클릭 한 번으로 Cisco SD-WAN을 통해 Google Cloud Interconnect를 전송으로 구성

목차

소개

이 문서에서는 Google Cloud Interconnect를 SD-WAN(Software-defined Wide Area Network) 전송으로 사용하는 방법에 대해 설명합니다.

배경 정보

Google Cloud Platform(GCP)에서 워크로드를 사용하는 엔터프라이즈 고객은 데이터 센터 또는 허브 연결을 위해 Cloud Interconnect를 사용합니다. 동시에 공용 인터넷 연결은 데이터 센터에서 매우 일반적이며 다른 위치와의 SD-WAN 연결을 위한 언더레이로 사용됩니다. 이 문서에서는 GCP Cloud Interconnect를 Cisco SD-WAN의 언더레이로 사용하는 방법에 대해 설명합니다.

이는 AWS용 동일한 솔루션을 설명하는 것과 매우 유사합니다.

GCP Cloud Interconnect를 Cisco SD-WAN의 또 다른 전송으로 사용할 경우 GCP Cloud Interconnect를 비롯한 모든 전송에서 SD-WAN 정책을 사용할 수 있다는 이점이 있습니다. 고객은 SD-WAN 애플리케이션 인식 정책을 생성하고 GCP Cloud Interconnect를 통해 중요 애플리케이션을 라우팅하고 SLA 위반 시 공용 인터넷을 통해 경로를 재지정할 수 있습니다.

문제

GCP Cloud Interconnect는 네이티브 SD-WAN 기능을 제공하지 않습니다. Enterprise SD-WAN 고객의 일반적인 질문은 다음과 같습니다.

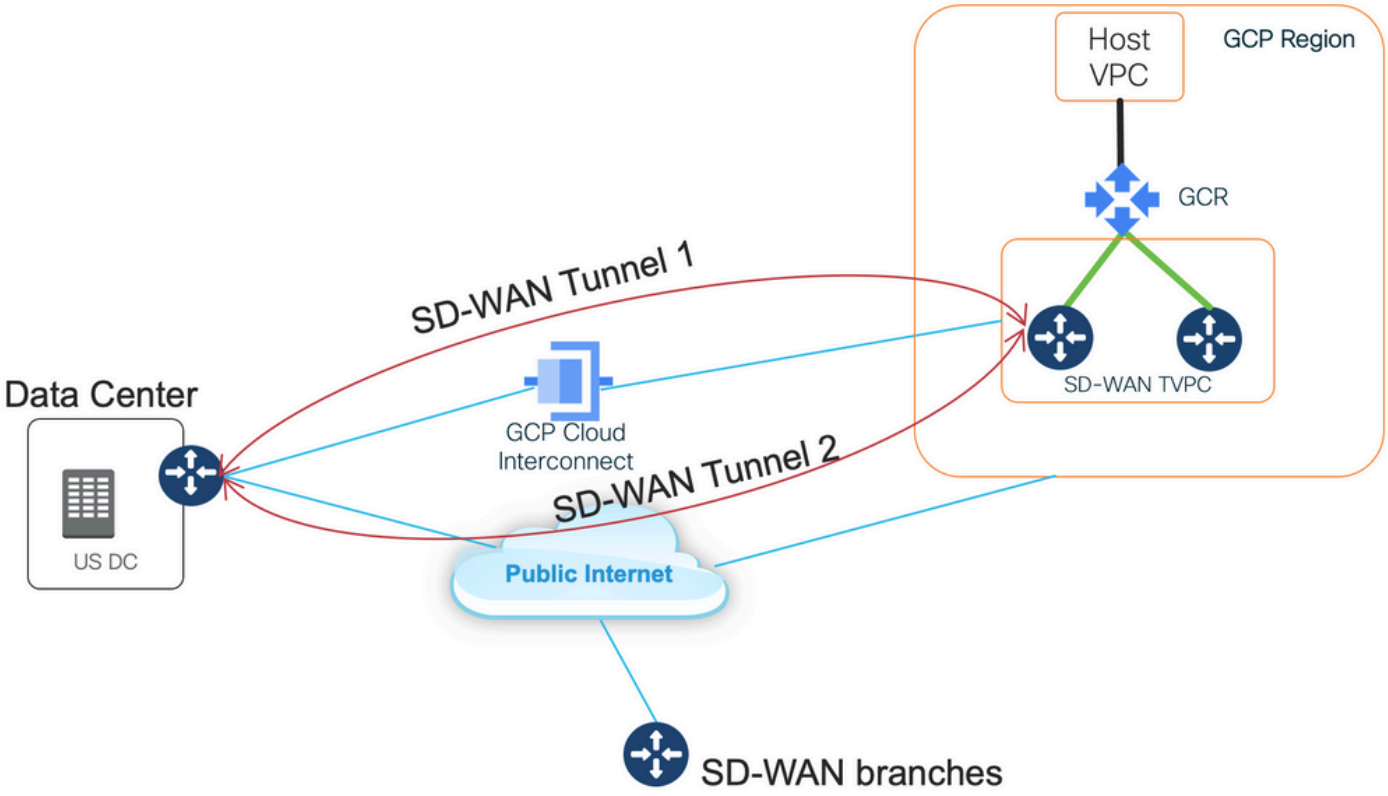
- "GCP Cloud Interconnect를 Cisco SD-WAN의 언더레이로 사용할 수 있습니까?"
- "GCP Cloud Interconnect 및 Cisco SD-WAN을 어떻게 상호 연결할 수 있습니까?"

- "복원력과 보안성, 확장성을 갖춘 솔루션을 만들려면 어떻게 해야 합니까?"

솔루션

설계 개요

핵심 설계 포인트는 GCP Cloud Interconnect를 통해 데이터 센터를 Cloud onRamp for Multicloud 프로비저닝에 의해 생성된 Cisco SD-Router에 연결하는 것입니다(그림 참조).



이 솔루션의 이점은 다음과 같습니다.

- 완전 자동: Cisco Cloud onRamp for Multicloud 자동화는 SD-WAN 트랜짓 VPC를 2개의 SD-WAN 라우터로 구축하는 데 사용할 수 있습니다. 호스트 VPC는 Cloud onRamp의 일부로 검색될 수 있으며, 클릭 한 번으로 SD-WAN 네트워크에 매핑됩니다.
- GCP Cloud Interconnect를 통한 전체 SD-WAN: GCP Cloud Interconnect는 또 다른 SD-WAN 전송에 불과합니다. 애플리케이션 인식 정책, 암호화 등과 같은 모든 SD-WAN 기능은 GCP Cloud Interconnect를 통한 SD-WAN 터널에서 기본적으로 사용할 수 있습니다.

이 솔루션의 확장성은 GCP의 C8000V 성능과 일치합니다. GCP의 C8000v 성능에 대한 자세한 내용은 SalesConnect를 참조하십시오.

솔루션 세부 정보

이 솔루션을 이해하는 핵심은 SD-WAN Colors입니다. GCP SD-WAN 라우터에는 인터넷 연결용 **전용색의2**가 있을 뿐만 아니라 인터커넥트를 통한 연결도 포함됩니다. SD-WAN 터널은 공용 IP 주소를 사용하여 인터넷을 통해 형성되며, SD-WAN 터널은 사설 IP 주소를 사용하여 DC/사이트에 대한 인터커넥트 회선을 통해 설정됩니다(동일한 인터페이스 사용). 즉, 데이터 센터 라우터(biz-internet color)는 공용 IP 주소를 사용하는 인터넷과 프라이빗 IP를 통한 전용 색상을 통해 GCP SD-WAN 라우터(private2 색상)에 대한 연결을 설정합니다.

SD-WAN 색상에 대한 일반 정보:

TLOC(Transport Locator)는 SD-WAN 라우터가 언더레이 네트워크에 연결되는 WAN 전송(VPN 0) 인터페이스를 나타냅니다. 각 TLOC는 SD-WAN 라우터의 시스템 IP 주소, WAN 인터페이스의 색상 및 전송 캡슐화(GRE 또는 IPsec)의 조합을 통해 고유하게 식별됩니다. Cisco OMP(Overlay Management Protocol)는 TLOC(TLOC 경로라고도 함), SD-WAN 오버레이 접두사(OMP 경로라고도 함) 및 SD-WAN 라우터 간의 기타 정보를 배포하는 데 사용됩니다. SD-WAN 라우터가 서로 연결하고 IPsec VPN 터널을 설정하는 방법을 알고 있는 TLOC 경로를 통해 이루어집니다.

SD-WAN 라우터 및/또는 컨트롤러(vManage, vSmart 또는 vBond)는 네트워크 내 NAT(Network Address Translation) 디바이스 뒤에 있을 수 있습니다. SD-WAN 라우터가 vBond 컨트롤러에 인증되면 vBond 컨트롤러는 교환 중에 SD-WAN 라우터의 프라이빗 IP 주소/포트 번호와 공용 IP 주소/포트 번호 설정을 모두 학습합니다. vBond 컨트롤러는 NAT(STUN) 서버용 세션 접근 유틸리티 역할을 하므로 SD-WAN 라우터가 WAN 전송 인터페이스의 매핑된 IP 주소 및/또는 변환된 IP 주소와 포트 번호를 검색할 수 있습니다.

SD-WAN 라우터에서 모든 WAN 전송은 공용 및 사설 IP 주소 쌍과 연결됩니다. 프라이빗 IP 주소는 pre-NAT 주소로 간주됩니다. SD-WAN 라우터의 WAN 인터페이스에 할당된 IP 주소입니다. 이 주소는 사설 IP 주소로 간주되지만 이 IP 주소는 공개적으로 라우팅 가능한 IP 주소 공간의 일부이거나 IETF RFC 1918 비공개적으로 라우팅 가능한 IP 주소 공간의 일부일 수 있습니다. 공용 IP 주소는 post-NAT 주소로 간주됩니다. 이는 SD-WAN 라우터가 처음에 vBond 서버와 통신하고 인증할 때 vBond 서버에서 탐지됩니다. 공용 IP 주소는 공개 라우팅 가능한 IP 주소 공간의 일부이거나 IETF RFC 1918 비공개적으로 라우팅 가능한 IP 주소 공간의 일부일 수도 있습니다. NAT가 없는 경우 SD-WAN 전송 인터페이스의 공용 및 전용 IP 주소가 모두 동일합니다.

TLOC 색상은 각 SD-WAN 라우터에서 개별 WAN 전송을 식별하는 데 사용되는 정적으로 정의된 키워드입니다. 지정된 SD-WAN 라우터의 각 WAN 전송에는 고유한 색상이 있어야 합니다. 또한 색상은 개별 WAN 전송을 공용 또는 사설 전송으로 식별하는 데 사용됩니다. metro-ethernet, Mpls, private1, private2, private3, private4, private5 및 private6의 색상은 전용 색상으로 간주됩니다. NAT가 없는 사설 네트워크 또는 장소에서 사용하기 위한 것입니다. 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, public-internet, red, silver 등의 색상은 공용 색상으로 간주됩니다. 이 솔루션은 공용 네트워크 또는 WAN 전송 인터페이스의 공용 IP 주소 지정이 있는 장소에서 기본적으로 또는 NAT를 통해 사용하도록 설계되었습니다.

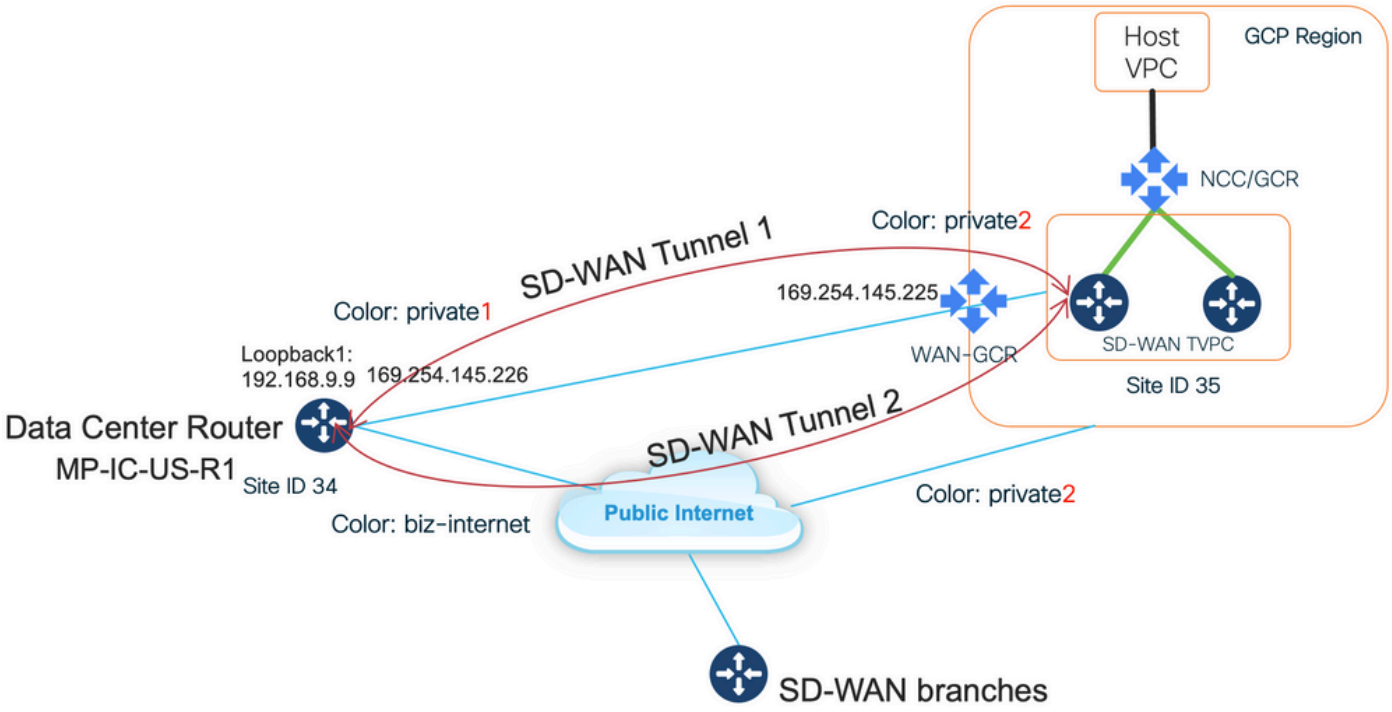
색상은 컨트롤 플레인과 데이터 플레인을 통해 통신할 때 사설 또는 공용 IP 주소를 사용하도록 지정합니다. 두 SD-WAN 라우터가 서로 통신을 시도할 때, 두 라우터는 모두 전용 색상으로 WAN 전송 인터페이스를 사용하여 원격 라우터의 전용 IP 주소에 연결을 시도합니다. 한쪽 또는 양쪽이 모두 공용 색상을 사용하는 경우 각 쪽은 원격 라우터의 공용 IP 주소에 연결을 시도합니다. 단, 두 디바이스의 사이트 ID가 동일할 경우 예외입니다. 사이트 ID가 동일하지만 색상이 공용이면 개인 IP 주소가 통신에 사용됩니다. 이는 동일한 사이트에 있는 vManage 또는 vSmart 컨트롤러와 통신하려는 SD-WAN 라우터에 대해 발생할 수 있습니다. SD-WAN 라우터는 동일한 사이트 ID가 있는 경우 기본적으로 서로 IPsec VPN 터널을 설정하지 않습니다.

다음은 인터넷을 통해 두 개의 터널(색상 비즈 인터넷)과 GCP Cloud Interconnect(color private1)를 통해 두 개의 SD-WAN 라우터에 두 개의 터널을 표시하는 데이터 센터 라우터의 출력입니다. 자세한 내용은 첨부 파일의 전체 DC 라우터 컨피그레이션을 참조하십시오.

```
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#
```

이 이미지는 솔루션 확인에 사용되는 IP 주소 및 SD-WAN 색상으로 토폴로지 세부사항을 보여줍니다.



사용된 소프트웨어:

- CCO 버전 20.7.1.1을 실행하는 SD-WAN 컨트롤러
- vManage Cloud onRamp for Interconnect with Megapport를 통해 프로비저닝된 17.06.01a를 실행하는 C8000v와 시뮬레이션된 데이터 센터 라우터
- GCP의 SD-WAN 라우터 2개: vManage Cloud onRamp for Multicloud를 통해 프로비저닝된 17.06.01a를 실행하는 C8000v

1단계. 준비

Cisco vManage에 작업 중인 GCP 계정이 정의되어 있고 Cloud onRamp 전역 설정이 올바르게 구성되어 있는지 확인합니다.

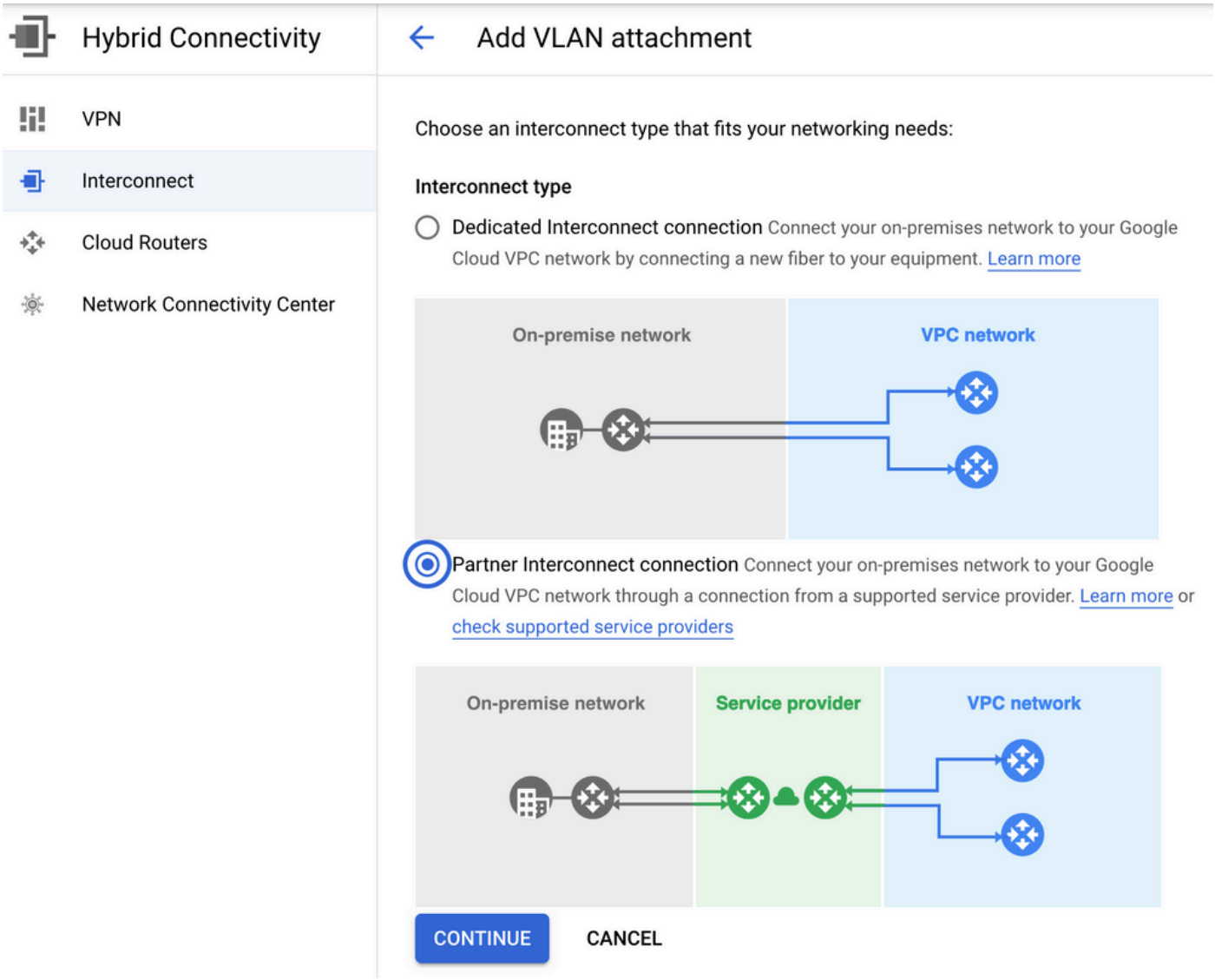
vManage에서도 상호 연결 파트너 어카운트를 정의하십시오. 이 블로그에서는 Megapport가 Interconnect 파트너로 사용되므로 적절한 어카운트 및 전역 설정을 정의할 수 있습니다.

2단계. Cloud onRamp for Multicloud Workflow로 Cisco Cloud Gateway 생성

이는 간단한 프로세스입니다. 두 개의 SD-WAN 디바이스를 선택하고 기본 GCP 템플릿을 연결한 다음 구축합니다. 자세한 내용은 Cloud onRamp for Multicloud 설명서를 참조하십시오.

3단계. GCP Console에서 Partner Interconnect 연결 추가

GCP 단계별 컨피그레이션 워크플로(**Hybrid Connectivity > Interconnect**)를 사용하여 선택한 파트너와의 파트너 상호 연결 연결을 생성합니다(이 블로그의 경우, 이미지에 표시된 대로 Megapport 포함).

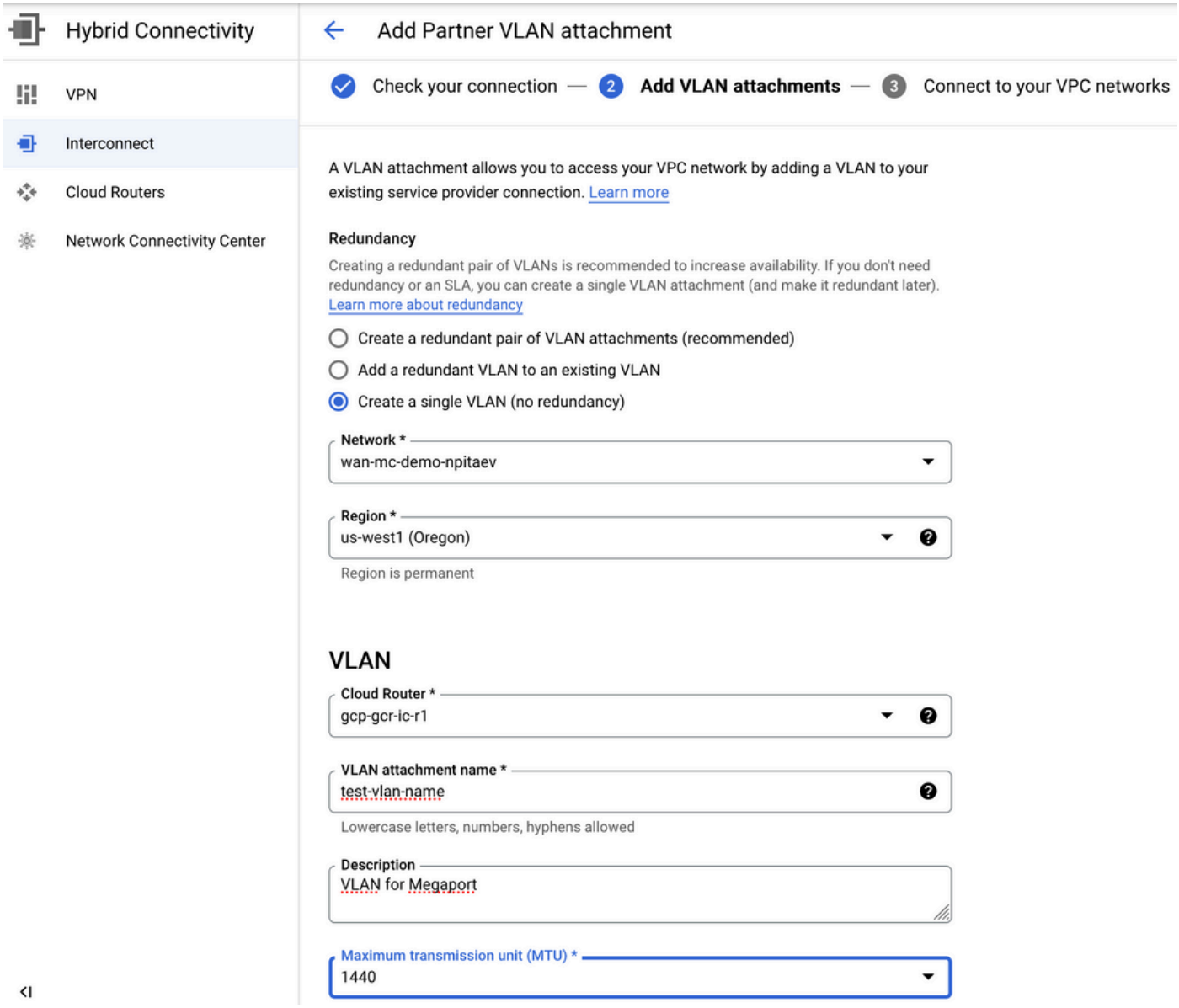


이미 서비스 제공자가 있는 옵션**을 선택하십시오**.

데모를 쉽게 하기 위해 이중화 없이 **단일 VLAN** 생성 옵션이 사용됩니다.

이전에 Cloud onRamp for Multicloud 워크플로에서 생성한 올바른 네트워크 이름을 선택합니다. VLAN 섹션에서 새 GCR 라우터를 생성하고 VLAN의 이름을 정의할 수 있습니다. 이 이름은 나중에 Cloud onRamp Interconnect 섹션에 표시됩니다.

이 이미지는 언급된 모든 점을 반영합니다.



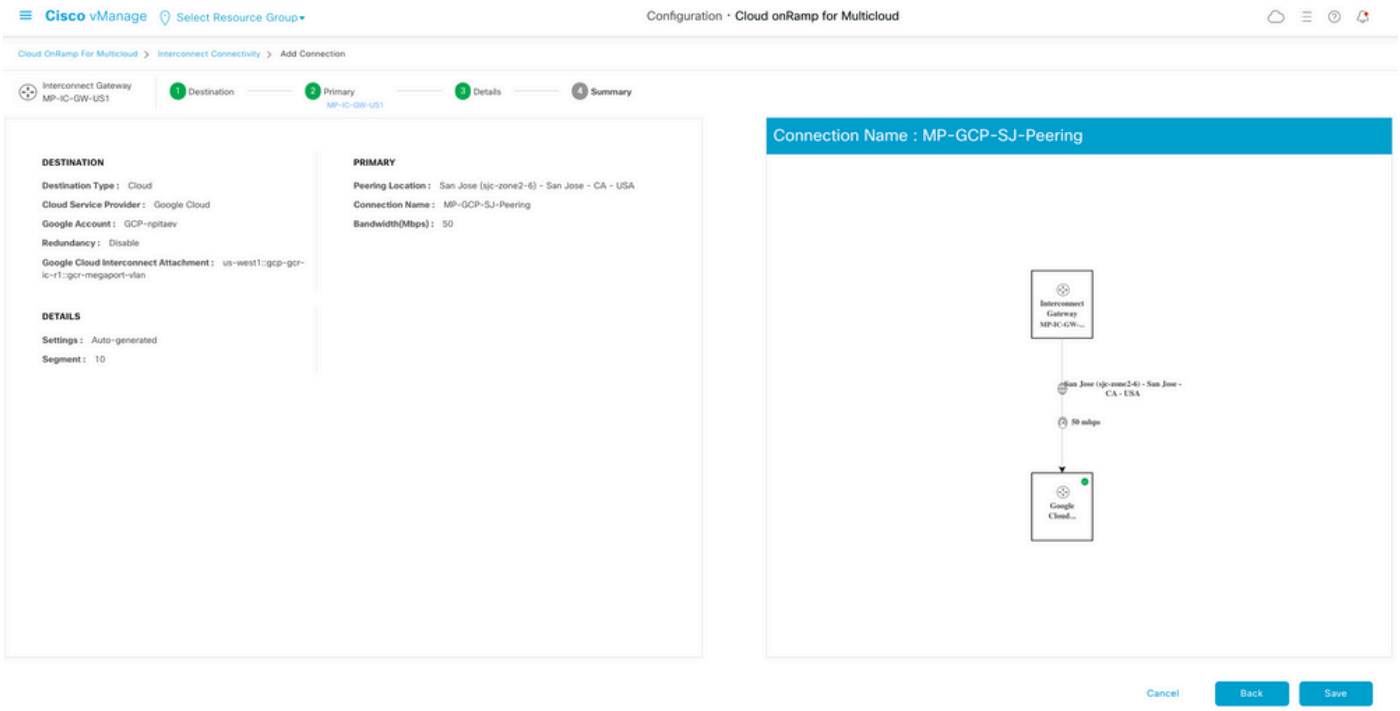
기본적으로 3단계가 완료되면 BGP 컨피그레이션을 가져와서 Interconnect 공급자가 사용한 것을 기반으로 연결을 설정할 수 있습니다. 이 경우 메가포트는 테스트에 사용됩니다. 그러나 Megapport, Equinix 또는 MSP를 통해 가능한 모든 종류의 상호 연결을 사용할 수 있습니다.

4단계. Cisco vManage의 Cloud onRamp Interconnect를 사용하여 DC 연결 생성

AWS 블로그와 마찬가지로 Cisco Cloud onRamp Interconnect 워크플로와 Megapport를 사용하여 데이터 센터 라우터를 생성하고 GCP 클라우드 인터커넥트에 사용합니다. Megapport는 테스트 용도로만 사용됩니다. 이미 데이터 센터 설정이 있는 경우 Megapport를 사용할 필요가 없습니다.

Cisco vManage에서 하나의 무료 SD-WAN 라우터를 선택하고 기본 CoR Megapport 템플릿을 연결한 다음 CoR Interconnect 워크플로를 사용하여 메가포트에서 Cisco Cloud Gateway로 배포합니다.

메가포트의 Cisco SD-WAN 라우터가 활성화되면 CoR Interconnect 워크플로를 사용하여 이미지에 표시된 대로 연결을 생성합니다.



5단계. 인터넷과 GCP Cloud Interconnect를 통해 터널을 설정하도록 DC 라우터 구성

SD-WAN 메가포트 라우터를 CLI 모드로 전환하고 서비스 측에서 VPN0으로 컨피그레이션을 **이동합니다**. GCP는 169.254.x.y IP 주소를 사용하므로 DC 라우터에서 루프백1 인터페이스를 만들고 GCP 클라우드 인터커넥트를 통한 SD-WAN 통신에 사용할 수 있습니다.

다음은 DC 라우터 컨피그레이션의 관련 부분입니다.

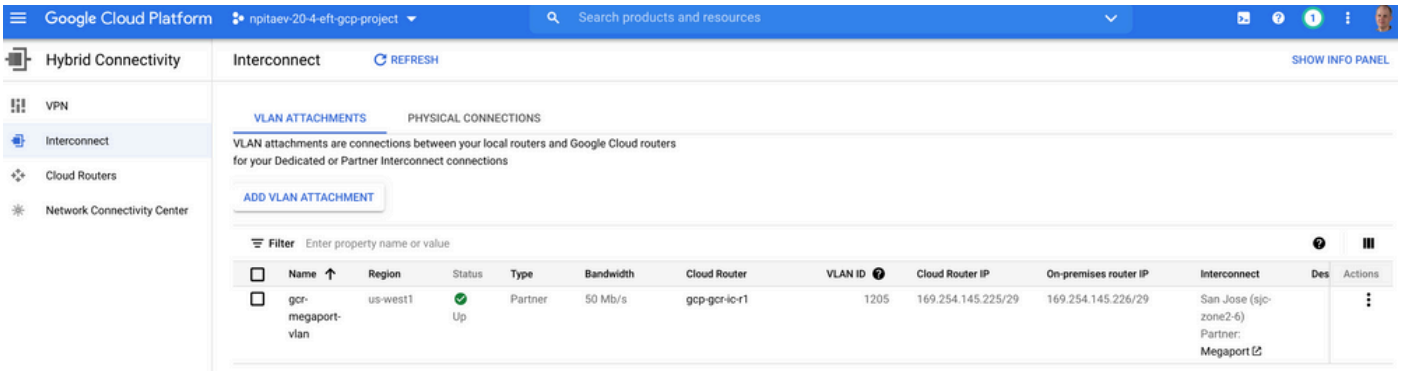
```
interface Loopback1
no shutdown
ip address 192.168.9.9 255.255.255.255
!
!
interface Tunnel2
ip unnumbered Loopback1
tunnel source Loopback1
tunnel mode sdwan
!
!
interface GigabitEthernet1.215
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
ip mtu 1440
!
!
router bgp 64513
bgp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

문서의 후단에서 전체 DC 라우터 컨피그레이션을 참조하십시오.

다음을 확인합니다.

GCP Cloud Interconnect 상태:



Cloud Interconnect를 구현하는 Data Center Router와 WAN GCR 간의 BGP 연결:

```
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 메가포트 SD-WAN 라우터 컨피그레이션

```
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 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 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/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#
```