AWS Direct Connect als transport configureren met SD-WAN in een klik

Inhoud

Inleiding

Dit document beschrijft hoe u Amazon Web Services (AWS) Direct Connect kunt gebruiken als softwaregedefinieerde Wide Area Network (SD-WAN) transport.

Achtergrondinformatie

Het belangrijkste voordeel van AWS Direct Connect als gewoon een ander transport voor Cisco SD-WAN is de mogelijkheid om SD-WAN beleid algemene transporten te gebruiken die omvatten

AWS Direct Connect

Gebruikers in ondernemingen met werkbelastingen op AWS gebruiken AWS Direct Connect voor datacenter- of hubconnectiviteit. Tegelijkertijd is openbare internetverbinding ook zeer gebruikelijk in datacenter en wordt gebruikt als onderlaag voor SD-WAN connectiviteit met andere locaties. Dit document beschrijft hoe AWS Direct Connect kan worden gebruikt als onderlaag voor Cisco SD-WAN. Gebruikers kunnen SD-WAN-toepassingsbewust beleid maken en kritische toepassingen via Direct Connect en omleiden via het openbare internet in geval van overtredingen van Service Level Agreement (SLA).

Probleem

AWS Direct Connect biedt geen native SD-WAN-mogelijkheden. De typische vragen van de gebruikers van SD-WAN van de Onderneming zijn:

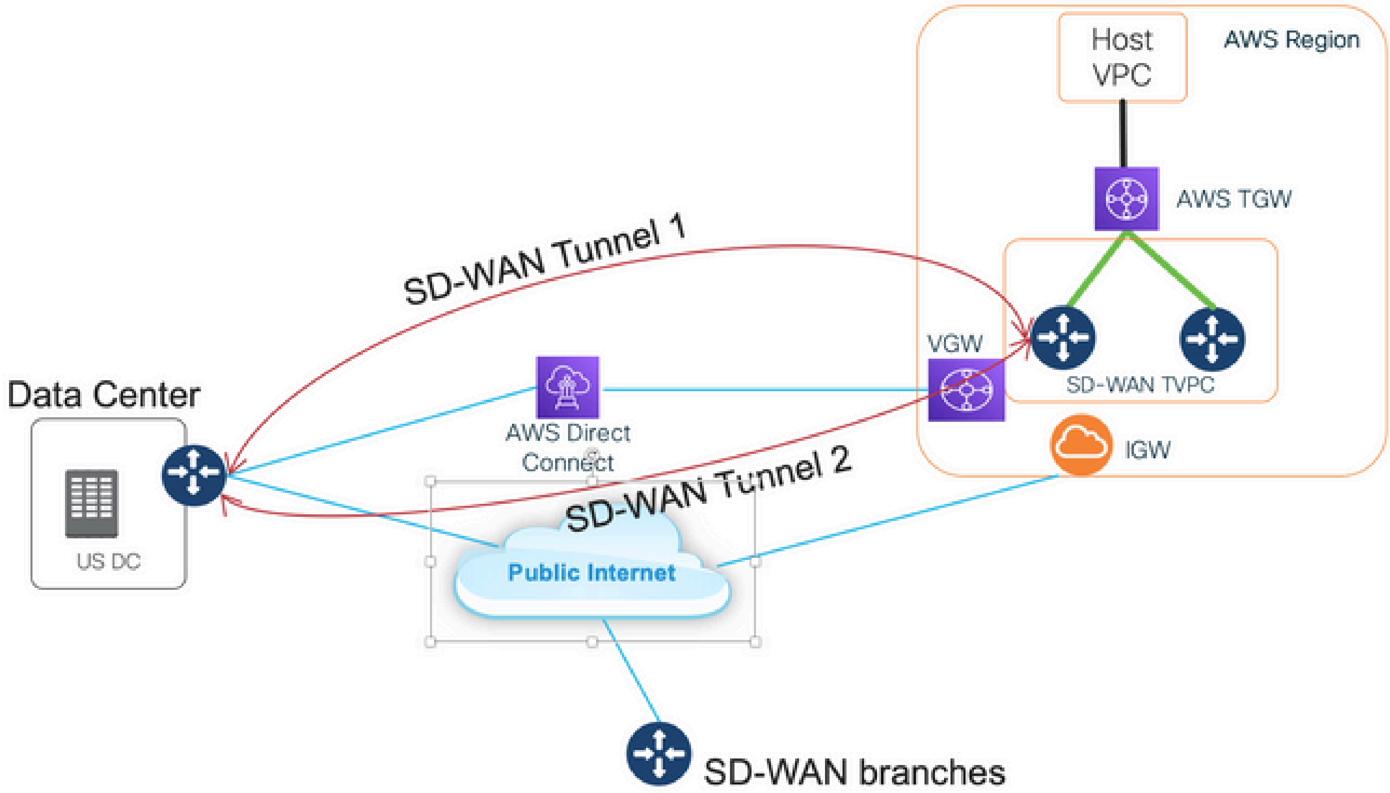
- Kan ik AWS Direct Connect als onderlegger voor Cisco SD-WAN gebruiken?

- Hoe kan ik AWS Direct Connect en Cisco SD-WAN onderling verbinden?
- Hoe kan ik veerkrachtige, veilige en schaalbare oplossingen maken?

Oplossing

Ontwerpoverzicht

Het belangrijkste ontwerppunt is de verbinding van het datacenter via AWS Direct Connect to Virtual Gateway (VGW) in SD-WAN Transit Virtual Private Cloud (VPC) zoals getoond in het beeld.

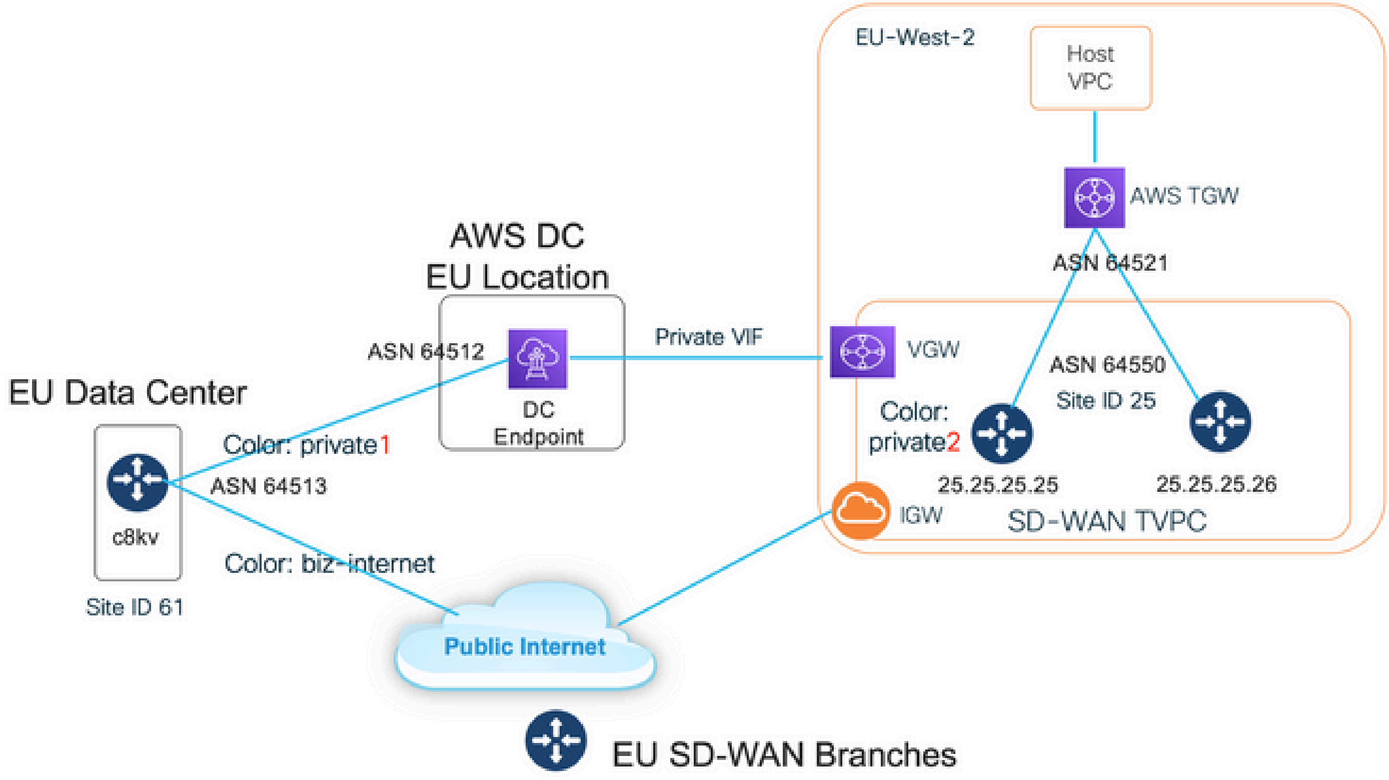


De voordelen van deze oplossing zijn:

- Volledig automatisch: Cisco Cloud onRamp voor Multicloud Automation kan worden gebruikt om SD-WAN transit VPC met twee SD-WAN routers en een nieuwe AWS Transit Gateway (TGW) te implementeren. Host VPC's kunnen worden ontdekt als onderdeel van Cloud onRamp en met één klik worden toegewezen aan SD-WAN-netwerken.
- Full SD-WAN over Direct Connect: AWS Direct Connect is gewoon een ander SD-WAN transport. Alle SD-WAN functies, zoals toepassingsbewust beleid, encryptie, enzovoort, kunnen op de SD-WAN tunnel via AWS Direct Connect worden gebruikt.
- Het voorgestelde ontwerp vermijdt de AWS-beperkingen van het aantal prefixes via een AWS Direct Connect (20/100).

Details van oplossing

Deze afbeelding toont een AWS-regio en datacenter verbonden via Direct Connect met VGW (color private1) in SD-WAN transit VPC en via het openbare internet (color biz-internet). Houd er rekening mee dat AWS SD-WAN c8kv routers SD-WAN kleur private2 voor de internetverbinding gebruiken.



Stap 1. Voorbereiding

Zorg ervoor dat Cisco vManager een actieve AWS-account heeft en dat Cloud onRamp Global Settings correct zijn geconfigureerd.

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

Stap 2. Configuratie van datacenter SD-WAN router

De interface Gigabit Ethernet1 wordt gebruikt voor openbare internetconnectiviteit met kleur biz-internet en de interface Gigabit Ethernet1.1352 wordt gebruikt voor AWS Direct Connect met kleur private1.

Houd er rekening mee dat AWS SD-WAN routers **private kleur private2** hebben voor de internetverbinding en voor de verbinding via Direct Connect. SD-WAN-tunnels worden gevormd via het internet met openbare IP-adressen en SD-WAN-tunnels worden opgezet (met dezelfde interface) via de Direct Connect-circuits met privé IP-adressen naar een DC/Site. Dit betekent dat de Datacenterrouter (biz-internet kleur) een verbinding tot stand brengt met AWS SD-WAN routers (private2 kleur) via het internet met openbare IP-adressen en via de eigen kleur via Private IP.

Generieke informatie over SD-WAN kleuren:

Transport Locators (TLOC's) verwijzen naar de WAN transport (VPN 0) interfaces waardoor SD-WAN routers verbinding maken met het onderliggende netwerk. Elke TLOC wordt uniek geïdentificeerd door een combinatie van het systeem IP-adres van de SD-WAN router, de kleur van de WAN-interface en de transportinsluiting (GRE of IPsec). Cisco Overlay Management Protocol (OMP) wordt gebruikt voor de distributie van TLOC’s (ook bekend als TLOC-routes), SD-

WAN overlay prefixes (ook bekend als OMP-routes) en andere informatie tussen SD-WAN routers. Het is via TLOC-routes dat SD-WAN routers weten hoe ze elkaar kunnen bereiken en IPsec VPN-tunnels met elkaar kunnen opzetten.

SD-WAN routers en/of controllers (vManager, vSmart of vBond) kunnen achter netwerkadresomzetting (NAT)-apparaten binnen het netwerk zitten. Wanneer een SD-WAN router authenticeert naar een vBond controller, leert de vBond controller zowel het privaat IP-adres/poortnummer als de openbare IP-adres/poortnummer-instellingen van de SD-WAN router op het moment van de uitwisseling. vBond controllers fungeren als Session Transversal Utilities voor NAT (STUN) servers en maken SD-WAN routers in staat om in kaart gebrachte en/of vertaalde IP-adressen en poortnummers van hun WAN-transportinterfaces te ontdekken.

Op SD-WAN routers wordt elk WAN-transport geassocieerd met een publiek en privaat IP-adrespaar. Het privé IP-adres wordt beschouwd als het pre-NAT-adres. Dit is het IP-adres dat is toegewezen aan de WAN-interface van de SD-WAN router. Hoewel dit wordt beschouwd als een privé IP-adres, kan dit IP-adres deel uitmaken van de openbare routeerbare IP-adresruimte of deel uitmaken van de IETF RFC 1918 niet-openbare routeerbare IP-adresruimte. Het openbare IP-adres wordt beschouwd als het post-NAT-adres. Dit wordt gedetecteerd door de vBond-server wanneer de SD-WAN router in eerste instantie communiceert en verificeert met de vBond-server. Het openbare IP-adres kan ook deel uitmaken van de niet-openbare routeerbare IP-adresruimte of van de IETF RFC 1918-adresruimte voor niet-openbare routeerbare IP-adressen. Bij gebrek aan NAT zijn zowel de openbare als de particuliere IP-adressen van de SD-WAN-transportinterface hetzelfde.

TLOC-kleuren zijn statisch gedefinieerde trefwoorden die worden gebruikt om individuele WAN-transporten op elke SD-WAN router te identificeren. Elk WAN-transport op een bepaalde SD-WAN router moet een unieke kleur hebben. De kleuren worden ook gebruikt om een individueel WAN vervoer als of openbaar of privé te identificeren. De kleuren metro-ethernett, Mpls, en private1, private2, private3, private4, private5 en private6 worden beschouwd als privé-kleuren. Zij zijn bedoeld voor gebruik in privé netwerken of plaatsen waar er geen NAT is. De kleuren zijn 3g, biz-internet, blauw, brons, custom1, custom2, custom3, standaard, goud, groen, lte, public-internet, rood en zilver worden beschouwd als publieke kleuren. Zij zijn bedoeld om in openbare netwerken of op plaatsen met openbare IP-adressering van de WAN-transportinterfaces te worden gebruikt, hetzij natief, hetzij door NAT.

De kleur dicteert het gebruik van privé of openbare IP-adressen wanneer deze communiceren via de besturings- en dataplanes. Wanneer twee SD-WAN routers proberen met elkaar te communiceren, beide gebruik WAN-transportinterfaces met privé-kleuren, probeert elke zijde om verbinding te maken met het privé IP-adres van de externe router. Als één of beide partijen openbare kleuren gebruiken, dan probeert elke partij om met het openbare IP adres van de verre router te verbinden. Een uitzondering hierop is wanneer de Site ID's van twee apparaten hetzelfde zijn. Wanneer de Site ID's hetzelfde zijn, maar de kleuren openbaar zijn, worden de privé IP-adressen gebruikt voor communicatie. Dit kan voorkomen voor SD-WAN routers die proberen te communiceren met een vManager of vSmart controller op dezelfde site. Merk op dat SD-WAN routers geen IPsec VPN-tunnels tussen elkaar opzetten wanneer ze dezelfde Site-ID’s hebben.

```
interface GigabitEthernet1 ip address dhcp client-id GigabitEthernet1 ip dhcp client default-
router distance 1 mtu 1500 ! interface GigabitEthernet1.1352 encapsulation dot1Q 1352 ip address
198.18.0.5 255.255.255.252 ip mtu 1496 ! interface Tunnel1 ip unnumbered GigabitEthernet1 tunnel
source GigabitEthernet1 tunnel mode sdwan ! interface Tunnel1352001 ip unnumbered
GigabitEthernet1.1352 tunnel source GigabitEthernet1.1352 tunnel mode sdwan ! ! sdwan interface
GigabitEthernet1 tunnel-interface encapsulation ipsec weight 1 color biz-internet allow-service
all ! ! interface GigabitEthernet1.1352 tunnel-interface encapsulation ipsec weight 1 color
```

```
private1 max-control-connections 0 allow-service all ! ! system system-ip 61.61.61.61 site-id 61
... ! DC-MP-CGW1#sh ip int bri GigabitEthernet1 162.43.145.3 YES DHCP up up
GigabitEthernet1.1352 198.18.0.5 YES other up up ... Tunnel1 162.43.145.3 YES TFTP up up
Tunnel1352001 198.18.0.5 YES TFTP up up DC-MP-CGW1# DC-MP-CGW1#sh sdwan bfd sessions | i
25.25.25.25 25.25.25.25 25 down biz-internet private1 162.43.145.3 10.211.1.89 12367 ipsec 7
1000 NA 0 25.25.25.25 25 up biz-internet private2 162.43.145.3 18.168.222.153 12387 ipsec 7 1000
10 0:09:34:05 0 25.25.25.25 25 up private1 private2 198.18.0.5 10.211.1.56 12387 ipsec 7 1000 10
0:09:33:17 0 25.25.25.25 25 down private1 private1 198.18.0.5 10.211.1.89 12367 ipsec 7 1000 NA
0 DC-MP-CGW1#
```

BGP-configuratie (border Gateway Protocol) op de datacenter SD-WAN router voor AWS Direct Connect:

```
router bgp 64513 neighbor 198.18.0.6 remote-as 64512 neighbor 198.18.0.6 description hosted-
connection neighbor 198.18.0.6 password
```

Data Center SD-WAN router leert IP Prefix 10.211.1.0/24 van SD-WAN Transit VPC. Het heeft AWS Direct Connect Router met het IP-adres 198.18.0.6 als volgende hop - zie hier regel 7:

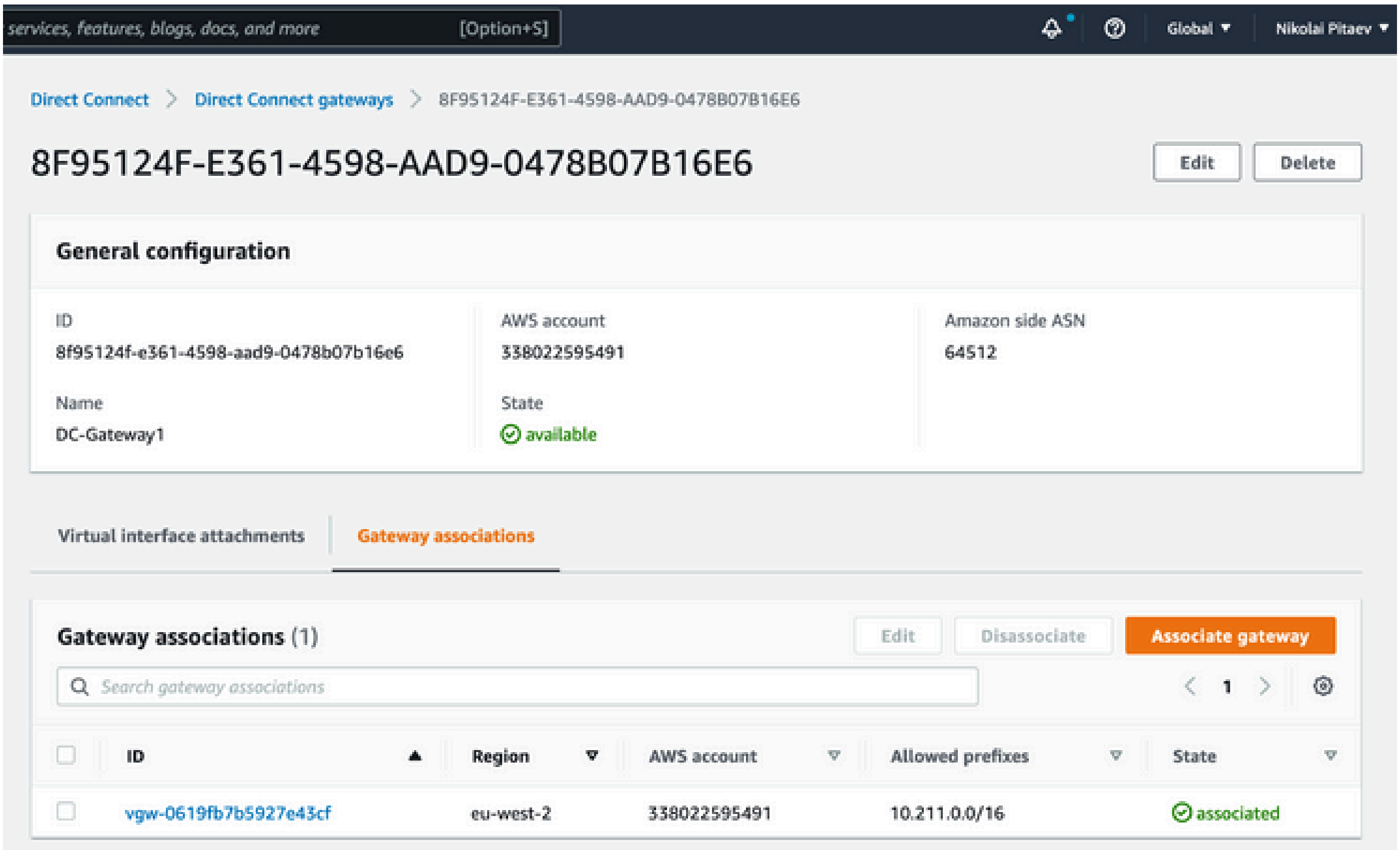
```
DC-MP-CGW1#sh ip ro ... Gateway of last resort is 162.43.145.2 to network 0.0.0.0 S* 0.0.0.0/0
[1/0] via 162.43.145.2 10.0.0.0/24 is subnetted, 1 subnets B 10.211.1.0 [20/0] via 198.18.0.6,
09:15:27 162.43.0.0/16 is variably subnetted, 2 subnets, 2 masks C 162.43.145.2/31 is directly
connected, GigabitEthernet1 L 162.43.145.3/32 is directly connected, GigabitEthernet1
198.18.0.0/24 is variably subnetted, 2 subnets, 2 masks C 198.18.0.4/30 is directly connected,
GigabitEthernet1.1352 L 198.18.0.5/32 is directly connected, GigabitEthernet1.1352 DC-MP-CGW1#s
```

Stap 3. Configuratie van AWS TVPC SD-WAN router

Beide SD-WAN routers in AWS Transit VPC zijn gemaakt met Cloud onRamp voor Multicloud Automation met standaard vManager-sjablonen. Beide c8kv routers gebruiken private2-kleur voor openbare internetconnectiviteit.

Stap 4. Configuratie AWS Direct Connect

VGW moet worden gecreëerd en gekoppeld aan SD-WAN transit VPC in de AWS-console of met een cloud automation tool. Dezelfde VGW moet worden gekoppeld aan Direct Connect zoals hier wordt getoond. Let op SD-WAN TVPC prefix 10.211.0.0/16 onder **toegestane prefixes**.


services, features, blogs, docs, and more [Option+S]
Global
Nikolai Pitaev

Direct Connect > Direct Connect gateways > 8F95124F-E361-4598-AAD9-0478B07B16E6

8F95124F-E361-4598-AAD9-0478B07B16E6

General configuration

ID 8f95124f-e361-4598-aad9-0478b07b16e6	AWS account 338022595491	Amazon side ASN 64512
Name DC-Gateway1	State ✓ available	

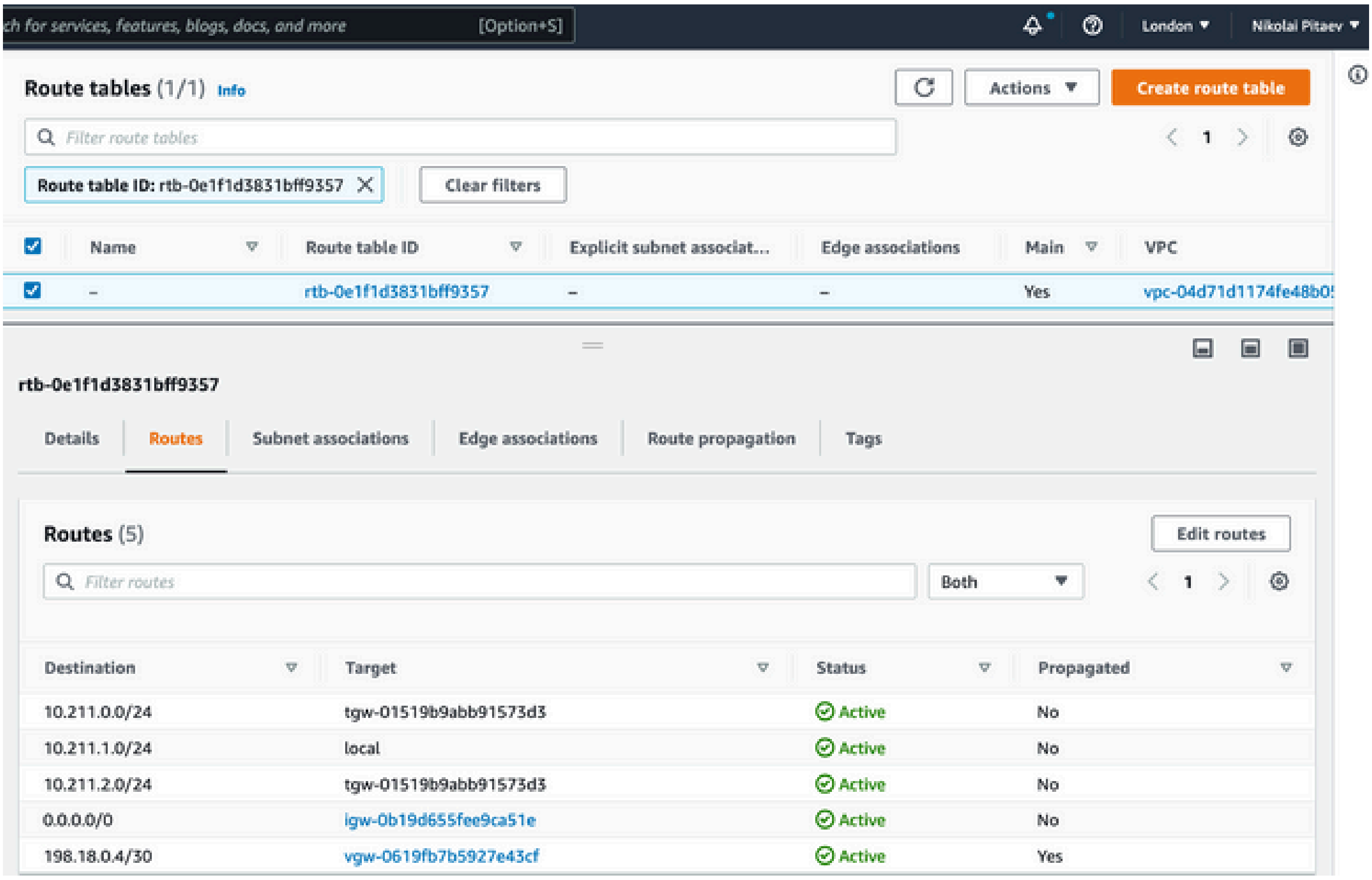
Virtual interface attachments
Gateway associations

Gateway associations (1)

Edit
Disassociate
Associate gateway
Search gateway associations
1

□	ID	Region	AWS account	Allowed prefixes	State
□	vgw-0619fb7b5927e43cf	eu-west-2	338022595491	10.211.0.0/16	✓ associated

De routedoorgifte voor de VGW moet zijn ingeschakeld in de AWS-routetabel voor de SD-WAN doorvoer VPC - zie de laatste route voor 198.18.0.4/30 in deze afbeelding. De routedoorgifte adverteert DC TLOC terug naar de Transit VPC-routetabel.



Route tables (1/1) Info

Route table ID: rtb-0e1f1d3831bff9357 ✕ Clear filters

☑	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
☑	–	rtb-0e1f1d3831bff9357	–	–	Yes	vpc-04d71d1174fe48b0!

rtb-0e1f1d3831bff9357

Routes (5)

Destination	Target	Status	Propagated
10.211.0.0/24	tgw-01519b9abb91573d3	✓ Active	No
10.211.1.0/24	local	✓ Active	No
10.211.2.0/24	tgw-01519b9abb91573d3	✓ Active	No
0.0.0.0/0	igw-0b19d655fee9ca51e	✓ Active	No
198.18.0.4/30	vgw-0619fb7b5927e43cf	✓ Active	Yes

De output van **show sdwan bfd sessies** CLI hier is genomen van een van c8kv SD-WAN routers in Transit VPC en toont twee SD-WAN tunnels:

1. De eerste tunnel (zie lijn 5) gaat via internet van c8kv in AWS TVPC naar Data Center: kleur private2 > biz-internet. Neem nota van het bestemmingsIP adres - het is het openbare IP adres 192.0.2.0 van de router van het Centrum van Gegevens - zie de routerconfiguratie in de vorige sectie.
2. De tweede tunnel (zie lijn 6) gaat via AWS Direct Connect: van kleur private2 naar private1 met 198.18.0.5 als IP-adres van bestemming.

```
DC-AWS-EU-CGW1#sh sdwan bfd sessions | i 61 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 ------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------------------ 61.61.61.61 61 up private2 biz-internet 10.211.1.56 162.43.145.3
12347 ipsec 7 1000 06:05:13 0 61.61.61.61 61 up private2 private1 10.211.1.56 198.18.0.5 12367
ipsec 7 1000 06:04:26 0 DC-AWS-EU-CGW1#
```

Beveiliging met firewall in gedeelde services (VPC) en AWS/GWLB

De inspectie van het oost-west- en het noord-zuidverkeer is een zeer algemeen vereiste. Normaal gesproken wordt elk verkeer tussen verschillende host-VPC's en/of SD-WAN VPN's onderworpen aan firewallinspectie. Virtuele firewalls die worden uitgevoerd in gedeelde services, VPC en taakverdeling kunnen worden geïmplementeerd met AWS Gateway Load Balancer (GWLB).

Het beschreven ontwerp werkt zeer goed met gecentraliseerde inspectie - zie .

Instellen voor concepttest

Deze afbeeldingen worden gebruikt om een testinstelling voor concepttest (PoC) te maken:

- vManager: 192.0.2.1R. Geen echte behoefte aan dit engineeringbeeld, moet het ook werken met 20.6
- c8kv voor AWS en Megaport (Direct Connect / Data Center simulation):17.4 of 17.5
- AWS Direct Connect werd gesimuleerd met Megaport

Direct Connect met SDCI Provider Megaport of Equinix

Het is niet eenvoudig om echte AWS Direct Connect te krijgen voor een labomgeving. Normaal vereist het een AWS Direct Connect-partner, wat kostbaar is en tijd kan vergen.

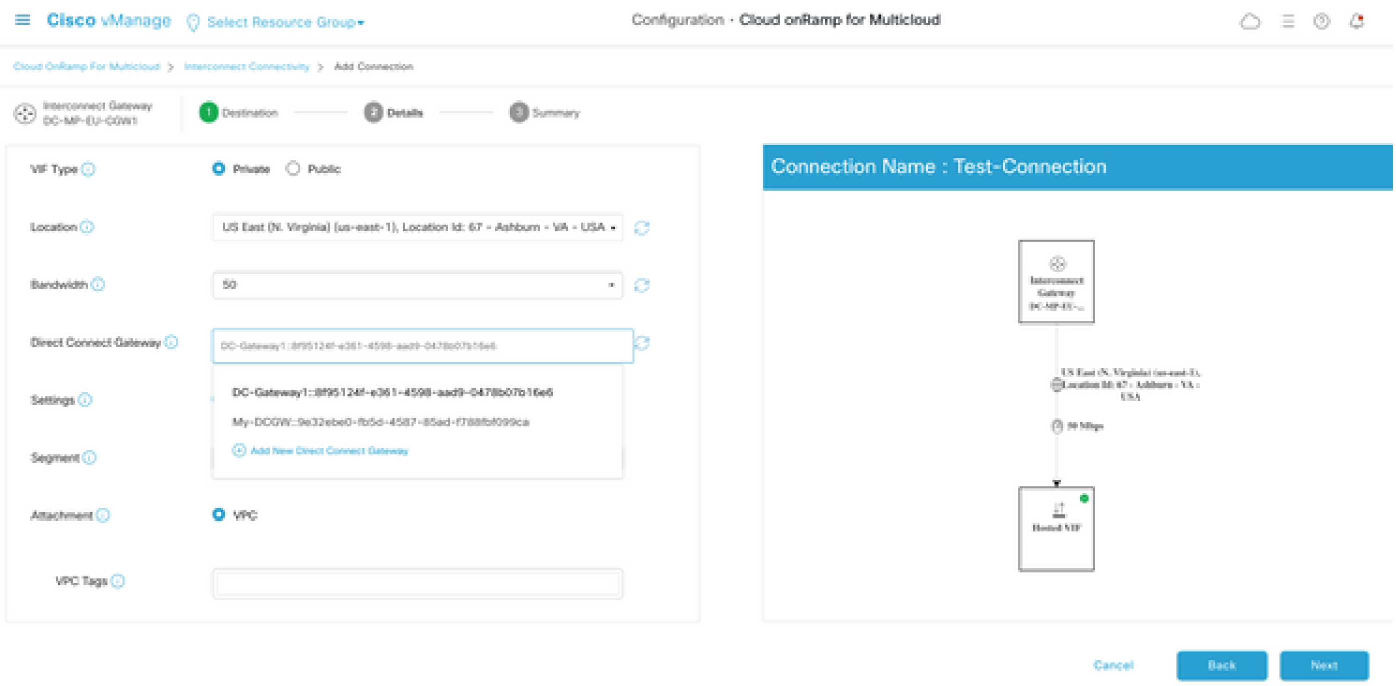
Als u echter een Megaport- of Equinix-account hebt, kunt u deze binnen enkele minuten gebruiken om een AWS Direct Connect Gateway te maken met Cisco Cloud onRamp voor Multicloud Automation!

Hier is een overzicht van de belangrijkste stappen, als u al uw softwaregedefinieerde datacenter Interconnect (SDCI) en AWS-referenties hebt geconfigureerd in vManager:

1. Als u nog geen twee c8kvs hebt die fungeren als Cloud Gateways in Transit VPC op AWS, gebruik dan Cloud onRamp (CoR) voor Multicloud workflow voor AWS en creëer het in de gewenste AWS regio met de standaard AWS CoR routersjabloon met elke private kleur.
2. In vManager, navigeer naar CoR voor Multicloud Interconnect configuratie en maak een Interconnect Gateway (c8kv) in de gewenste SDCI regio met de standaard SDCI provider routersjabloon.

3. Op de pagina van de Configuratie van de Interconnect van het CvdR Multicloud in vManager creeer een nieuw verbindingstype Cloud met Private Virtual Interface (VIF). Op het moment van deze configuratieworkflow hebt u de mogelijkheid om een nieuwe AWS Direct Connect Gateway te maken en er een host-VPC aan te koppelen. Dus, zorg ervoor dat u een "dummy" host VPC voor deze stap.
4. Voor de nieuwe c8kv gemaakt in Stap 2. switch van vManager-configuratiemodus naar de CLI-modus en verplaats de tunnel van de servicekant naar VPN0 (verwijder de vrf-voorwaartse instructie). Controleer de BGP-verbinding en zorg ervoor dat u de netwerkverklaring in de BGP-configuratie hebt: netwerk 198.18.0.4 masker 25.255.255.252. Zie de volledige routerconfiguratie voor datacenter en AWS-routers in bijlage.
5. Selecteer in de AWS Management Console de juiste VGW (of maak een nieuwe) en schakel routedoorgifte in de AWS Route Table-instellingen in. Zorg er ook voor dat u **Toegestane prefixes** hebt geconfigureerd in de sectie Direct Connect - raadpleeg de afbeelding later in dit hoofdstuk.

Deze afbeelding illustreert de Direct Connect-creatie uit Stap 3.:


Cisco vManage
Select Resource Group
Configuration · Cloud onRamp for Multicloud
Cloud OnRamp For Multicloud > Interconnect Connectivity > Add Connection
Interconnect Gateway
DC-MP-EU-CGW1
1 Destination
2 Details
3 Summary
Interconnect Gateway DC-MP-EU-...
US East (N. Virginia) (us-east-1), Location Id: 67 - Ashburn - VA - USA
50 Mbps
Hosted VIF
Add New Direct Connect Gateway
Cancel
Back
Next

VIF Type: ● Private ○ Public

Location: US East (N. Virginia) (us-east-1), Location Id: 67 - Ashburn - VA - USA

Bandwidth: 50

Direct Connect Gateway: DC-Gateway1::8f95124f-e361-4598-aad9-0478b07b16e6

DC-Gateway1::8f95124f-e361-4598-aad9-0478b07b16e6

My-DCGW::9e32ebe0-fb5d-4587-85ad-f788fbf099ca

Settings

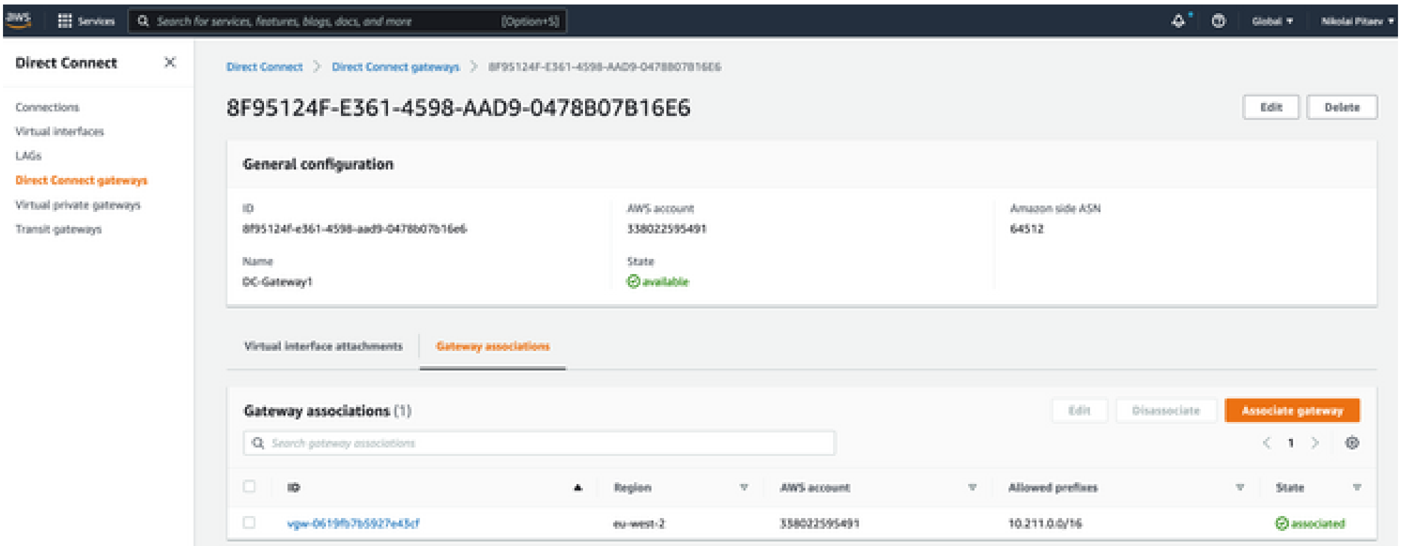
Segment

Attachment: ● VPC

VPC Tags

Connection Name : Test-Connection

Als eindresultaat ziet u een nieuwe Direct Connect Gateway in uw AWS Management Console zoals hier getoond. Let op het veld Toegestane prefixes, dat het CIDR-blok van de transit SD-WAN VPC heeft.



8F95124F-E361-4598-AAD9-0478B07B16E6

General configuration

ID
8f95124f-e361-4598-aad9-0478b07b16e6

Name
DC-Gateway1

AWS account
338022595491

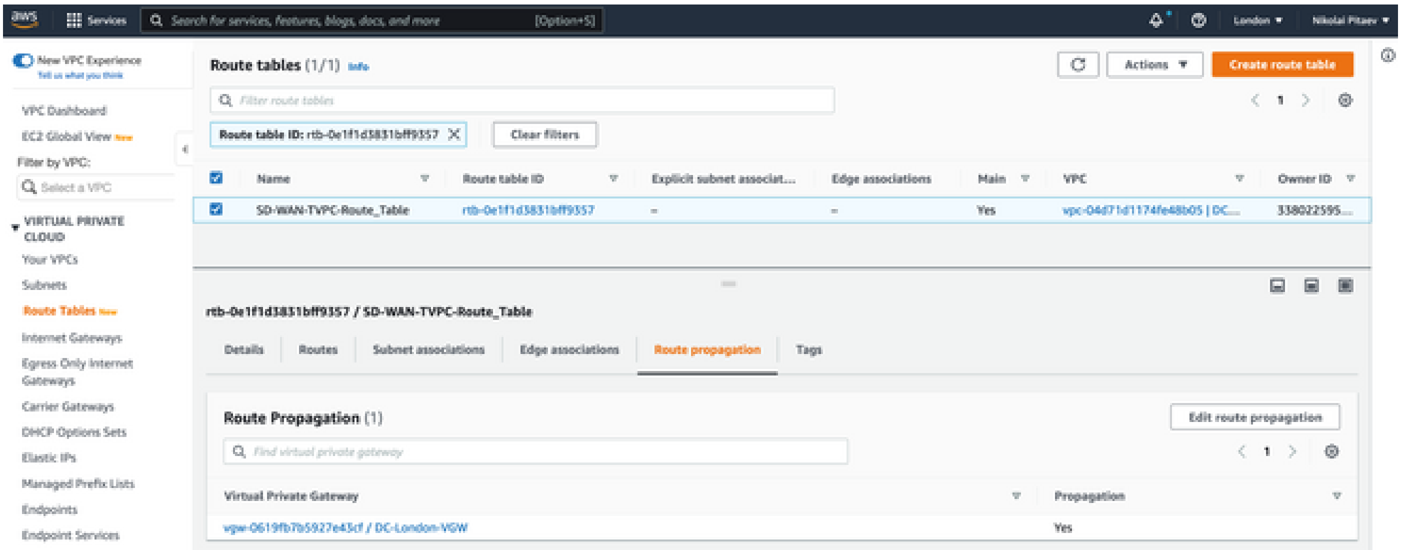
State
available

Amazon side ASN
64512

Gateway associations (1)

☐	ID	Region	AWS account	Allowed prefixes	State
☐	vgw-0619fb7b5927e43cf	eu-west-2	338022595491	10.211.0.0/16	associated

Dubbelcontroleer de routetabel voor de SD-WAN transit VPC. Het moet een voortplanting hebben waarbij de juiste VGW ingeschakeld is zoals in de afbeelding.



Route tables (1/1)

Route table ID: rtb-0e1f1d3831bff9357

☑	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
☑	SD-WAN-TVPC-Route_Table	rtb-0e1f1d3831bff9357	–	–	Yes	vpc-04d71d1174fe48b05 | DC...	338022595...

rtb-0e1f1d3831bff9357 / SD-WAN-TVPC-Route_Table

Route Propagation (1)

Virtual Private Gateway	Propagation
vgw-0619fb7b5927e43cf / DC-London-VGW	Yes

Raadpleeg deze sectie voor de volledige routerconfiguratie en toon de uitgangen.

```
DC-MP-CGW1#sh sdwan running-config
system
location "14 Coriander Avenue, London, -E14 2AA, United Kingdom"
gps-location latitude 51.51155
gps-location longitude -0.002916
system-ip 192.0.2.2
overlay-id 1
site-id 61
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 192.0.2.3 port 12346
!
```

```
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname DC-MP-CGW1
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
speed 10000
no negotiation auto
exit
interface GigabitEthernet1.1352
no shutdown
encapsulation dot1Q 1352
ip address 198.18.0.5 255.255.255.252
no ip redirects
ip mtu 1496
exit
interface Loopback100
no shutdown
vrf forwarding 10
ip address 192.168.7.7 255.255.255.255
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 Tunnel1352001
no shutdown
```

```
ip unnumbered GigabitEthernet1.1352
ipv6 unnumbered GigabitEthernet1.1352
tunnel source GigabitEthernet1.1352
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
neighbor 198.18.0.6 remote-as 64512
neighbor 198.18.0.6 description hosted-connection
neighbor 198.18.0.6 password 7 072A02687E243C2A4545322B2A0B12077E1961123F
address-family ipv4 unicast
neighbor 198.18.0.6 activate
neighbor 198.18.0.6 send-community both
network 198.18.0.4 mask 255.255.255.252
exit-address-family
!
!
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 GigabitEthernet1.1352
tunnel-interface
encapsulation ipsec 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
!

DC-MP-CGW1#
DC-MP-CGW1#
DC-MP-CGW1#
DC-MP-CGW1#
DC-MP-CGW1#sh run
Building configuration...

Current configuration : 4679 bytes
!
! Last configuration change at 18:06:53 UTC Fri Dec 10 2021 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 DC-MP-CGW1
!
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-1684160503
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1684160503
revocation-check none
rsakeypair TP-self-signed-1684160503
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-1684160503
crypto pki certificate chain SLA-TrustPoint
!
!
!
!
!
!
!
!
license udi pid C8000V sn 9FTTYDEBR7O
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 Loopback100
vrf forwarding 10
ip address 192.168.7.7 255.255.255.255
!
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 Tunnel1352001
ip unnumbered GigabitEthernet1.1352
ipv6 unnumbered GigabitEthernet1.1352
tunnel source GigabitEthernet1.1352
tunnel mode sdwan
!
interface GigabitEthernet1
ip dhcp client default-router distance 1
ip address dhcp client-id GigabitEthernet1
no ip redirects
load-interval 30
speed 10000
no negotiation auto
arp timeout 1200
!
interface GigabitEthernet1.1352
encapsulation dot1Q 1352
ip address 198.18.0.5 255.255.255.252
no ip redirects
ip mtu 1496
arp timeout 1200
!
router omp
!
router bgp 64513
bgp log-neighbor-changes
neighbor 198.18.0.6 remote-as 64512
neighbor 198.18.0.6 description hosted-connection
neighbor 198.18.0.6 password 7 072A02687E243C2A4545322B2A0B12077E1961123F
!
address-family ipv4
network 198.18.0.4 mask 255.255.255.252
neighbor 198.18.0.6 activate
neighbor 198.18.0.6 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

DC-MP-CGW1#
```

```
DC-MP-CGW1#
DC-MP-CGW1#sh ip ro
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 192.0.2.4 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.0.2.4
10.0.0.0/24 is subnetted, 1 subnets
B 10.211.1.0 [20/0] via 198.18.0.6, 3d07h
192.0.2.5/16 is variably subnetted, 2 subnets, 2 masks
C 192.0.2.4/31 is directly connected, GigabitEthernet1
L 192.0.2.0/32 is directly connected, GigabitEthernet1
198.18.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 198.18.0.4/30 is directly connected, GigabitEthernet1.1352
L 198.18.0.5/32 is directly connected, GigabitEthernet1.1352
DC-MP-CGW1#
DC-MP-CGW1#
DC-MP-CGW1#sh sdw
DC-MP-CGW1#sh sdwan bfd sess
DC-MP-CGW1#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
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
------------------
192.0.2.6 64 up biz-internet private2 192.0.2.0 192.0.2.7 12387 ipsec 7 1000 10 3:06:56:39 0
192.0.2.8 65 down biz-internet private1 192.0.2.0 10.211.0.68 12367 ipsec 7 1000 NA 0
192.0.2.9 65 down biz-internet private1 192.0.2.0 10.211.0.180 12367 ipsec 7 1000 NA 0
192.0.2.10 25 down biz-internet private1 192.0.2.0 10.211.1.89 12367 ipsec 7 1000 NA 0
192.0.2.11 25 down biz-internet private1 192.0.2.0 10.211.1.184 12367 ipsec 7 1000 NA 0
192.0.2.6 64 down biz-internet private1 192.0.2.0 10.211.2.76 12367 ipsec 7 1000 NA 0
192.0.2.24 64 down biz-internet private1 192.0.2.0 10.211.2.176 12367 ipsec 7 1000 NA 0
10.11.1.11 11 up biz-internet public-internet 192.0.2.0 192.0.2.13 12386 ipsec 7 1000 10
3:07:48:35 0
10.12.1.11 12 up biz-internet public-internet 192.0.2.0 192.0.2.14 12386 ipsec 7 1000 10
2:08:51:12 1
192.0.2.10 25 up biz-internet private2 192.0.2.0 192.0.2.15 12387 ipsec 7 1000 10 3:06:56:35 0
192.0.2.24 64 up biz-internet private2 192.0.2.0 192.0.2.16 12387 ipsec 7 1000 10 3:06:56:40 0
192.0.2.11 25 up biz-internet private2 192.0.2.0 192.0.2.17 12387 ipsec 7 1000 10 3:06:56:35 0
10.103.1.11 103 up biz-internet default 192.0.2.0 192.0.2.18 12346 ipsec 7 1000 10 3:07:48:35 0
10.103.1.12 103 up biz-internet default 192.0.2.0 192.0.2.19 12346 ipsec 7 1000 10 3:07:48:35 0
192.0.2.9 65 up biz-internet public-internet 192.0.2.0 192.0.2.20 12347 ipsec 7 1000 10
3:07:48:35 0
192.0.2.8 65 up biz-internet public-internet 192.0.2.0 192.0.2.21 12347 ipsec 7 1000 10
3:07:48:35 0
192.0.2.8 65 down private1 private1 198.18.0.5 10.211.0.68 12367 ipsec 7 1000 NA 0
192.0.2.9 65 down private1 private1 198.18.0.5 10.211.0.180 12367 ipsec 7 1000 NA 0
192.0.2.10 25 up private1 private2 198.18.0.5 10.211.1.56 12387 ipsec 7 1000 10 3:06:55:47 0
192.0.2.10 25 down private1 private1 198.18.0.5 10.211.1.89 12367 ipsec 7 1000 NA 0
192.0.2.11 25 up private1 private2 198.18.0.5 10.211.1.155 12387 ipsec 7 1000 10 0:15:27:22 1
192.0.2.11 25 down private1 private1 198.18.0.5 10.211.1.184 12367 ipsec 7 1000 NA 0
192.0.2.6 64 down private1 private2 198.18.0.5 10.211.2.41 12387 ipsec 7 1000 NA 0
```

```
192.0.2.6 64 down private1 private1 198.18.0.5 10.211.2.76 12367 ipsec 7 1000 NA 0
192.0.2.24 64 down private1 private2 198.18.0.5 10.211.2.154 12387 ipsec 7 1000 NA 0
192.0.2.24 64 down private1 private1 198.18.0.5 10.211.2.176 12367 ipsec 7 1000 NA 0
10.11.1.11 11 down private1 public-internet 198.18.0.5 192.0.2.13 12386 ipsec 7 1000 NA 0
10.12.1.11 12 down private1 public-internet 198.18.0.5 192.0.2.14 12386 ipsec 7 1000 NA 0
10.103.1.11 103 down private1 default 198.18.0.5 192.0.2.18 12346 ipsec 7 1000 NA 0
10.103.1.12 103 down private1 default 198.18.0.5 192.0.2.19 12346 ipsec 7 1000 NA 0
192.0.2.9 65 down private1 public-internet 198.18.0.5 192.0.2.20 12347 ipsec 7 1000 NA 0
192.0.2.8 65 down private1 public-internet 198.18.0.5 192.0.2.21 12347 ipsec 7 1000 NA 0

DC-MP-CGW1#
DC-MP-CGW1#
DC-MP-CGW1#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

DC-MP-CGW1 uptime is 3 days, 7 hours, 51 minutes
Uptime for this control processor is 3 days, 7 hours, 53 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 9FTTYDEBR7O
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

DC-MP-CGW1#

DC-AWS-EU-CGW1#sh sdwan running-config
system
location "Europe (London)"
gps-location latitude 51.507321
gps-location longitude 0.127647
system-ip 192.0.2.10
overlay-id 1
site-id 25
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 192.0.2.3 port 12346
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname DC-AWS-EU-CGW1
username admin privilege 15 secret 9
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
vrf definition 10
rd 1:10
address-family ipv4
route-target export 64550:10
route-target import 64550:10
exit-address-family
!
address-family ipv6
exit-address-family
!
!
vrf definition Mgmt-intf
description Management
rd 1:512
address-family ipv4
route-target export 64550:512
route-target import 64550:512
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
ip as-path access-list 15 permit ^645[2-4][0-9]$
ip as-path access-list 25 permit .*
no ip dhcp use class
ip route 10.211.0.0 255.255.255.0 10.211.1.65
ip route 10.211.2.0 255.255.255.0 10.211.1.65
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
vrf forwarding Mgmt-intf
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 GigabitEthernet2
no shutdown
arp timeout 1200
ip address dhcp client-id GigabitEthernet2
no ip redirects
ip dhcp client default-router distance 1
ip mtu 1500
load-interval 30
mtu 1500
negotiation auto
exit
interface GigabitEthernet3
no shutdown
arp timeout 1200
ip address dhcp client-id GigabitEthernet3
no ip redirects
ip dhcp client default-router distance 20
ip mtu 1500
load-interval 30
mtu 1500
exit
interface Tunnel2
no shutdown
ip unnumbered GigabitEthernet2
no ip redirects
ipv6 unnumbered GigabitEthernet2
no ipv6 redirects
tunnel source GigabitEthernet2
tunnel mode sdwan
exit
interface Tunnel3
no shutdown
ip unnumbered GigabitEthernet3
no ip redirects
```

```
ipv6 unnumbered GigabitEthernet3
no ipv6 redirects
tunnel source GigabitEthernet3
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
vrf forwarding 10
ip address 169.254.0.22 255.255.255.252
ip mtu 1500
tunnel source 10.211.1.56
tunnel destination 192.0.2.22
tunnel mode ipsec ipv4
tunnel path-mtu-discovery
tunnel protection ipsec profile if-ipsec1-ipsec-profile
exit
interface Tunnel100002
no shutdown
vrf forwarding 10
ip address 169.254.0.26 255.255.255.252
ip mtu 1500
tunnel source 10.211.1.56
tunnel destination 192.0.2.23
tunnel mode ipsec ipv4
tunnel path-mtu-discovery
tunnel protection ipsec profile if-ipsec2-ipsec-profile
exit
route-map AWS_TGW_CSR_ROUTE_POLICY deny 1
match as-path 15
!
route-map AWS_TGW_CSR_ROUTE_POLICY permit 11
match as-path 25
!
route-map AWS_TGW_CSR_ROUTE_POLICY deny 65535
!
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
no logging monitor
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
port 1700
!
crypto ipsec transform-set if-ipsec1-ikev1-transform esp-aes 256 esp-sha-hmac
mode tunnel
!
crypto ipsec transform-set if-ipsec2-ikev1-transform esp-aes 256 esp-sha-hmac
mode tunnel
!
crypto ipsec profile if-ipsec1-ipsec-profile
set isakmp-profile if-ipsec1-ikev1-isakmp-profile
set pfs group2
set transform-set if-ipsec1-ikev1-transform
set security-association lifetime kilobytes disable
set security-association lifetime seconds 3600
set security-association replay window-size 512
!
crypto ipsec profile if-ipsec2-ipsec-profile
set isakmp-profile if-ipsec2-ikev1-isakmp-profile
set pfs group2
set transform-set if-ipsec2-ikev1-transform
set security-association lifetime kilobytes disable
set security-association lifetime seconds 3600
set security-association replay window-size 512
!
crypto keyring if-ipsec1-ikev1-keyring
pre-shared-key address 192.0.2.22 key qOWzTrRGM95OOa8j35VT7eQRMmzgHCEq
!
crypto keyring if-ipsec2-ikev1-keyring
pre-shared-key address 192.0.2.23 key E4cayBdglWSBUaaDi1ukyngzbUzUP8Hp
!
crypto isakmp aggressive-mode disable
crypto isakmp keepalive 10 3 on-demand
crypto isakmp policy 1
authentication pre-share
encryption aes 128
group 2
hash sha
lifetime 28800
!
crypto isakmp policy 2
authentication pre-share
encryption aes 128
group 2
hash sha
lifetime 28800
!
crypto isakmp profile if-ipsec1-ikev1-isakmp-profile
keyring if-ipsec1-ikev1-keyring
match identity address 192.0.2.22 255.255.255.255
!
crypto isakmp profile if-ipsec2-ikev1-isakmp-profile
keyring if-ipsec2-ikev1-keyring
match identity address 192.0.2.23 255.255.255.255
!
router bgp 64550
bgp log-neighbor-changes
address-family ipv4 unicast vrf 10
distance bgp 20 200 20
maximum-paths eibgp 2
neighbor 169.254.0.21 remote-as 64521
neighbor 169.254.0.21 activate
neighbor 169.254.0.21 ebgp-multihop 255
neighbor 169.254.0.21 route-map AWS_TGW_CSR_ROUTE_POLICY out
neighbor 169.254.0.21 send-community both
neighbor 169.254.0.25 remote-as 64521
neighbor 169.254.0.25 activate
neighbor 169.254.0.25 ebgp-multihop 255
neighbor 169.254.0.25 route-map AWS_TGW_CSR_ROUTE_POLICY out
neighbor 169.254.0.25 send-community both
propagate-aspath
redistribute omp
exit-address-family
!
timers bgp 60 180
!
snmp-server ifindex persist
line aux 0
stopbits 1
!
line con 0
login authentication default
speed 19200
stopbits 1
!
line vty 0 4
login authentication default
```

```
transport input ssh
!
line vty 5 80
login authentication default
transport input ssh
!
lldp run
nat64 translation timeout tcp 3600
nat64 translation timeout udp 300
sdwan
interface GigabitEthernet2
tunnel-interface
encapsulation ipsec weight 1
no border
color private2
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 GigabitEthernet3
tunnel-interface
encapsulation ipsec weight 1
no border
color private1
no last-resort-circuit
no low-bandwidth-link
max-control-connections 0
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
hello-tolerance 12
no allow-service all
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
!
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
authentication-type ah-sha1-hmac sha1-hmac
!
!
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
!
policy
no app-visibility
no app-visibility-ipv6
no flow-visibility
no flow-visibility-ipv6
no implicit-acl-logging
log-frequency 1000
!

DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#sh run
DC-AWS-EU-CGW1#sh running-config
Building configuration...

Current configuration : 11607 bytes
!
! Last configuration change at 18:26:47 UTC Fri Dec 10 2021 by NETCONF
!
version 17.4
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 DC-AWS-EU-CGW1
!
boot-start-marker
boot-end-marker
!
!
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 64550:10
route-target import 64550:10
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition 65528
!
address-family ipv4
exit-address-family
!
vrf definition Mgmt-intf
description Management
rd 1:512
!
address-family ipv4
route-target export 64550:512
route-target import 64550:512
exit-address-family
!
```

```
address-family ipv6
exit-address-family
!
logging buffered 512000
logging persistent size 104857600 filesize 10485760
no logging rate-limit
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-1070810043
enrollment selfsigned
```

```
subject-name cn=IOS-Self-Signed-Certificate-1070810043
revocation-check none
rsakeypair TP-self-signed-1070810043
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-1070810043
certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31303730 38313030 3433301E 170D3231 31323130 30303339
34325A17 0D333131 32313030 30333934 325A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 30373038
31303034 33308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100AC49 2292437D CC1AB211 204B33F2 9AE40F1B A41355FA 9832FD65
69C4FDCD 57AEE5A1 5D30B8A8 F62C842E 487D9AD4 EF2E5F55 4C26D746 EA381D42
C4F259DA 19CFDE22 76582EAD 1C878CE7 B596E439 94EF0023 D0B0A1EC C79D582C
43DC3116 350675F7 6B42B33F DF500EF0 323ECFBD A0FBD612 8ABFD343 96C8BB40
330697C0 4BB5DE18 39DB9203 C5132855 5FE5C0C6 80635F69 9DA90B4F 578F7861
81F5AD28 C1732F99 CCE788FB 0F8EA20A 29E2A57B 6879AAE9 9CAAF05C 9F6D95FD
F114EA04 5ADE11C7 C8C93379 3FA8CA0F 5E3ADEFE 61197C3E DBC20084 2F0B1BF9
9A1CFC95 730AAE31 CACE6EE8 D0DABFE1 B995B6C0 0C072343 CA115DC4 5A802A21
256C3291 22370203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 149E76BD 12EAD2B9 9F58797A 7A93625C 7ABB6953
C4301D06 03551D0E 04160414 9E76BD12 EAD2B99F 58797A7A 93625C7A BB6953C4
300D0609 2A864886 F70D0101 05050003 82010100 12D28F08 C5367501 E131A43F
A102433E 9E2C22AA 403FEAAE 311CEC4D 37353098 C9EAF160 C46C95C1 61073D63
B41F9191 2567CA23 C069E365 96DC55CD 368D9E1D 7A9B39B9 060BB27E AB456414
3DDEB3B9 1398C49B 570839FA BB090B72 5D51E6FE 8250A8D0 299DCD04 22168D8A
9EF3F9DF 58A9C3FC 1DB848FA 32089028 A88AA158 52E05BBF EA13129F C902E11F
96D23BDA EFEC8521 F8566815 ED2D703F 2B7E64B8 53A9799B 93DFF82D 7713A7A3
4FF271E8 B438678E 2A1706CE F9EE665C 40B9C1B5 7AC51491 B3327948 4B432168
2F2F46D2 E8B14961 69976E15 95A07771 756AF6AA F090B4DD BE41A10E C22A6611
008A2D16 C7751721 CF90413A 29019B95 DC7704EA
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
```

```
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
!
!
!
!
!
!
license udi pid C8000V sn 9SAQCJXHS8G
license boot level network-premier+dna-premier
diagnostic bootup level minimal
memory free low-watermark processor 226459
!
!
spanning-tree extend system-id
!
username admin privilege 15 secret 9
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
!
redundancy
!
!
!
!
no crypto ikev2 diagnose error
!
!
lldp run
cdp run
!
!
crypto keyring if-ipsec1-ikev1-keyring
pre-shared-key address 192.0.2.22 key qOWzTrRGM95OOa8j35VT7eQRMmzgHCEq
crypto keyring if-ipsec2-ikev1-keyring
pre-shared-key address 192.0.2.23 key E4cayBdglWSBUaaDi1ukyngzbUzUP8Hp
!
!
!
!
!
!
!
crypto isakmp policy 1
encryption aes
authentication pre-share
group 2
lifetime 28800
!
crypto isakmp policy 2
encryption aes
authentication pre-share
group 2
lifetime 28800
crypto isakmp keepalive 10 3
crypto isakmp aggressive-mode disable
crypto isakmp profile if-ipsec1-ikev1-isakmp-profile
keyring if-ipsec1-ikev1-keyring
match identity address 192.0.2.22 255.255.255.255
crypto isakmp profile if-ipsec2-ikev1-isakmp-profile
keyring if-ipsec2-ikev1-keyring
match identity address 192.0.2.23 255.255.255.255
```

```
!
!
crypto ipsec transform-set if-ipsec1-ikev1-transform esp-aes 256 esp-sha-hmac
mode tunnel
crypto ipsec transform-set if-ipsec2-ikev1-transform esp-aes 256 esp-sha-hmac
mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set if-ipsec1-ikev1-transform
set pfs group2
set isakmp-profile if-ipsec1-ikev1-isakmp-profile
!
crypto ipsec profile if-ipsec2-ipsec-profile
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set if-ipsec2-ikev1-transform
set pfs group2
set isakmp-profile if-ipsec2-ikev1-isakmp-profile
!
!
!
!
!
!
!
!
!
interface Loopback65528
vrf forwarding 65528
ip address 192.168.1.1 255.255.255.255
!
interface Tunnel2
ip unnumbered GigabitEthernet2
no ip redirects
ipv6 unnumbered GigabitEthernet2
no ipv6 redirects
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface Tunnel3
ip unnumbered GigabitEthernet3
no ip redirects
ipv6 unnumbered GigabitEthernet3
no ipv6 redirects
tunnel source GigabitEthernet3
tunnel mode sdwan
!
interface Tunnel100001
vrf forwarding 10
ip address 169.254.0.22 255.255.255.252
ip mtu 1500
tunnel source 10.211.1.56
tunnel mode ipsec ipv4
tunnel destination 192.0.2.22
tunnel path-mtu-discovery
tunnel protection ipsec profile if-ipsec1-ipsec-profile
!
interface Tunnel100002
vrf forwarding 10
ip address 169.254.0.26 255.255.255.252
ip mtu 1500
```

```
tunnel source 10.211.1.56
tunnel mode ipsec ipv4
tunnel destination 192.0.2.23
tunnel path-mtu-discovery
tunnel protection ipsec profile if-ipsec2-ipsec-profile
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
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 GigabitEthernet2
ip dhcp client default-router distance 1
ip address dhcp client-id GigabitEthernet2
no ip redirects
load-interval 30
negotiation auto
arp timeout 1200
!
interface GigabitEthernet3
ip dhcp client default-router distance 20
ip address dhcp client-id GigabitEthernet3
no ip redirects
load-interval 30
speed 1000
no negotiation auto
arp timeout 1200
!
router omp
!
router bgp 64550
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
redistribute omp
propagate-aspath
neighbor 169.254.0.21 remote-as 64521
neighbor 169.254.0.21 ebgp-multihop 255
neighbor 169.254.0.21 activate
neighbor 169.254.0.21 send-community both
neighbor 169.254.0.21 route-map AWS_TGW_CSR_ROUTE_POLICY out
neighbor 169.254.0.25 remote-as 64521
neighbor 169.254.0.25 ebgp-multihop 255
neighbor 169.254.0.25 activate
neighbor 169.254.0.25 send-community both
neighbor 169.254.0.25 route-map AWS_TGW_CSR_ROUTE_POLICY out
maximum-paths eibgp 2
distance bgp 20 200 20
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip as-path access-list 15 permit ^645[2-4][0-9]$
ip as-path access-list 25 permit .*
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 route 10.211.0.0 255.255.255.0 10.211.1.65
ip route 10.211.2.0 255.255.255.0 10.211.1.65
ip scp server enable
!
!
!
route-map AWS_TGW_CSR_ROUTE_POLICY deny 1
match as-path 15
!
route-map AWS_TGW_CSR_ROUTE_POLICY permit 11
match as-path 25
!
route-map AWS_TGW_CSR_ROUTE_POLICY deny 65535
!
!
!
!
!
!
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

DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#sh ip ro
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 10.211.1.33 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.211.1.33
10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S 10.211.0.0/24 [1/0] via 10.211.1.65
C 10.211.1.32/27 is directly connected, GigabitEthernet2
L 10.211.1.56/32 is directly connected, GigabitEthernet2
C 10.211.1.64/27 is directly connected, GigabitEthernet3
L 10.211.1.89/32 is directly connected, GigabitEthernet3
S 10.211.2.0/24 [1/0] via 10.211.1.65
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#sh ip ro vrf 10

Routing Table: 10
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 not set

10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
m 10.11.3.0/24 [251/0] via 10.11.1.11, 3d07h, Sdwan-system-intf
m 10.12.3.0/24 [251/0] via 10.12.1.11, 3d07h, Sdwan-system-intf
m 10.12.10.11/32 [251/0] via 10.12.1.11, 3d07h, Sdwan-system-intf
B 10.25.0.0/16 [20/100] via 169.254.0.25, 3d14h
[20/100] via 169.254.0.21, 3d14h
```

```
m 10.64.0.0/16 [251/0] via 192.0.2.24, 3d07h, Sdwan-system-intf
[251/0] via 192.0.2.6, 3d07h, Sdwan-system-intf
m 10.103.0.0/16 [251/0] via 10.103.1.11, 3d07h, Sdwan-system-intf
m 10.111.0.0/16 [251/0] via 10.103.1.11, 3d07h, Sdwan-system-intf
m 10.112.0.0/16 [251/0] via 10.103.1.11, 3d07h, Sdwan-system-intf
m 10.131.0.0/16 [251/0] via 192.0.2.9, 15:30:32, Sdwan-system-intf
[251/0] via 192.0.2.8, 15:30:32, Sdwan-system-intf
169.254.0.0/16 is variably subnetted, 13 subnets, 3 masks
m 169.254.0.4/30 [251/0] via 192.0.2.8, 2d18h, Sdwan-system-intf
m 169.254.0.8/30 [251/0] via 192.0.2.8, 3d07h, Sdwan-system-intf
m 169.254.0.12/30 [251/0] via 192.0.2.9, 15:30:32, Sdwan-system-intf
m 169.254.0.16/30 [251/0] via 192.0.2.9, 15:30:32, Sdwan-system-intf
C 169.254.0.20/30 is directly connected, Tunnel100001
L 169.254.0.22/32 is directly connected, Tunnel100001
C 169.254.0.24/30 is directly connected, Tunnel100002
L 169.254.0.26/32 is directly connected, Tunnel100002
m 169.254.0.36/30 [251/0] via 192.0.2.6, 3d07h, Sdwan-system-intf
m 169.254.0.40/30 [251/0] via 192.0.2.6, 3d07h, Sdwan-system-intf
m 169.254.0.44/30 [251/0] via 192.0.2.24, 3d07h, Sdwan-system-intf
m 169.254.0.48/30 [251/0] via 192.0.2.24, 3d07h, Sdwan-system-intf
m 169.254.10.0/29 [251/0] via 10.103.1.11, 3d07h, Sdwan-system-intf
192.168.7.0/32 is subnetted, 1 subnets
m 192.168.7.7 [251/0] via 192.0.2.2, 3d06h, Sdwan-system-intf
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#sh sdwa
DC-AWS-EU-CGW1#sh sdwan bfd
DC-AWS-EU-CGW1#sh sdwan bfd sess
DC-AWS-EU-CGW1#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
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------
192.0.2.8 65 up private2 private1 10.211.1.56 10.211.0.68 12367 ipsec 7 1000 07:00:18 0
192.0.2.9 65 up private2 private1 10.211.1.56 10.211.0.180 12367 ipsec 7 1000 07:00:17 0
192.0.2.6 64 up private2 private2 10.211.1.56 10.211.2.41 12387 ipsec 7 1000 07:00:18 0
192.0.2.6 64 up private2 private1 10.211.1.56 10.211.2.76 12367 ipsec 7 1000 07:00:18 0
192.0.2.24 64 up private2 private2 10.211.1.56 10.211.2.154 12387 ipsec 7 1000 15:30:40 1
192.0.2.24 64 up private2 private1 10.211.1.56 10.211.2.176 12367 ipsec 7 1000 07:00:18 0
10.11.1.11 11 up private2 public-internet 10.211.1.56 192.0.2.13 12386 ipsec 7 1000 07:00:17 0
10.12.1.11 12 up private2 public-internet 10.211.1.56 192.0.2.14 12386 ipsec 7 1000 07:00:17 0
10.103.1.11 103 up private2 default 10.211.1.56 192.0.2.18 12346 ipsec 7 1000 07:00:18 0
10.103.1.12 103 up private2 default 10.211.1.56 192.0.2.19 12346 ipsec 7 1000 07:00:17 0
192.0.2.9 65 up private2 public-internet 10.211.1.56 192.0.2.20 12347 ipsec 7 1000 15:30:41 1
192.0.2.8 65 up private2 public-internet 10.211.1.56 192.0.2.21 12347 ipsec 7 1000 07:00:18 0
192.0.2.2 61 up private2 biz-internet 10.211.1.56 192.0.2.0 12347 ipsec 7 1000 07:00:18 0
192.0.2.2 61 up private2 private1 10.211.1.56 198.18.0.5 12367 ipsec 7 1000 06:59:31 0
192.0.2.8 65 up private1 private1 10.211.1.89 10.211.0.68 12367 ipsec 7 1000 22:50:11 2
192.0.2.9 65 up private1 private1 10.211.1.89 10.211.0.180 12367 ipsec 7 1000 22:50:16 2
192.0.2.6 64 up private1 private2 10.211.1.89 10.211.2.41 12387 ipsec 7 1000 07:00:22 0
192.0.2.6 64 up private1 private1 10.211.1.89 10.211.2.76 12367 ipsec 7 1000 22:50:01 2
192.0.2.24 64 up private1 private2 10.211.1.89 10.211.2.154 12387 ipsec 7 1000 07:00:23 0
192.0.2.24 64 up private1 private1 10.211.1.89 10.211.2.176 12367 ipsec 7 1000 22:50:10 2
10.11.1.11 11 down private1 public-internet 10.211.1.89 192.0.2.13 12386 ipsec 7 1000 NA 0
10.12.1.11 12 down private1 public-internet 10.211.1.89 192.0.2.14 12386 ipsec 7 1000 NA 0
10.103.1.11 103 down private1 default 10.211.1.89 192.0.2.18 12346 ipsec 7 1000 NA 0
10.103.1.12 103 down private1 default 10.211.1.89 192.0.2.19 12346 ipsec 7 1000 NA 0
192.0.2.9 65 down private1 public-internet 10.211.1.89 192.0.2.20 12347 ipsec 7 1000 NA 0
192.0.2.8 65 down private1 public-internet 10.211.1.89 192.0.2.21 12347 ipsec 7 1000 NA 0
192.0.2.2 61 down private1 biz-internet 10.211.1.89 192.0.2.0 12347 ipsec 7 1000 NA 0
192.0.2.2 61 down private1 private1 10.211.1.89 198.18.0.5 12367 ipsec 7 1000 NA 0
```

```
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#
DC-AWS-EU-CGW1#sh ver
Cisco IOS XE Software, Version 17.04.01a
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
17.4.1a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Fri 18-Dec-20 05:01 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2020 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

DC-AWS-EU-CGW1 uptime is 4 days, 47 minutes
Uptime for this control processor is 4 days, 49 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
Last reload reason: Unknown reason




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 2264734K/3075K bytes of memory.
Processor board ID 9SAQCJXHS8G
Router operating mode: Controller-Managed
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
7784912K bytes of physical memory.
11526144K bytes of virtual hard disk at bootflash:.
```

```
Configuration register is 0x2102

DC-AWS-EU-CGW1#
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.