Configurer Google Cloud Interconnect en tant que transport avec Cisco SD-WAN en un clic

Table des matières

- Introduction
- Informations générales
- Problème
- Solution
  - Présentation de la conception
  - Détails de la solution
    - Étape 1. Préparation
    - Étape 2. Créer une passerelle cloud Cisco avec Cloud onRamp pour le workflow multicloud
    - Étape 3. Dans la console GCP, ajoutez une connexion d'interconnexion de partenaires
    - Étape 4. Utilisation de l'interconnexion Cloud onRamp dans Cisco vManage pour créer la connexion CC
    - Étape 5. Configuration du routeur DC pour établir des tunnels sur Internet et sur l'interconnexion cloud GCP
    - Vérifier
  - Configuration du routeur SD-WAN à mégaport CC

Introduction

Ce document décrit comment utiliser Google Cloud Interconnect comme transport de réseau étendu défini par logiciel (SD-WAN).

Informations générales

Les entreprises clientes avec des charges de travail sur la plate-forme cloud Google (GCP) utilisent Cloud Interconnect pour la connectivité des data centers ou des concentrateurs. En même temps, la connexion Internet publique est également très courante dans les centres de données et est utilisée comme une sous-couche pour la connectivité SD-WAN avec d'autres sites. Cet article décrit comment l'interconnexion cloud GCP peut être utilisée comme sous-couche pour le SD-WAN de Cisco.

Il est très similaire à celui qui décrit la même solution pour AWS.

Le principal avantage de l'utilisation de l'interconnexion cloud GCP comme simple transport supplémentaire pour Cisco SD-WAN est la possibilité d'utiliser des politiques SD-WAN sur tous les transports, y compris l'interconnexion cloud GCP. Les clients peuvent créer des politiques sensibles aux applications SD-WAN et acheminer les applications critiques via GCP Cloud Interconnect et réacheminer via Internet public en cas de violation des SLA.

Problème

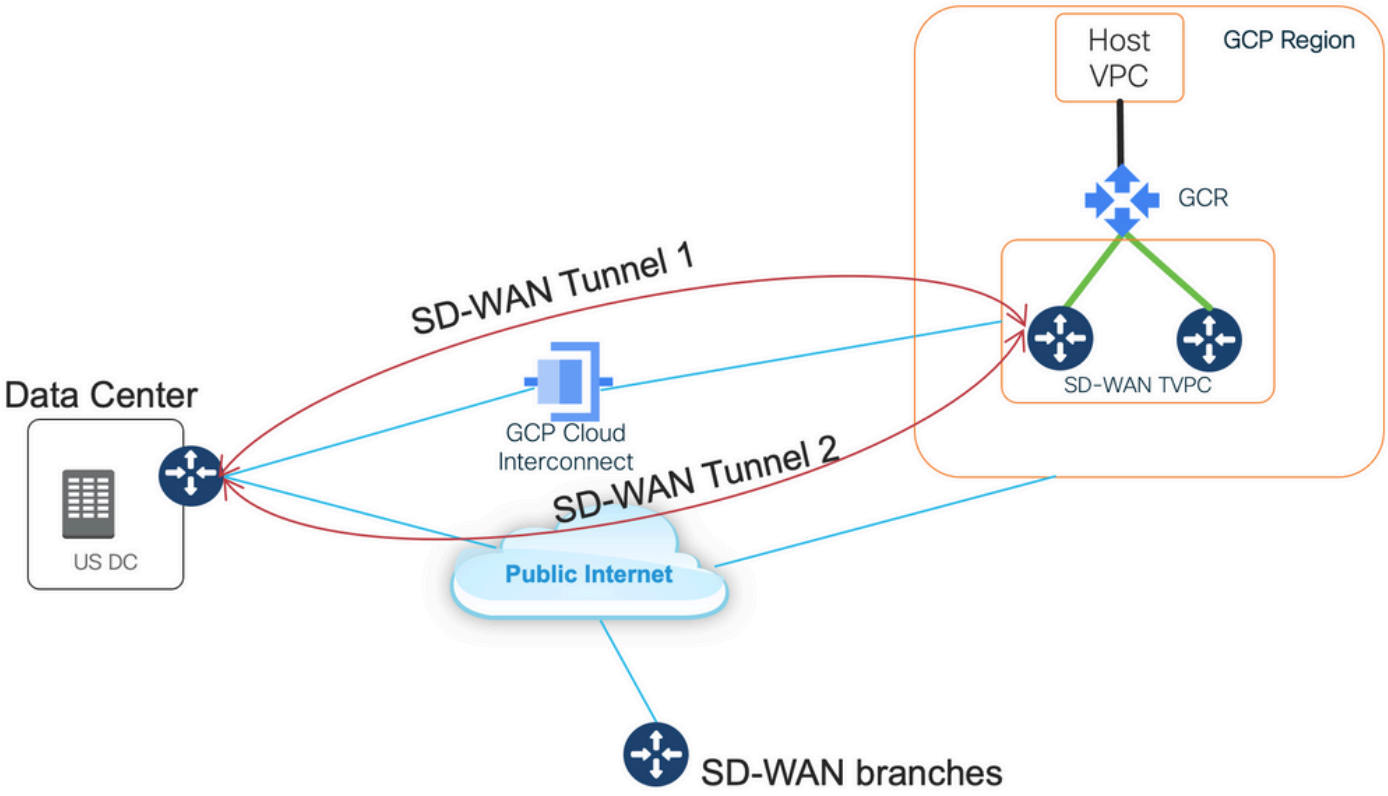
GCP Cloud Interconnect ne fournit pas de fonctionnalités SD-WAN natives. Les questions types des clients SD-WAN d'entreprise sont les suivantes :

- « Puis-je utiliser GCP Cloud Interconnect comme couche sous-jacente pour Cisco SD-WAN ? »
- « Comment puis-je interconnecter GCP Cloud Interconnect et Cisco SD-WAN ? »
- « Comment puis-je créer une solution résiliente, sécurisée et évolutive ? »

Solution

Présentation de la conception

Le point de conception clé est la connexion du data center via GCP Cloud Interconnect aux routeurs SD Cisco créés par Cloud onRamp pour le provisionnement multicloud, comme illustré dans l'image.



Les avantages de cette solution sont les suivants :

- Entièrement automatique : Cisco Cloud onRamp pour l'automatisation multicloud peut être utilisé pour déployer un VPC de transit SD-WAN avec deux routeurs SD-WAN. Les VPC hôtes peuvent être détectés dans le cadre de Cloud onRamp et mappés aux réseaux SD-WAN en un seul clic.
- Interconnexion cloud SD-WAN sur GCP : GCP Cloud Interconnect n'est qu'un autre transport SD-WAN. Toutes les fonctionnalités SD-WAN, telles que les politiques de reconnaissance des applications, le cryptage, etc., peuvent être utilisées nativement sur le tunnel SD-WAN via l'interconnexion cloud GCP.

Veuillez noter que l'évolutivité de cette solution va de pair avec les performances de C8000V sur GCP. Reportez-vous à SalesConnect pour plus de détails sur les performances de C8000v sur GCP.

Détails de la solution

Le point clé pour comprendre cette solution est les couleurs SD-WAN. Veuillez noter que les routeurs GCP SD-WAN auront une couleur privée private2 pour la connectivité Internet ainsi que la connectivité via l'interconnexion, les tunnels SD-WAN seront formés sur Internet à l'aide d'adresses IP publiques ainsi que les tunnels SD-WAN seront établis (à l'aide de la même interface) sur les circuits d'interconnexion à l'aide d'adresses IP privées vers un DC/Site. Cela signifie que le routeur de centre de données (couleur biz-internet) établira une connexion aux routeurs GCP SD-WAN (couleur private2) via Internet avec des adresses IP publiques et via sa couleur privée sur IP privée.

Informations génériques sur les couleurs SD-WAN :

Les localisateurs de transport (TLOC) font référence aux interfaces de transport WAN (VPN 0) par lesquelles les routeurs SD-WAN se connectent au réseau sous-jacent. Chaque TLOC est identifié de manière unique par une combinaison de l'adresse IP système du routeur SD-WAN, de la couleur de l'interface WAN et de l'encapsulation de transport (GRE ou IPsec). Le protocole Cisco Overlay Management Protocol (OMP) est utilisé pour distribuer les TLOC (également appelées routes TLOC), les préfixes de superposition SD-WAN (également appelés routes OMP) et d'autres informations entre les routeurs SD-WAN. C'est par le biais des routes TLOC que les routeurs SD-WAN savent comment se joindre et établir des tunnels VPN IPsec entre eux.

Les routeurs et/ou contrôleurs SD-WAN (vManage, vSmart ou vBond) peuvent être placés derrière les périphériques NAT (Network Address Translation) du réseau. Lorsqu'un routeur SD-WAN s'authentifie auprès d'un contrôleur vBond, le contrôleur vBond apprend les paramètres de l'adresse IP privée/numéro de port et de l'adresse IP publique/numéro de port du routeur SD-WAN pendant l'échange. Les contrôleurs vBond agissent comme des utilitaires de traversée de session pour les serveurs NAT (STUN), permettant aux routeurs SD-WAN de découvrir les adresses IP mappées et/ou traduites et les numéros de port de leurs interfaces de transport WAN.

Sur les routeurs SD-WAN, chaque transport WAN est associé à une paire d'adresses IP publiques et privées. L'adresse IP privée est considérée comme étant l'adresse pré-NAT. Il s'agit de l'adresse IP attribuée à l'interface WAN du routeur SD-WAN. Bien qu'il s'agisse de l'adresse IP privée, cette adresse IP peut faire partie de l'espace d'adressage IP routable publiquement ou de l'espace d'adressage IP non routable publiquement selon la norme IETF RFC 1918. L'adresse IP publique est considérée comme étant l'adresse post-NAT. Ceci est détecté par le serveur vBond lorsque le routeur SD-WAN communique et s'authentifie initialement avec le serveur vBond. L'adresse IP publique peut également faire partie de l'espace d'adressage IP routable publiquement ou de l'espace d'adressage IP routable non public IETF RFC 1918. En l'absence de NAT, les adresses IP publiques et privées de l'interface de transport SD-WAN sont identiques.

Les couleurs TLOC sont des mots clés définis de manière statique et utilisés pour identifier les transports WAN individuels sur chaque routeur SD-WAN. Chaque transport WAN sur un routeur

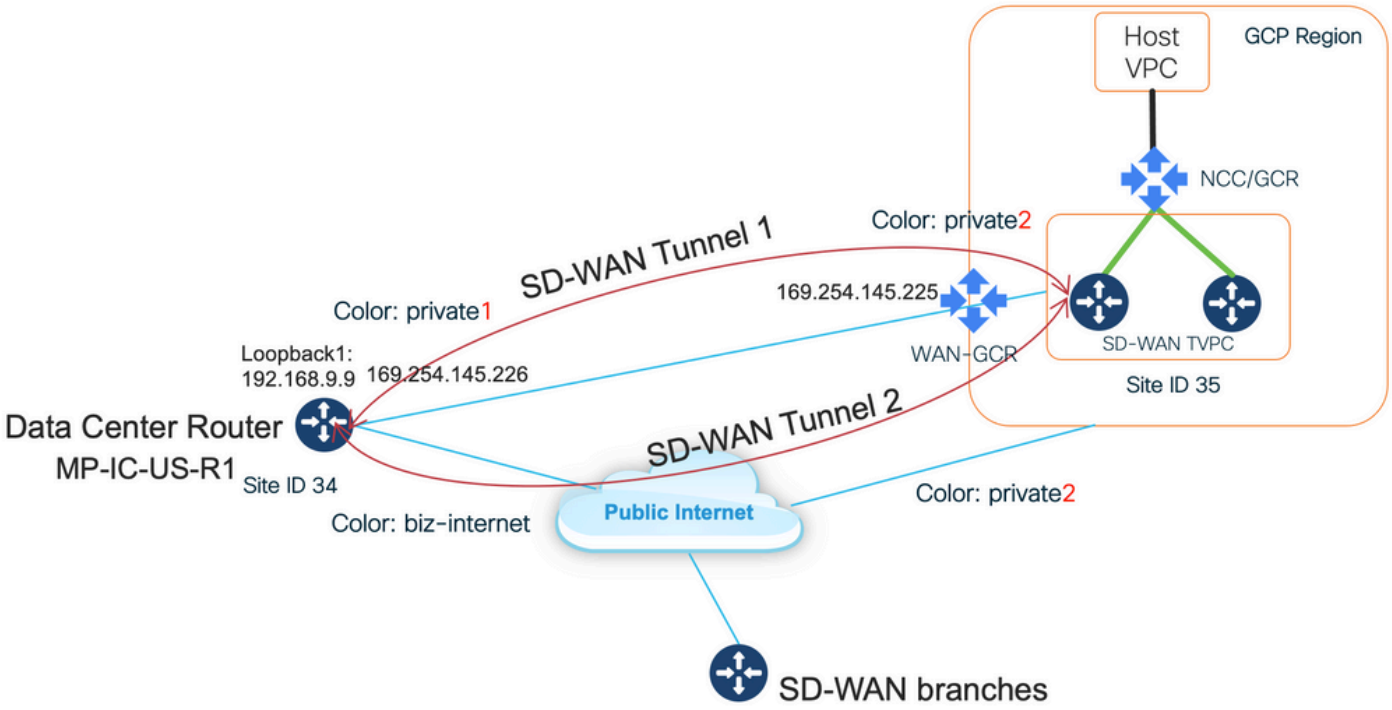
SD-WAN donné doit avoir une couleur unique. Les couleurs sont également utilisées pour identifier un transport WAN individuel comme étant public ou privé. Les couleurs metro-ethernet, Mpls et private1, private2, private3, private4, private5 et private6 sont considérées comme des couleurs privées. Ils sont destinés à être utilisés dans des réseaux privés ou des endroits où il n'y a pas de NAT. Les couleurs sont 3g, biz-internet, bleu, bronze, custom1, custom2, custom3, default, gold, green, lte, public-internet, red et silver sont considérées comme des couleurs publiques. Ils sont destinés à être utilisés dans des réseaux publics ou dans des endroits avec un adressage IP public des interfaces de transport WAN, soit nativement, soit via NAT.

La couleur dicte l'utilisation d'adresses IP privées ou publiques lors de la communication via les plans de contrôle et de données. Lorsque deux routeurs SD-WAN tentent de communiquer entre eux, tous deux à l'aide d'interfaces de transport WAN de couleurs privées, chaque côté tente de se connecter à l'adresse IP privée du routeur distant. Si l'un des côtés ou les deux utilisent des couleurs publiques, chaque côté tentera de se connecter à l'adresse IP publique du routeur distant. Une exception à cette règle est lorsque les ID de site de deux périphériques sont identiques. Lorsque les ID de site sont identiques, mais que les couleurs sont publiques, les adresses IP privées sont utilisées pour la communication. Cela peut se produire lorsque des routeurs SD-WAN tentent de communiquer avec un contrôleur vManage ou vSmart situé sur le même site. Notez que les routeurs SD-WAN n'établissent pas, par défaut, de tunnels VPN IPsec entre eux lorsqu'ils ont les mêmes ID de site.

Voici le résultat du routeur de centre de données, qui montre deux tunnels via Internet (color biz-internet) et deux tunnels via GCP Cloud Interconnect (color private1) vers deux routeurs SD-WAN. Reportez-vous à la configuration complète du routeur CC dans la pièce jointe pour plus de détails.

```
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
35.35.35.1  35  up  biz-internet  private2   162.43.150.15  35.212.232.51  12347  ipsec  7  1000  10  4
35.35.35.1  35  up  private1      private2   192.168.9.9    10.35.0.2      12347  ipsec  7  1000  10  0
35.35.35.2  35  up  private1      private2   192.168.9.9    10.35.0.3      12347  ipsec  7  1000  10  0
...
MP-IC-US-R1#
```

Cette image illustre les détails de la topologie avec les adresses IP et les couleurs SD-WAN utilisées pour vérifier la solution.



Logiciels utilisés :

- Contrôleurs SD-WAN exécutant CCO version 20.7.1.1
- Routeur de data center simulé avec C8000v exécutant 17.06.01a provisionné via vManage Cloud onRamp pour l'interconnexion avec Megaport
- Deux routeurs SD-WAN dans GCP : C8000v exécutant 17.06.01a provisionné via vManage Cloud onRamp pour Multicloud

Étape 1. Préparation

Assurez-vous que Cisco vManage dispose d'un compte GCP opérationnel et que les paramètres globaux Cloud onRamp sont configurés correctement.

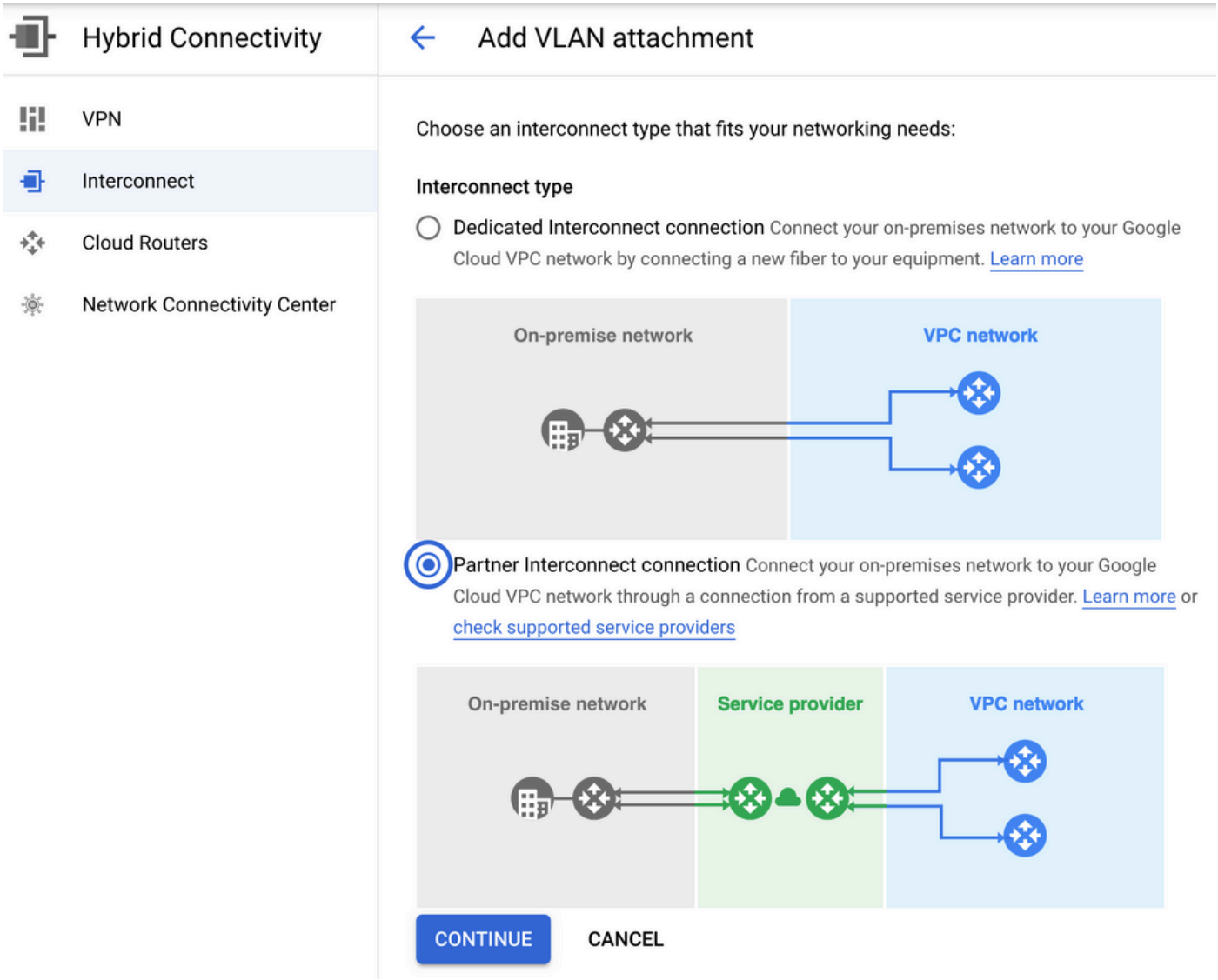
Définissez également un compte de partenaire d'interconnexion dans vManage. Dans ce blog Megaport est utilisé comme partenaire d'interconnexion, de sorte que vous pouvez définir un compte approprié et des paramètres globaux.

Étape 2. Créer une passerelle cloud Cisco avec Cloud onRamp pour le workflow multicloud

Il s'agit d'un processus simple : sélectionnez deux périphériques SD-WAN, associez le modèle GCP par défaut, déployez. Reportez-vous à la documentation Cloud onRamp for Multicloud pour plus d'informations.

Étape 3. Dans la console GCP, ajoutez une connexion d'interconnexion de partenaires

Utilisez le workflow de configuration étape par étape GCP (Connectivité hybride > Interconnexion) pour créer une connexion d'interconnexion de partenaire avec un partenaire sélectionné, dans le cas de ce blog - avec Megaport comme illustré dans l'image.

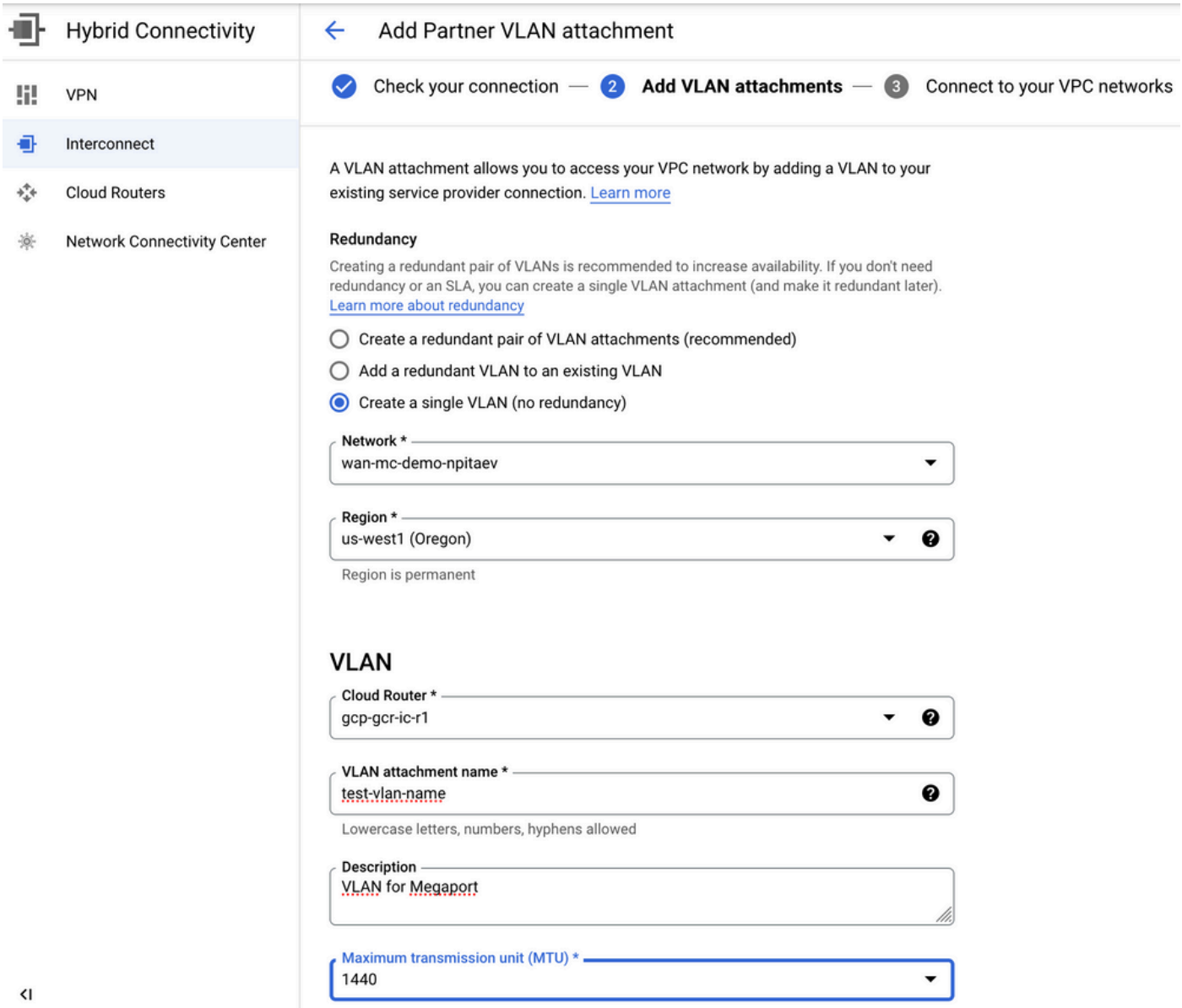


Sélectionnez l'option J'AI DÉJÀ UN FOURNISSEUR DE SERVICES.

Pour faciliter la démonstration, l'option Create a single VLAN est utilisée sans redondance.

Sélectionnez le nom de réseau correct, précédemment créé par Cloud onRamp pour le flux de travail multicloud. Dans la section VLAN, vous pouvez créer un nouveau routeur GCR et définir un nom pour le VLAN, qui sera affiché plus tard dans la section Cloud on Ramp Interconnect.

Cette image reflète tous les points qui sont mentionnés.



En fait, une fois l'étape 3. terminée, vous pouvez simplement prendre la configuration BGP et établir la connectivité en fonction de ce que le fournisseur d'interconnexion a utilisé. Dans ce cas, Megaport est utilisé pour tester. Cependant, vous pouvez utiliser n'importe quel type d'interconnexion qui peut être via Megaport, Equinix ou un MSP.

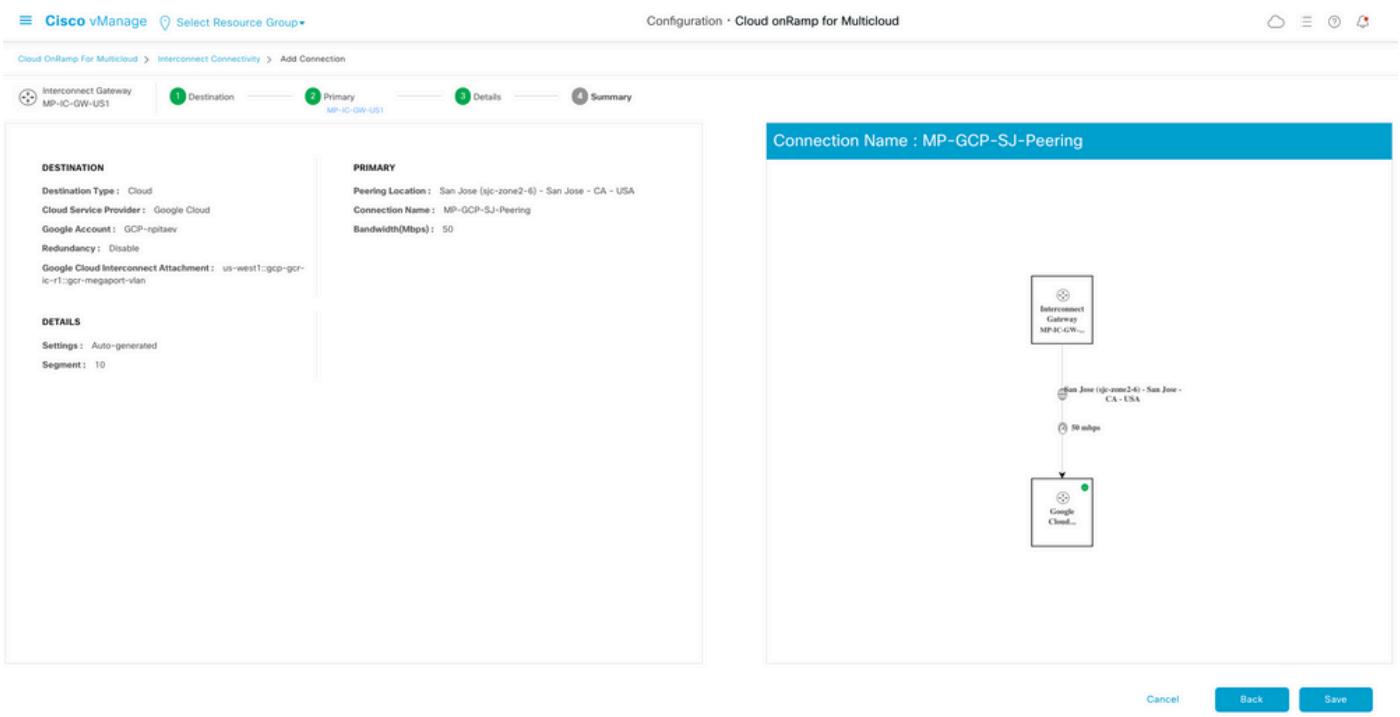
Étape 4. Utilisation de l'interconnexion Cloud onRamp dans Cisco vManage pour créer la connexion CC

Tout comme le blog AWS, utilisez le workflow Cisco Cloud onRamp Interconnect avec Megaport pour créer un routeur de data center et l'utiliser pour l'interconnexion cloud GCP. Notez que Megaport est utilisé ici uniquement à des fins de test. Si vous disposez déjà d'une configuration de centre de données, il n'est pas nécessaire d'utiliser Megaport.

Dans Cisco vManage, sélectionnez un routeur SD-WAN gratuit, joignez le modèle CoR Megaport par défaut et déployez-le en tant que passerelle cloud Cisco dans Megaport à l'aide du workflow CoR Interconnect.

Une fois que le routeur SD-WAN Cisco de Megaport sera actif, utilisez le workflow CoR

Interconnect pour créer une connexion, comme illustré dans l'image.



Étape 5. Configuration du routeur DC pour établir des tunnels sur Internet et sur l'interconnexion cloud GCP

Mettez le routeur mégaport SD-WAN en mode CLI et déplacez la configuration du côté service vers VPN0. Comme GCP utilise des adresses IP 169.254.x.y, vous pouvez créer l'interface de bouclage 1 sur le routeur DC et l'utiliser pour la communication SD-WAN via l'interconnexion cloud GCP.

Voici les parties pertinentes de la configuration du routeur CC.

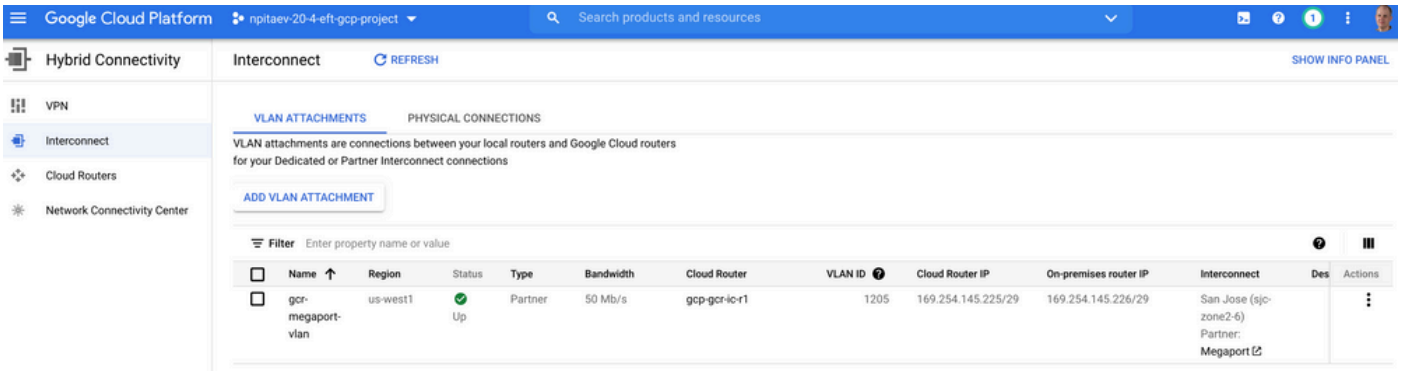
```
interface Loopback1
 no shutdown
 ip address 192.168.9.9 255.255.255.255
!
!
interface Tunnel2
 ip unnumbered Loopback1
 tunnel source Loopback1
 tunnel mode sdwan
!
!
interface GigabitEthernet1.215
 encapsulation dot1Q 215
 ip address 169.254.145.226 255.255.255.248
 ip mtu 1440
!
!
router bgp 64513
 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
!
```

Reportez-vous à la configuration complète du routeur CC dans la dernière section du document.

Vérifier

État de l'interconnexion cloud GCP :



Connectivité BGP entre le routeur de centre de données et le WAN GCR implémentant l'interconnexion cloud :

```
MP-IC-US-R1#sh ip ro bgp
...
10.0.0.0/27 is subnetted, 1 subnets
B 10.35.0.0 [20/100] via 169.254.145.225, 01:25:26
MP-IC-US-R1#
```

Configuration du routeur SD-WAN à mégaport CC

```
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:
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 private1
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
rsakeypair 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
!
!
!
!
!
!
!
!
!
license udi pid C8000V sn 9SRWHHH66II
license boot level network-premier+dna-premier
diagnostic bootup level minimal
memory free low-watermark processor 202832
!
!
spanning-tree extend system-id
!
username admin privilege 15 secret 9 $9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
!
redundancy
!
!
!
!
no crypto ikev2 diagnose error
!
!
lldp run
cdp run
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
interface Loopback1
ip address 192.168.9.9 255.255.255.255
!
interface Loopback65528
vrf forwarding 65528
ip address 192.168.1.1 255.255.255.255
!
interface Tunnel1
ip unnumbered GigabitEthernet1
no ip redirects
ipv6 unnumbered GigabitEthernet1
no ipv6 redirects
tunnel source GigabitEthernet1
tunnel mode sdwan
!
interface Tunnel2
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 s
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,
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/wwl/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#
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.