

لقنك رشابم لـ AWS لاصتـا نيوكـت رقنلـا يـف SD-WAN مادختـساب

تايوت حملـا

[قمدقم لـا](#)

[قيساس ا تامولعم](#)

[قلكش م لـا](#)

[لحلـا](#)

[ميصصت لـا يلع قماع قرظن](#)

[لحلـا لـي صافات](#)

[ريصحت 1. قوطخلـا](#)

[تانايبلـا زك رمل SD-WAN هجوم نيوكـت 2. قوطخلـا](#)

[AWS TVPC SD-WAN هجوم نيوكـت 3. قوطخلـا](#)

[لـا رشابم لـا لاصتـا لـا نيوكـت 4. قوطخلـا](#)

[AWS GWLB و قكرتش م لـا تامدخلـا لـا VPC يـف قوامحلـا رادج مادختـساب نام لـا](#)

[مي هاف م لـا قحص تابلـا دادع لـا](#)

[SDCI رفوم ب صاخ لـا EquallX ذفنم و ايسـيـئر لـا ذفنم لـا رشابم لـا لاصتـا لـا](#)

قمدقم لـا

Amazon نم بيولـا تامدخلـا (AWS) [رشابم لـا لاصتـا لـا](#) مادختـسا قيفيـك دنـتس م لـا اذـه حضوي جمـاربلـا ب فرعم لـا (SD-WAN) قعـساو لـا قطنـم لـا قكبش لقنـه نـا يلع

قيساس ا تامولعم

يـف Cisco SD-WAN لـا رخـا لقنـه درجمـك رشابم لـا AWS لاصتـا نم قيساس ا لـا قديـاف لـا لـثمتـت لقنـلـا تايـل مـع نمضتـت يـتلـا قلمـاش لـا SD-WAN تاسايس مادختـسا يلع قردقـلـا

AWS لـا رشابم لـا لاصتـا لـا.

رشابم لـا AWS لاصتـا AWS يلع لمـع لامحـا مهـيـدل نم تاسـسـوم لـا ومـدختـسم مـدختـسيـ عئاش تنـرتنـالـا ب ماعـلـا لاصتـا لـا نـا فـ، هـسـفن تقولـا يـفو .عزوم لـا و ا تانايبلـا زك رمل لاصتـا لـا حضوي .رخـا عقاوم ب SD-WAN قكبش لاصتـا لـا ساسـا كـ مدختـسيـ و تانايبلـا زك رمل يـف اضيـا ادج Cisco SD-WAN لـا ساسـا كـ رشابم لـا AWS لاصتـا مادختـسا اهبـن كميـ يـتلـا قيفيـك لـا دنـتس م لـا اذـه هـيـجوتـو SD-WAN قـيـبـطـت يـلع قـمـئـاق تاسايس عـاشـنـا نـيـمدختـسم لـلـن كميـ . SD-WAN قـلـاح يـف ماعـلـا تنـرتنـالـا ب ربع هـيـجوتـلـا قـداعـو رشابم لـا لاصتـا لـا ربع قـيـبـطـتـلـا قـمـدخـلـا يـوتـسم قـيـقـافـتـالـا تـاكاهـتـنا ثوـدح (SLA).

قلكش م لـا

نم قـيـجـذومـنـلـا قـلـئـسـا لـا .قـيـلـصـا لـا SD-WAN تايـنا كـم رشابم لـا AWS لاصتـا رفويـا لـا :قـيـه تاسـسـوم لـا يـف SD-WAN يـمدختـسم

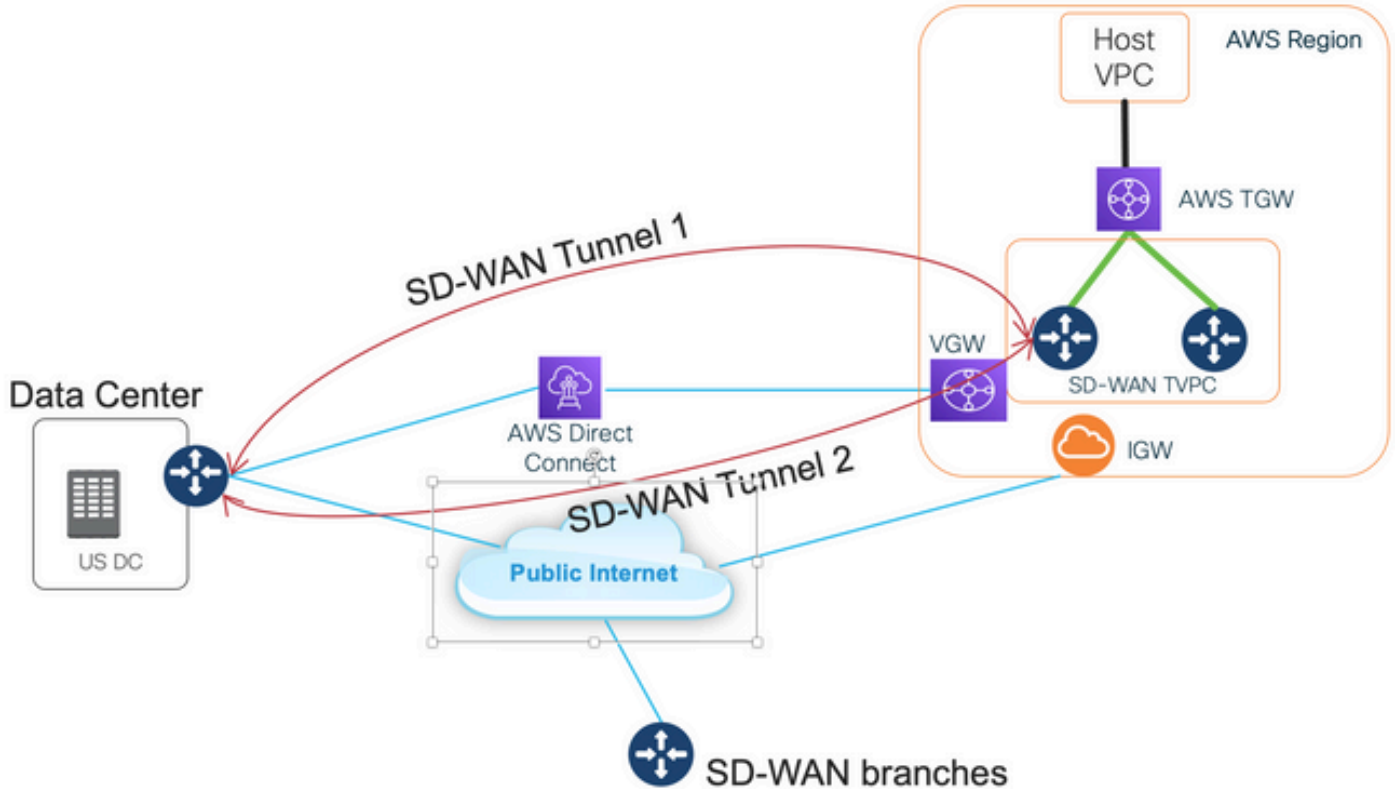
- Cisco SD-WAN لـا ساسـا كـ رشابم لـا AWS لاصتـا مادختـسا يـنـنـكـميـ لـه ؟

- AWS Direct Connect و Cisco SD-WAN طبريننك مي فيك
- ريوطتلل ةلباقو ةنم أو ةنرم لولح ءاشن إنيننك مي فيك

لحل

ميمصتلا لىل ةماع ةرظن

ب AWS Direct Connect ربع تانايبالا زكرم لاصتا في ةيساسألا ميمصتلا ةطقن لثمتت حضورم وه امك SD-WAN Transport Virtual Private Cloud (VPC) ةكبش في Virtual Gateway (VGW) ةروصلال في.



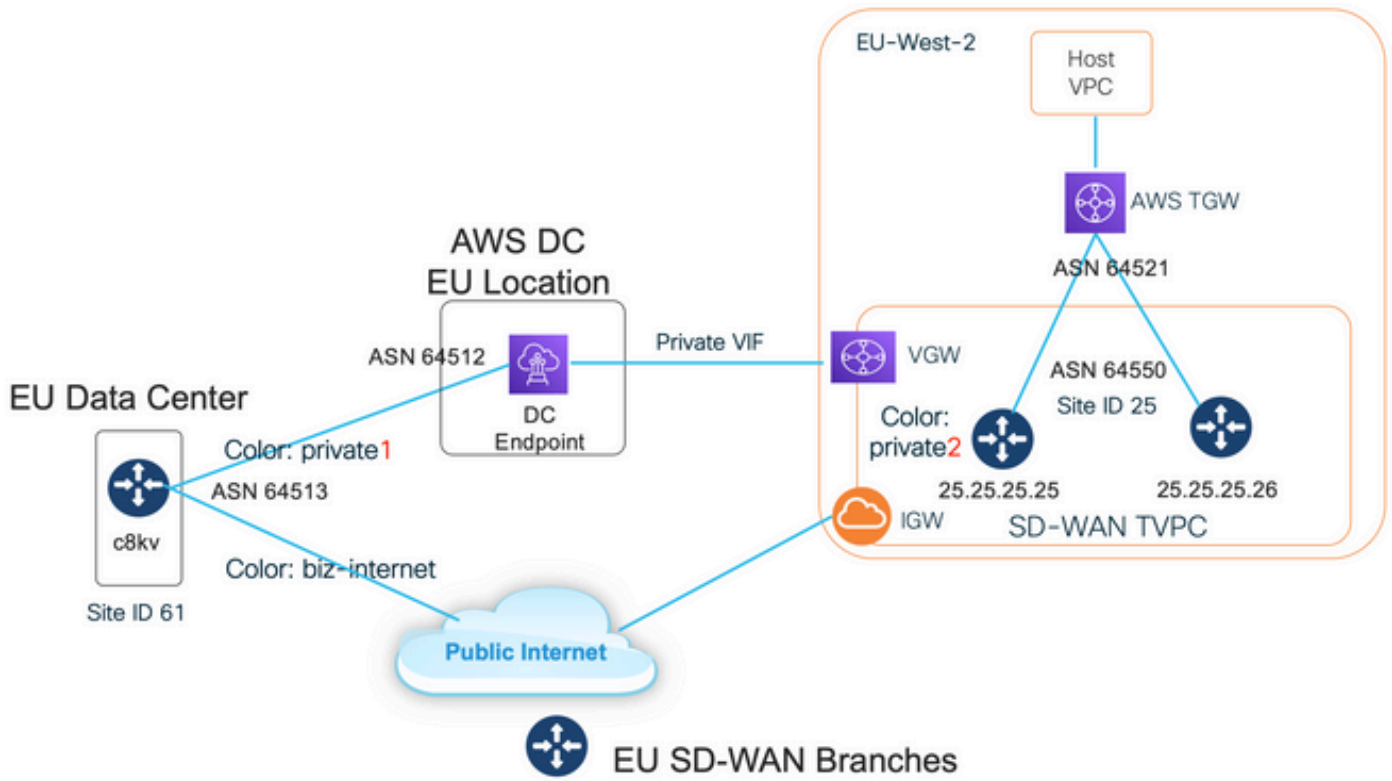
يلى امي في لحل اذه ةئاوف لثمتت

- رشنل Multicloud Automation ل Cisco Cloud OnRamp مادختسا نكمي: لمالكاب يئاقلت نكمي (TGW) ةديج AWS رورم ةباوبو SD-WAN تاهجوم عم SD-WAN Transport VPC ةكبش فيك ءاشتكا SD-WAN ةكبش لىل ءهطيختو Cloud OnRamp نم ءزجك ةفيضملا VPCs ءزهجأ فاشتكا ءدحاو ةرقنن ب SD-WAN.
- لقن ةليسو رشابملا AWS لاصتا لثمي: رشابملا لاصتالا ربع ةلمك SD-WAN ةقابط ل SD-WAN ةكبش تازيم عيجم مادختسا نكمي. SD قيرط نع ةفرعملا WAN ةكبش ربع ىرخأ يعيبط لكش ب كلذ لىل امو ريفشتلاو تاقيبطتلا لىل ةمئاقلا تاسايسلا لثم SD-WAN ربع رشابملا لاصتالا ربع SD-WAN قفن لىل رشابملا AWS لاصتا ربع تاءابلا ددعب ةصاخلا AWS دويق حرتقملا ميمصتلا بنجتي (20/100).

لحل لىل صافات

ب VGW رشابملا لاصتالا لالخنم نيلصتت تانايبالا زكرم و AWS ةقطنم ةروصلال هذه رهظت ءاجرلا (color biz-internet) ماعلا تنرتنالا ربعو SD-WAN ربع روعلا VPC في (color private1)

تنترتن إلالا لاصتال SD-WAN Color Private2 مدختست AWS SD-WAN C8kv تاهجوم نأ ةظحالم



ريضحت 1. ةوطخلال

Cloud onRamp تادادعإ نيوكت متو طشن AWS باسح ىلع يوتحي Cisco vManage نأ نم دكأت جحيحص لكشب ةي مومع ال

،نودملا هذه يف .اضيأ vManage يف Interconnect ةمدخي في كيرش باسح ديدحت يجري امك تادادعإو بسانم باسح ديدحت كنكمي ىتح ،ينيبل لاصتال كيرشك MegPort مادختسإ متي ةي مومع

تانايبال زكرم ل SD-WAN هجوم نيوكت 2. ةوطخلال

Color BIZ-Internet ةينقت مادختساب ماعال تنترتن إلالا لاصتال GigabitEthernet1 ةهجاو مادختسإ متي Color Private1 عم رشابم ال AWS لاصتال GigabitEthernet1.1352 ةهجاو اول مادختسإ متي و Internet Private1.

ىلإ ةفاضلإاب تنترتن إلالا لاصتال ل 2 ةصاخ ناولأ اهب AWS SD-WAN تاهجوم نأ ةظحالم يجري تنترتن إلالا ربع SD-WAN ةكبش قافنأ نيوكت متي .رشابم ل لاصتال ربع لاصتال (ةهجاو اول سفن مادختساب) SD-WAN قافنأ عاشنإ ىلإ ةفاضلإاب ةماع ال IP نيوانع مادختساب .عقوم ال/الاجم لالاب مكحتللا ةدحو ىلإ ةصاخ ال IP نيوانع مادختساب رشابم ل لاصتال رئاود ربع AWS SD-WAN تاهجوم ب لاصتال ميقي (biz-internet نولل) تانايبال زكرم هجوم نأ ينعني اذهو IP ربع صاخ ال هنول لال خ نمو ةماع ال IP نيوانع مادختساب تنترتن إلالا ربع (2 صاخ ال نولل) لاصتال

SD-WAN: ناولأ لوح ةماع تامولعم

اهل لال خ نم لصلتت يتي ال (VPN 0) WAN لقن تاهجاو ىلإ (TLOCs) لقنللا عقوم تاددحم ريشت لال خ نم ديرف لكشب TLOC ةدحو لك فيرعت متي .ةي ساسألأ ةكبش لال SD-WAN تاهجوم ني مضتو ، WAN ةكبش ةهجاو نولو ، SD-WAN هجوم ب صاخ ال ماظنل لل IP ناووع نم ةعومجم

عيزوتل Cisco نم (OMP) ةيشغتلل ةرادا لوكوتورب مادختسا متي (GRE أو IPsec) لقنلل ةيشغت تائدابو، (TLOC تاراسم مساب اضيا فورعما) (TLOC) لوصولي فم كحتلا ميأوق لالخنم. SD-WAN تاهجوم نيبي رخا تامولعمو، (OMP تاراسم مساب اضيا فورعما) SD-WAN قافنا عاشناو وضعبل اهضعب لوصولي ةيفي SD-WAN تاهجوم فرعت، TLOC تاراسم وضعبل اهضعب عم IPsec لوكوتوربل VPN.

زهجا فلخ (vBond أو vSmart أو vManage) م كحتلا تادحو وأ/أو SD-WAN تاهجوم عضوت نا نكمي في م كحت ةدحو ل SD-WAN هجوم قداصي ام دنع. ةكبشلا لخاد (NAT) ةكبشلا ناو نع ةم جرت ناو نع تاداعوا ماعلا ذفنملا مقر/صاخلا IP ناو نع نم لك vBond في م كحتلا ةدحو ملعي، vBond في م كحتلا تادحو لمعت. لدابتلا تقوي في SD-WAN هجومل ةماعلا ذفنملا مقر/صاخلا IP فاشتكاب SD-WAN تاهجومل حمستو (STUN) NAT مداوخل لمعلا ةسلج زاي تجال ةدعاسم تاوداك اهت م جرت وأ/أو اهني يعت مت يتلا واهب ةصاخلا WAN لقن ةهجاو ذفانم ماقرا وأ/أو IP نيوانع.

IP ناو نع ربتعي. صاخلا وماعلا IP نيوانع جوزب WAN لقن لك نرتقي، SD-WAN تاهجوم لىل SD-WAN هجومل WAN ةهجاول هني يعت مت يذلا IP ناو نع وه اذه. قباصل NAT ناو نع صاخلا ةحاسم نم اعزج اما نوكي نا نكمي اذه IP ناو نع نا ال، صاخ IP ناو نع ربتعي هنا نم مغرلا لىل هيجوتلل ةلباقلا ريغ IP ناو نع ةحاسم نم اعزج و ماع لكشب هيجوتلل لباقلا IP ناو نع كلذ فاشتكاب متي و NAT دعب ام ناو نع ماعلا IP ناو نع ربتعي. IETF RFC 1918 ب ةصاخلا امك. هيلع قداصي و vBond مداخ ايئدبم SD-WAN هجوم لصتي ام دنع vBond مداخ ةطساوب نم اعزج و ماع لكشب هيجوتلل لباقلا IP ناو نع ةحاسم نم اعزج ماعلا IP ناو نع نوكي نا نكمي NAT، ب ايغ في IETF RFC 1918 ب ةصاخلا ماع لكشب هيجوتلل ةلباقلا ريغ IP ناو نع ةحاسم. اهسفن يه SD-WAN لقن ةهجاول ةصاخلا و ماعلا IP نيوانع نم لك نوكي.

WAN لقن تاي لمع في رعتل مدختست تباث لكشب ةفرعم ةيساسا تاملك يه TLOC ناو ال SD-WAN هجوم لىل WAN ةكبش ربع لقن لكل نوكي نا بجي. SD-WAN هجوم لك لىل ةي درفلا و ماع هنا لىل ةي درفلا WAN ةكبش لقن في رعتل ناو ال مادختسا متي امك. ديرف نول ددحم Private1 و Private2 و Private3 و Private4 و Private5 و Metro-ethernet و MPLS و Private6 و Private6 يه ناو ال. NAT دجوي ال شيح نكاما و ةصاخ تاكشب في مدختست نا. ةصاخ ناو ال Private6 و lte، رضخا، يبهذ، يضارتفا، custom3، custom2، custom1، صصخم، يزورب، قرزا، biz-internet، 3G، و ماعلا تاكشب لىل في مدختست نا اهنم ضرغلاو. ةماع ناو ال ربتعت ي ضفو، رمحا، ماع تنرتنا و NAT قيرط نع و اي لحم اما، WAN لقنلا تاهجاول ةماعلا IP نيوانع اهل يتلا نكاما لىل في.

م كحتلا تايوتسم لالخنم اهل اصتا دنع ةماعلا و ةصاخلا IP نيوانع مادختسا نوللا ضرفي تاهجاو ال ك مدختسي، وضعبل اهضعبب لاصتالا SD-WAN تاهجوم لواحي ام دنع. تاناي بلاو دحا ناك اذا. دي عبلا هجوملل صاخلا IP ناو نع ب لاصتالا بناج لك لواحي، ةصاخ ناو ال اب WAN لقن ماعلا IP ناو نع ب لاصتالا بناج لك لواحي سف، ةماع ناو ال مدختسي امهالك و ني بنجال يه ني زاهج ةصاخلا عقوملا تافرعم نوكت ام دنع وه كلذ نم اناثتسالو. دي عبلا هجوملل IP نيوانع مادختسا متي، ةماع ناو ال نكلو، ةدحاو عقوملا تافرعم نوكت ام دنع. اهسفن م كحت ةدحوب لاصتالا لواحتي لتلا SD-WAN تاهجومل كلذ ثدحي نا نكمي و. لاصتال ةصاخلا لكشب، موقت ال SD-WAN تاهجوم نا ظحال. عقوملا سفن لخاد ةدوجوم vSmart و vManage تافرعم سفن اهل نوكت ام دنع وضعبل اهضعب نيبي IPsec ل VPN قافنا عاشنا ب، يضارتفا عقوملا.

```
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 Tunnell1 ip unnumbered GigabitEthernet1 tunnel source GigabitEthernet1 tunnel mode sdwan ! interface Tunnell1352001 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 ... Tunnell1 162.43.145.3 YES TFTP up up Tunnell1352001 198.18.0.5 YES TFTP up up 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#
```

لاصتال انايبال زك رمل SD-WAN هجوم يلع (BGP) ةي دودخال ةباوبال لوكوتورب نيوكت
رشابم ل AWS:

```
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
```

يوتحي SD-WAN Transport VPC. نم IP 10.211.1.0/24 ةئداب ملعي Data Center SD-WAN هجوم
انه 7 طخال ل عجا - ةيلال ةوطخال IP 198.18.0.6 ناونع عم AWS Direct Connect هجوم يلع:

```
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
```

3. ةوطخال AWS TVPC SD-WAN هجوم نيوكت

ليغشال عارجال Cloud OnRamp مادختساب لقنل VPC في SD-WAN تاهجوم الك عاشنإ متي
تاهجوم نم لك مدختسي. ةيضارتفال vManage بلاوق مادختساب ةباحسلا ددعتم يئاقللال
تنترنإلاب ماعال لاصتال 2 صخال نولل C8kv.

4. ةوطخال AWS رشابم ل لاصتال نيوكت

في ةرباعال SD-WAN ةكبش ب صخال (VPC) درومال ةئف فرع م هنارتقاو VGW عاشنإ بجي
هسفن VGW نوكي نأ بجي. ةباحسلا ربع ةتمتأ ةادأ ي مادختساب وأ AWS مكحتلال ةدحو
SD-WAN TVPC ةئداب ةظحال عاجرلا. انه حضوم وه امك رشابم ل لاصتال اباطبترم
اهب حومسمل تائدابلا نمض 10.211.0.0/16.

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

Edit Delete

General configuration

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

Virtual interface attachments | Gateway associations

Gateway associations (1)

Edit Disassociate Associate gateway

Search gateway associations

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

عجاء - SD-WAN Transport VPC ل AWS راسم لودج في VGW ل راسم الراش نيكمت بجي
 رخا قرم DC TLOC ءءو نع راسم الراش نلعي . ءروصلال هءه في 198.18.0.4/30 ل ريخال راسم الراش
 ل. لقلنلاب صخال VPC راسم لودج ل.

ch for services, features, blogs, docs, and more [Option+S] London Nikolai Pitaev

Route tables (1/1) Info

Filter route tables

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

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (5)

Filter routes Both

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

ءرباعل VPC في SD-WAN C8KV تاءجوم ءءا نم انه اء show sdwan bfd session CLI ءارخال نءا مت
 SD-WAN: نيقلن رهظو

1. زكرم ىل | AWS TVPC في c8kv نم تنرتنإل ربع رمي (5 رطسلا عجار) لوال قفنل. 192.0.2.0 ماعل IP ناووع وه - ةهوجلل IP ناووع طحال: color private2 > biz-internet. تانايبل ق. باسلا مسقلل في هجومل نيوكت عجار - تانايبل زكرم هجومل.
2. ىل | color private2 نم: رشابم ال AWS لاصتا ربع رمي (6 رطسلا عجار) ينال قفنل. ةهوجلل IP ناووعك 198.18.0.5 عم private1.

```
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#
```

AWS GWLB و ةكرتشم ال تامدخلل VPC في ةيامل راج مادختساب نامال

بونجالو لامشل او بيبرغل قرشلل في رورم ال ةكرتشم اذ ةعئاشل تابللم ال نم لى | SD-WAN VPNs و/و ةفللم ال ةفيضم ال VPN تاكلش ني رورم ةكرتشم اذ ةعئاشل، ةداع ةزهجأ في اهليغشت ممتي يتل ةيرهظال ةيامل ناريج ذيفنت نكمي. ةيامل راج صحف لمح نزاوم مادختساب لامحال ةنزاوم و ةكرتشم ال تامدخلل (VPC) ةيرهظال ةصاخال رتوي بمك ال (AWS (GWLB) ةرابع.

. رظنا - يزكرم ال صحف ال عم اذ ديچ لكش ب فوصوم ال ميمصتلا لمعي

ميهافل ةحص تابلل دادع ال

(PoC): ميهافل ةحص ليلى رابلل دادع | عاشنإل روصل ال هذه مادختساب ممتي

- مزال ةيسدنهل ةروصل ال لهل ريتك يوررض وم 192.0.2.1R رادصل ال vManage جم انرب 20.6 ب نامك لغتشي
- 17.5 و 17.4: (تانايبل زكرم ةكاحم / رشابم ال لاصتال) Megaport و AWS ل c8kv
- يسيئرل ذفنم ال مادختساب رشابم ال AWS لاصتا ةكاحم ممتي

SDCI رفومب صاخال EquallX ذفنم و ايسيئرل ذفنم لابل رشابم ال لاصتال

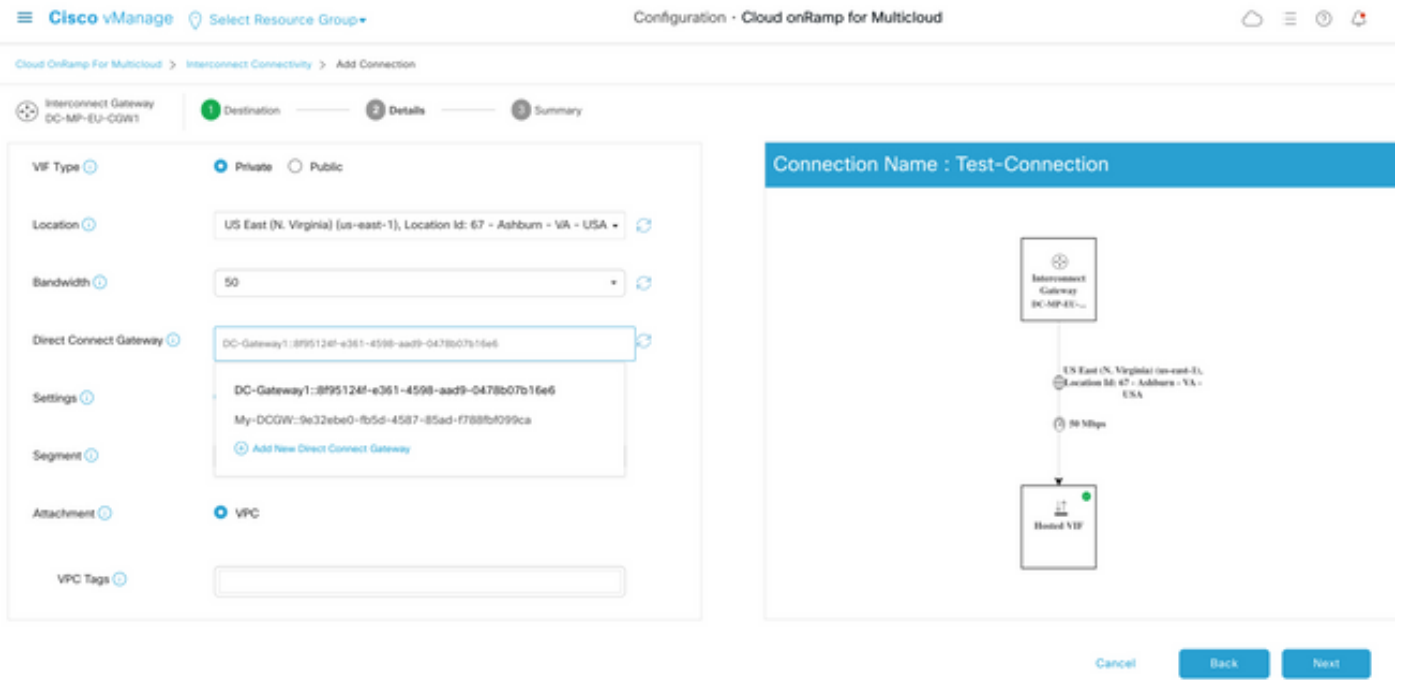
بلمتلي ام ةداع. ةيلممع ةئيبل يقيقح رشابم AWS لاصتا يلع لوصحل لهسل نم سيلي اتقو قرغتسي دقو افلكم نوكي يذلو، رشابم ال AWS لاصتا كي رش دوو رمال

لاصتا ةباب عاشنإل همادختساب | كنكمي في Equinix و Megaport باسح كيلى ناك اذ، كلذعمو ةباحسل ةدعتم ةتمتأل Cisco Cloud OnRamp عم قئاقد نوضغ في رشابم ال AWS!

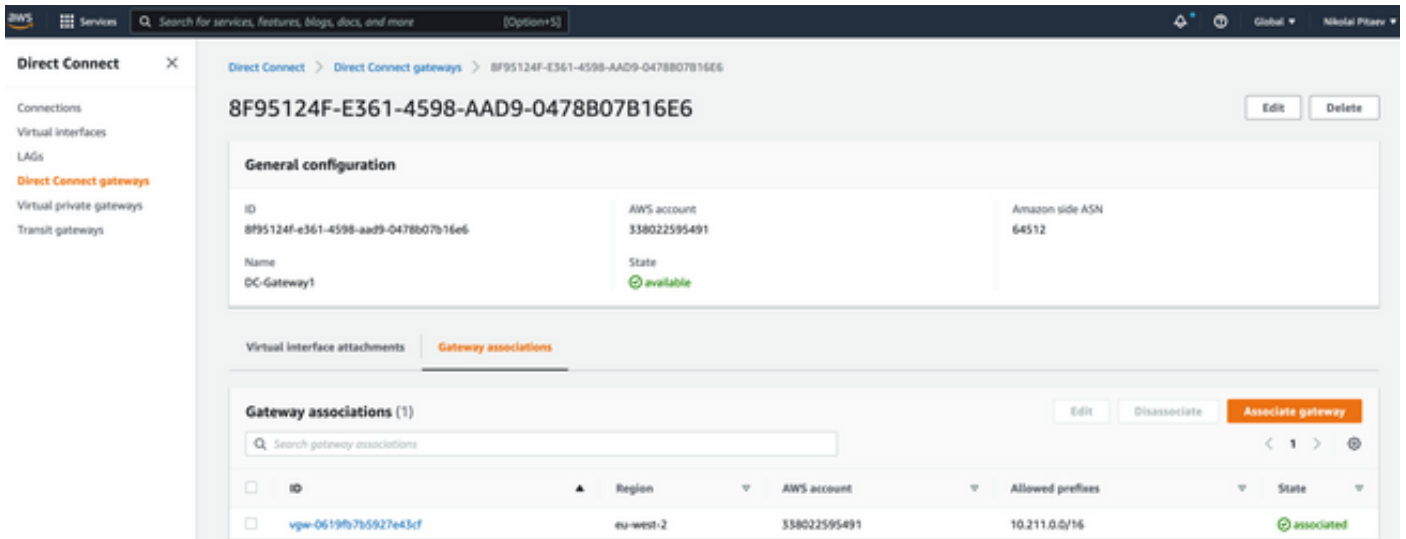
لاصتال ةزيم نيوكتب لعلابل تمق دق تنك اذ، ايسيئرل تاوطللاب صخلم يلي امي في vManage في AWS تاغوسم وجماربلل ةدحمال (SDCI) تانايبل زكرم لي نيبل

1. AWS يلع ةرباع ال VPC في ةباحس تابلابل نالمعي c8kvs نانثا | كيلى نكمي مل اذ. ةعئاشنإل و AWS ل Multicloud لمع ريسل Cloud onRamp (CoR) مادختساب | جري في، لعلابل نول ياعم يضا رتفال ال AWS CoR هجوم بلال مادختساب ةبولطم ال AWS ةقطنم في صاخ.
2. ةباب ةش نأ و ةباحسل ددعتم ينيبل لاصتال نيوكتل CoR لى | لقتنا، vManage في. SDCI رفوم هجوم بلال مادختساب ةبولطم ال SDCI ةقطنم في (c8kv) ينيبل لاصتا يضا رتفال.

3. مق vManage، في CoR بة صاخلة باحسلا ددعت ميني بلبا لاصتالا نيوكت ةحفص في (VIF). ةصاخلة ةيره اظلالا ةهجاو لا مادختساب لاصتالا عون نم ةديج ةباحس عاشناب نارقوا ةديج رشابم ال AWS لاصتالا ةباوب عاشناب راين كيدل، اذ نيوكتلا لمع ريس تقو ةوطخال هذهل VPC "يمهو" فيضم زاهج كيدل نأ نم دكأت، كذلذ. اهب فيضم لل VPC زاهج بولسأ ال ال بولسأ ليكشت vManage نم حاتفم 2. ةوطخ في قلخي ديغ c8kv ال ال نم ققحت (ناي ب VRF forwarding ال لزلزا) VPN0 ال بناج ةمدخال نم قفنلا لقنوا عانق 198.18.0.4 ةكبشلا BGP نيوكت في ةكبشلا ناي ب كيدل نأ، دكأتو BGP لاصتالا ةق فرم ال AWS تاهج ومو تانايبلا زكرم ل لمكلا هجوم ال نيوكت عجار. 255.255.255.252.
4. نيكم تب مقو (ديج دحاو عاشناب مق وا) بسانم ال VGW دح AWS ةرادم كحت ةدحو في اهب حومس ال تائدا بلبا نيوكت نم اضيا دكأت. AWS راسم لودج تادادع في راسم ال رشن لصللا اذ في اقحال ةروصل ال عجار - رشابم ال لاصتالا مسق في 3. ةوطخال نم رشابم ال لاصتالا عاشناب ةروصل هذو حضوت

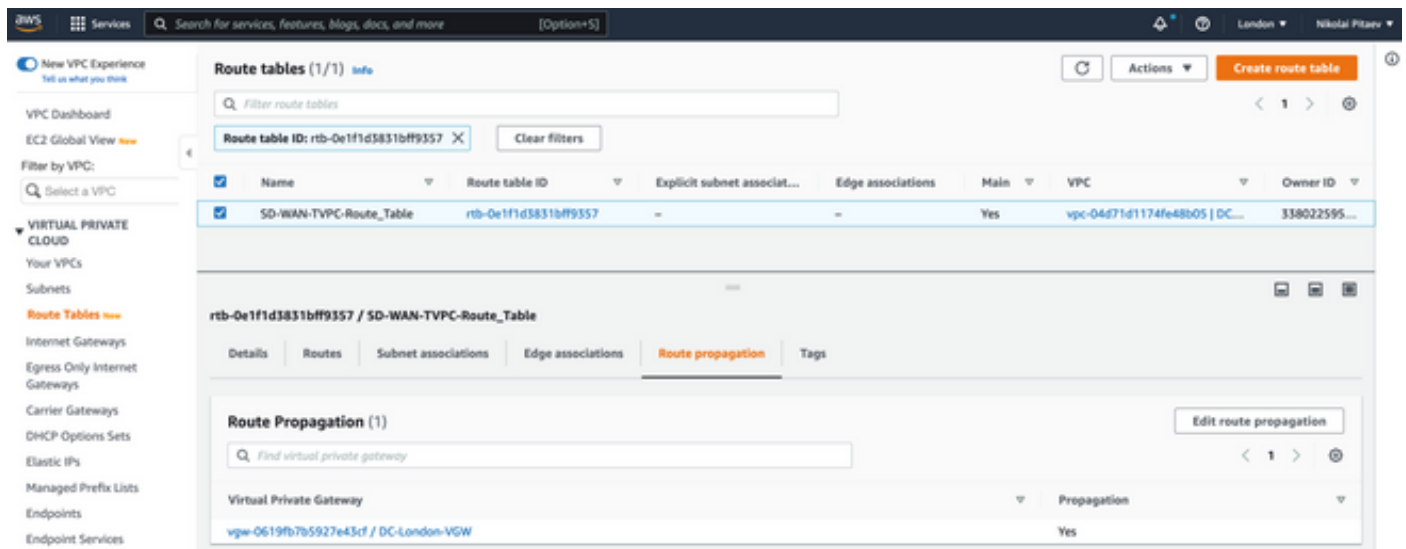


وه امك كب ةصاخلة ال AWS ةرادم كحت ةدحو في ةديج رشابم لاصتالا ةرابع دهاشت، كذلذ ةجيتنو ةصاخلة ال CIDR ةلتك ال ع يوتحي يذلاو، اهب حومس ال تائدا بلبا ل قح ةظحال م عا ج رلا. انه حضوم ب ةرباع ال SD-WAN VPC.



ةينك م كيدل نوكت نأ بجي. SD-WAN Transport VPC ل تاراسم ال لودج نم نيترم ققحت

ةروصلال ي ف حضم وه امك نميال ال VGW ن كمت عم رشنال



تاجرخلما راهظاولم الكال هجومال نوكت يلع لوصحلل مسقلا اذه يلا عوچرلا يجرى

```
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$3V6L3V6L2VUI2k$ysPnXOd98RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
vrf definition 10
rd 1:10
address-family ipv4
route-target export 64513:10
route-target import 64513:10
exit-address-family
!
address-family ipv6
exit-address-family
!
!
ip arp proxy disable
```

```
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
no ip dhcp use class
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
no shutdown
arp timeout 1200
ip address dhcp client-id GigabitEthernet1
no ip redirects
ip dhcp client default-router distance 1
ip mtu 1500
load-interval 30
mtu 1500
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 privatel
max-control-connections 0
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
```

```
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
appqoe
no tcptopt enable
no dreopt enable
!
omp
no shutdown
send-path-limit 4
ecmp-limit 4
graceful-restart
no as-dot-notation
timers
holdtime 60
advertisement-interval 1
graceful-restart-timer 43200
eor-timer 300
exit
address-family ipv4
advertise bgp
advertise connected
advertise static
!
address-family ipv6
advertise bgp
advertise connected
advertise static
!
!
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
hello-interval 1000
no pmtu-discovery
multiplier 1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
ipsec
rekey 86400
replay-window 512
!
!
sslproxy
no enable
rsa-key-modulus 2048
certificate-lifetime 730
eckey-type P256
ca-tp-label PROXY-SIGNING-CA
settings expired-certificate drop
settings untrusted-certificate drop
settings unknown-status drop
```

```
settings certificate-revocation-check none
settings unsupported-protocol-versions drop
settings unsupported-cipher-suites drop
settings failure-mode close
settings minimum-tls-ver TLSv1
dual-side optimization enable
!
```

```
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  
rsa-keypair 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  
!  
!  
!  
!
```



```
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 privatel 192.0.2.0 10.211.0.68 12367 ipsec 7 1000 NA 0
192.0.2.9 65 down biz-internet privatel 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 privatel 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 privatel privatel 198.18.0.5 10.211.0.68 12367 ipsec 7 1000 NA 0
192.0.2.9 65 down privatel privatel 198.18.0.5 10.211.0.180 12367 ipsec 7 1000 NA 0
192.0.2.10 25 up privatel 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 privatel privatel 198.18.0.5 10.211.1.89 12367 ipsec 7 1000 NA 0
192.0.2.11 25 up privatel 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 privatel privatel 198.18.0.5 10.211.1.184 12367 ipsec 7 1000 NA 0
192.0.2.6 64 down privatel private2 198.18.0.5 10.211.2.41 12387 ipsec 7 1000 NA 0
192.0.2.6 64 down privatel privatel 198.18.0.5 10.211.2.76 12367 ipsec 7 1000 NA 0
192.0.2.24 64 down privatel private2 198.18.0.5 10.211.2.154 12387 ipsec 7 1000 NA 0
192.0.2.24 64 down privatel privatel 198.18.0.5 10.211.2.176 12367 ipsec 7 1000 NA 0
10.11.1.11 11 down privatel public-internet 198.18.0.5 192.0.2.13 12386 ipsec 7 1000 NA 0
10.12.1.11 12 down privatel public-internet 198.18.0.5 192.0.2.14 12386 ipsec 7 1000 NA 0
10.103.1.11 103 down privatel default 198.18.0.5 192.0.2.18 12346 ipsec 7 1000 NA 0
10.103.1.12 103 down privatel default 198.18.0.5 192.0.2.19 12346 ipsec 7 1000 NA 0
192.0.2.9 65 down privatel public-internet 198.18.0.5 192.0.2.20 12347 ipsec 7 1000 NA 0
192.0.2.8 65 down privatel 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/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:
Controller-managed

The current throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C8000V (VXE) processor (revision VXE) with 2028465K/3075K bytes of memory.
Processor board ID 9FTTYDEBR70
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 qOWzTrRGM9500a8j35VT7eQRMmzgHCEq
!
crypto keyring if-ipsec2-ikev1-keyring
pre-shared-key address 192.0.2.23 key E4cayBdglWSBUaaDilukyngzbUzUP8Hp
!
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-shal-hmac shal-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  
rsa-keypair 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 qOWzTrRGM9500a8j35VT7eQRmzgHCEq
crypto keyring if-ipsec2-ikev1-keyring
pre-shared-key address 192.0.2.23 key E4cayBdglWSBUaaDilukyngzbUzUP8Hp
!
!
!
!
!
!
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/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:
Controller-managed

The current throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C8000V (VXE) processor (revision VXE) with 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#

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسملا اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچي ف ني م دختسم ل م عدد ي و ت م م ي دقتل ل ي رش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ل ع م ل ا ح ل ا و ه
ى ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ل ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن ت س م ل ا