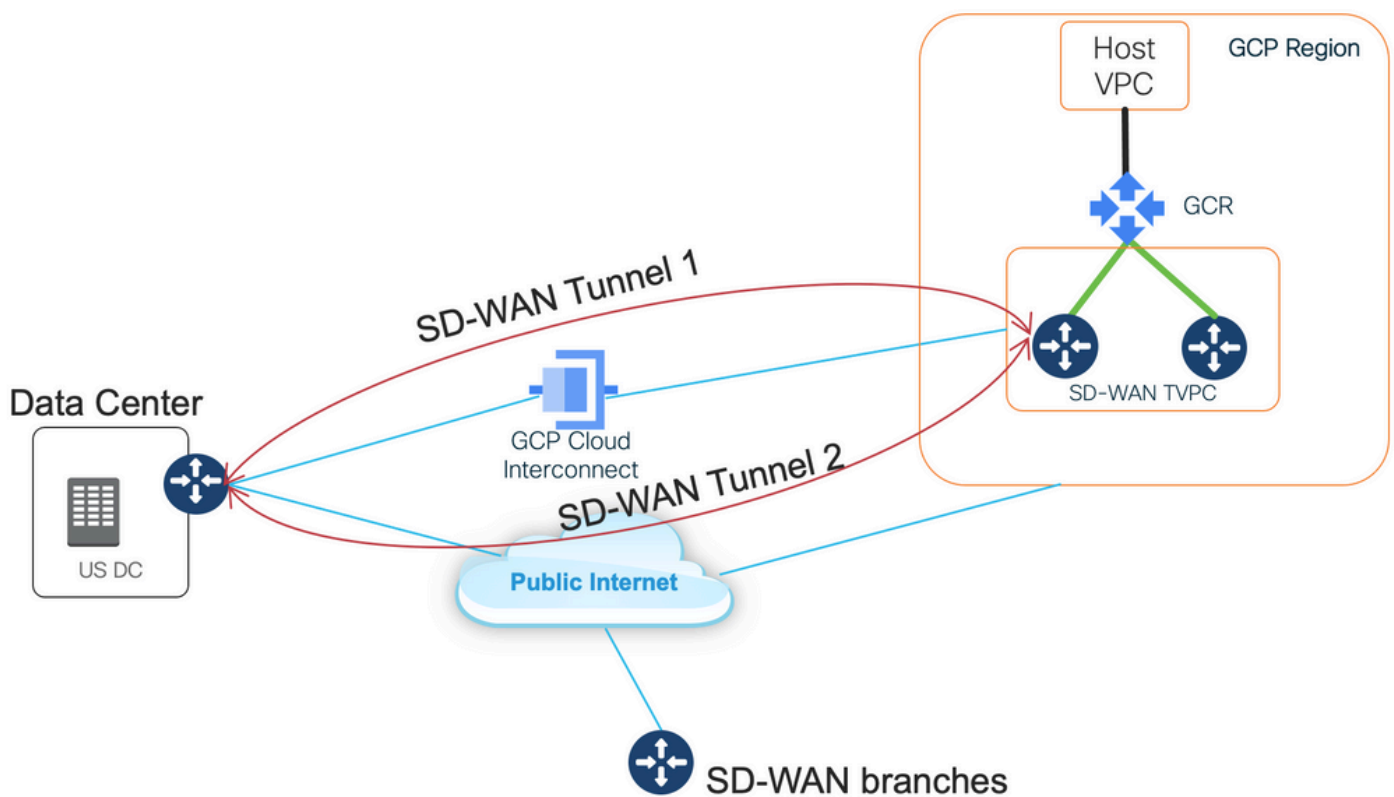
ズSD-WANのお客様からの一般的な質問は次のとおりです。

- 「Cisco SD-WANのアンダーレイとしてGCP Cloud Interconnectを使用できますか」
- 「GCP Cloud InterconnectとCisco SD-WANを相互接続するにはどうすればよいですか。」
- 「復元力と安全性に優れたスケーラブルなソリューションを作成するにはどうすればよいか」

解決方法

設計の概要

主な設計ポイントは、図に示すように、Cloud onRampによって作成されたマルチクラウドプロビジョニング用のCisco SDルーターへのGCPクラウドインターコネクトを介したデータセンターの接続です。



このソリューションの利点は次のとおりです。

- 完全自動：Cisco Cloud onRamp for Multicloud Automationを使用すると、2つのSD-WANルーターを使用してSD-WAN中継VPCを導入できます。ホストVPCはCloud onRampの一部として検出でき、ワンクリックでSD-WANネットワークにマッピングできます。
- 完全なSD-WAN over GCPクラウドインターコネクト：GCPクラウドインターコネクトは、単なるSD-WANトランスポートです。アプリケーション対応ポリシー、暗号化などのすべてのSD-WAN機能は、GCPクラウドインターコネクト上のSD-WANトンネルでネイティブに使用できます。

このソリューションの拡張性は、GCPのC8000Vのパフォーマンスと連動することに注意してください。GCPでのC8000vのパフォーマンスの詳細については、[SalesConnect](#)を参照してください。

ソリューションの詳細

このソリューションを理解するための重要なポイントは、SD-WANカラーです。GCP SD-WANルータはインターコネクト経由の接続だけでなくインターネット接続用のプライベートカラー **private2**を持ち、パブリックIPアドレスを使用してインターネット経由でSD-WANトンネルが形成されます。つまり、データセンタールータ(biz-internet color)は、パブリックIPアドレスを持つインターネット経由およびプライベートIP経由のプライベートカラー経由で、GCP SD-WANルータ(private2 color)への接続を確立します。

SD-WANの色に関する一般情報：

トランスポートロケータ(TLOC)は、SD-WANルータがアンダーレイネットワークに接続するWANトランスポート(VPN 0)インターフェイスを指します。各TLOCは、SD-WANルータのシステムIPアドレス、WANインターフェイスの色、およびトランスポートカプセル化 (GREまたはIPsec) の組み合わせによって一意に識別されます。Cisco Overlay Management Protocol(OMP)は、TLOC (TLOCルートとも呼ばれる)、SD-WANオーバーレイプレフィックス (OMPルートとも呼ばれる)、およびその他の情報をSD-WANルータ間で配布するために使用されます。SD-WANルータが相互に到達し、相互にIPsec VPNトンネルを確立する方法を認識するのは、TLOCルートです。

SD-WANルータおよび/またはコントローラ (vManage、vSmart、またはvBond) は、ネットワーク内のネットワークアドレス変換(NAT)デバイスの背後に配置できます。 SD-WANルータがvBondコントローラに対して認証を行うと、vBondコントローラは、交換中にSD-WANルータのプライベートIPアドレス/ポート番号とパブリックIPアドレス/ポート番号設定の両方を学習します。vBondコントローラはNAT(STUN)サーバのセッショントラバーサルユーティリティとして機能し、SD-WANルータがWANトランスポートインターフェイスのマッピングおよび/または変換されたIPアドレスとポート番号を検出できるようにします。

SD-WANルータでは、すべてのWANトランスポートがパブリックIPアドレスとプライベートIPアドレスのペアに関連付けられます。プライベートIPアドレスはプレNATアドレスと見なされます。これは、SD-WANルータのWANインターフェイスに割り当てられたIPアドレスです。これはプライベートIPアドレスと見なされますが、このIPアドレスは、パブリックにルーティング可能なIPアドレス空間の一部か、IETF RFC 1918のパブリックにルーティングできないIPアドレス空間の一部のどちらかになります。パブリックIPアドレスはポストNATアドレスと見なされます。これは、SD-WANルータが最初にvBondサーバと通信して認証するとき、vBondサーバによって検出されます。パブリックIPアドレスは、パブリックにルーティング可能なIPアドレス空間の一部またはIETF RFC 1918のパブリックにルーティングできないIPアドレス空間の一部にすることもできます。NATがない場合、SD-WANトランスポートインターフェイスのパブリックIPアドレスとプライベートIPアドレスの両方が同じです。

TLOCカラーは、各SD-WANルータで個々のWANトランスポートを識別するために使用される静的に定義されたキーワードです。特定のSD-WANルータ上の各WANトランスポートは、一意の色を持つ必要があります。色は、個々のWANトランスポートをパブリックまたはプライベートとして識別するためにも使用されます。メトロイーサネット、Mpls、およびprivate1、private2、private3、private4、private5、およびprivate6の色は、プライベートカラーと見なされます。これらは、プライベートネットワークまたはNATが存在しない場所で使用することを目的としています。色は3g、biz-internet、blue、bronze、custom1、custom2、custom3、default、gold、green、lte、public-internet、red、およびsilverです。これらのプロトコルは、WANトランスポートインターフェイスのパブリックIPアドレスを持つパブリックネットワークや場所で、ネイティブまたはNATを介して使用することを目的としています。

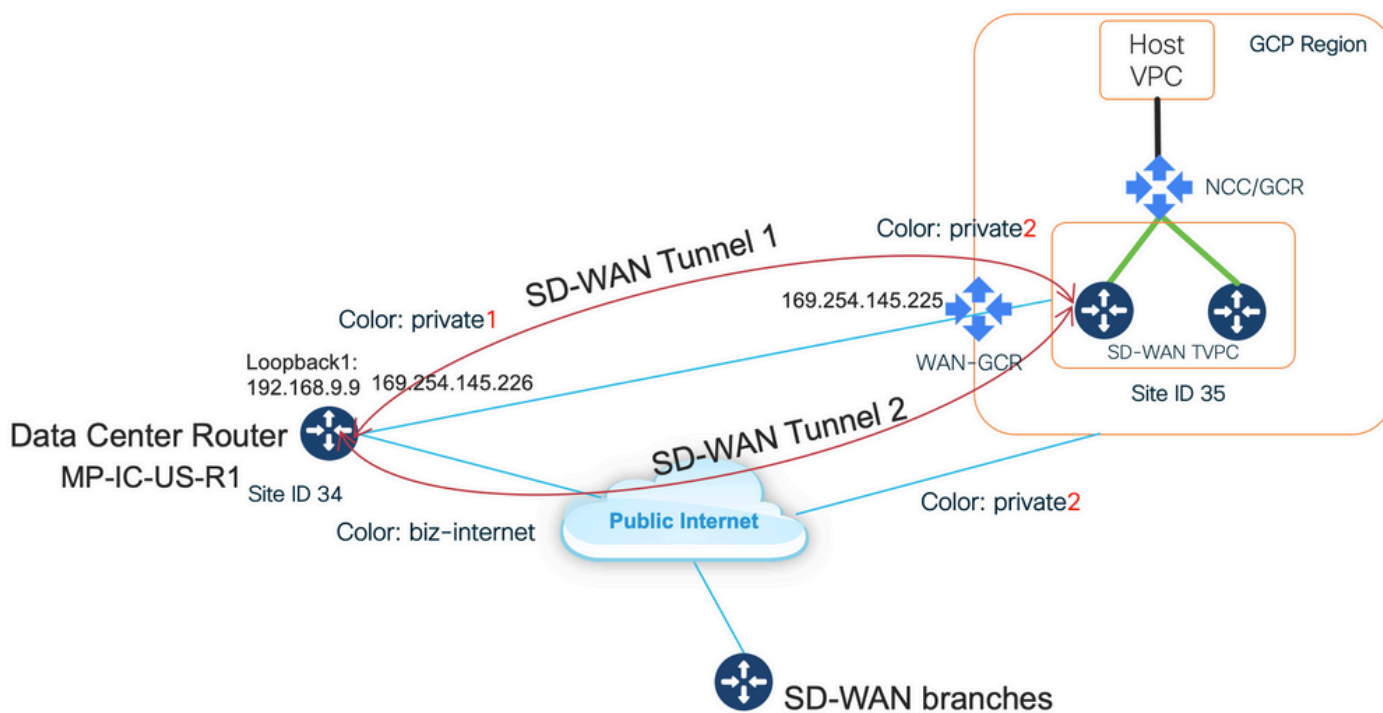
色は、コントロールプレーンとデータプレーンを介して通信する際のプライベートIPアドレスまたはパブリックIPアドレスの使用を指定します。2台のSD-WANルータが互いに通信を試み、両方

がプライベートカラーのWANトランスポートインターフェイスを使用する場合、それぞれの側がリモートルータのプライベートIPアドレスへの接続を試みます。一方または両方の側が公開カラーを使用している場合、各側はリモートルータの公開IPアドレスへの接続を試みます。ただし、2つのデバイスのサイトIDが同じである場合は例外です。サイトIDが同じで、色がパブリックの場合、プライベートIPアドレスが通信に使用されます。これは、同じサイトにあるvManageまたはvSmartコントローラと通信しようとしているSD-WANルータで発生する可能性があります。SD-WANルータが同じサイトIDを持つ場合、デフォルトでは互いにIPsec VPNトンネルを確立しないことに注意してください。

次に、Data Centerルータからの出力を示します。このルータは、インターネット（カラービズインターネット）経由の2つのトンネルと、GCPクラウド相互接続（カラープライベート1）経由の2つのトンネルを2つのSD-WANルータに示します。詳細については、添付ファイルの完全なDCルータ設定を参照してください。

```
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#
```

次の図は、ソリューションの検証に使用されるIPアドレスとSD-WAN色を使用したトポロジの詳細を示しています。



使用するソフトウェア：

- CCOバージョン20.7.1.1が稼働するSD-WANコントローラ

- 17.06.01aを実行するC8000vでシミュレートされたデータセンタールータ (vManage Cloud onRampを介してプロビジョニング、メガポートを使用した相互接続)
- GCPの2つのSD-WANルータ : 17.06.01aを実行するC8000vは、マルチクラウド用vManage Cloud onRampを介してプロビジョニング

ステップ1 : 準備

Cisco vManageに動作中のGCPアカウントが定義されており、Cloud onRampグローバル設定が正しく設定されていることを確認します。

vManageでインターコネクトパートナーアカウントも定義してください。このブログでは、相互接続パートナーとしてメガポートが使用されているため、適切なアカウントとグローバル設定を定義できます。

ステップ2 : マルチクラウドワークフロー用のクラウドオンランプを使用したCisco Cloud Gatewayの作成

これは簡単なプロセスです。2つのSD-WANデバイスを選択し、デフォルトのGCPテンプレートを添付して導入します。詳細は、マルチクラウド [のCloud onRampのドキュメントを参照](#)してください。

ステップ3:GCPコンソールでのパートナーインターコネクト接続の追加

GCPの設定手順のワークフロー([ハイブリッド接続(Hybrid Connectivity)] > [相互接続(Interconnect)])を使用して、選択したパートナーとのパートナーインターコネクト接続を作成します。このブログの場合、図に示すように、メガポートが使用されます。

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

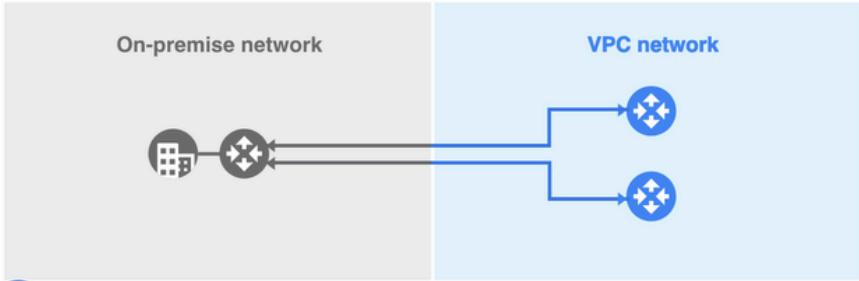
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

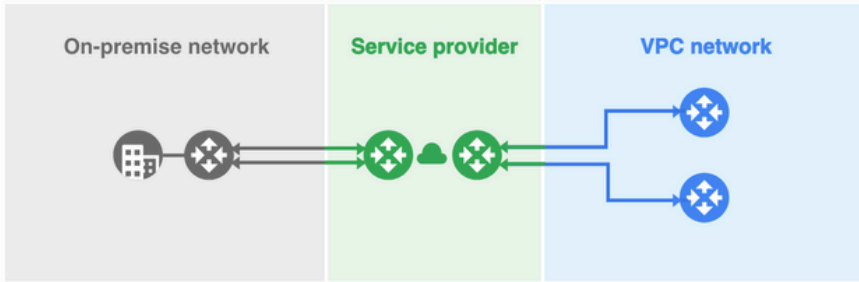
Interconnect type

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 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 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

[I ALREADY HAVE A SERVICE PROVIDER]オプションを選択してください。

デモンストレーションを簡単にするために、冗長性なしで[Create a single VLAN]オプションを使用します。

Cloud onRamp for Multicloudワークフローで以前に作成した正しいネットワーク名を選択します。
[VLAN]セクションで、新しいGCRルータを作成し、VLANの名前を定義できます。この名前は、後の「クラウドonRamp相互接続」セクションで示します。

この画像は、言及されているすべての点を反映しています。

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

基本的に、ステップ3が完了したら、BGP設定を取得し、相互接続プロバイダーが使用した内容に基づいて接続を確立できます。この場合、メガポートはテストに使用されます。ただし、メガポート、Equinix、またはMSPを使用して、どのような種類の相互接続でも使用できます。

ステップ4: Cisco vManageでCloud onRamp Interconnectを使用してDC接続を作成する

AWSブログと同様に、Cisco Cloud onRamp Interconnectワークフローとメガポートを使用してデータセンタールータを作成し、GCPクラウドインターコネクต์に使用します。メガポートはテスト目的でのみ使用されます。すでにデータセンターのセットアップを行っている場合は、メガポートを使用する必要はありません。

Cisco vManageで、1台の無料SD-WANルータを選択し、デフォルトのCoRメガポートテンプレートを接続し、CoR相互接続ワークフローを使用してメガポートのCisco Cloud Gatewayとして導入します。

メガポートのCisco SD-WANルータがアクティブになったら、図に示すように、CoR相互接続ワークフローを使用して接続を作成します。

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

手順5：インターネットおよびGCPクラウド相互接続を介してトンネルを確立するようにDCルータを設定する

SD-WANメガポートルータをCLIモードにして、サービス側からVPN0に設定を移動します。GCPは169.254.x.yのIPアドレスを使用するため、DCルータ上にLoopback1インターフェイスを作成し、SD WAN通信にににに使用を使用使用できます相互接続

DCルータ設定の関連部分を次に示します。

```
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
!

```

ドキュメントの後半のセクションで、完全なDCルータ設定を参照してください。

確認

GCPクラウド相互接続のステータス：

The screenshot shows the Google Cloud Platform console for the project 'npitaev-20-4-ef-gcp-project'. The 'Interconnect' page is active, displaying 'VLAN ATTACHMENTS'. A table lists one 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		

クラウドインターコネクトを実装するデータセンタールータとWAN GCR間のBGP接続：

```

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#

```

DCメガポートSD-WANルータの設定

```

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$3V6L3V6L2VUI2k$ysPnXOd98RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
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  
!  
!  
!  
!  
!
```



```
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#