Configurazione di AWS Direct Connect come trasporto con SD-WAN in un clic

Sommario

Introduzione

Questo documento descrive come usare Amazon Web Services (AWS) Direct Connect come trasporto SD-WAN (Wide Area Network) definito dal software.

Premesse

Il vantaggio principale di AWS Direct Connect come un altro trasporto per Cisco SD-WAN è la possibilità di utilizzare le policy SD-WAN per i trasporti complessivi che includono

Connessione diretta AWS.

Gli utenti aziendali con carichi di lavoro su AWS utilizzano AWS Direct Connect per la connettività di centri dati o hub. Allo stesso tempo, la connessione a Internet pubblica è molto comune nei centri dati e viene utilizzata come base per la connettività SD-WAN con altre postazioni. Questo documento descrive come AWS Direct Connect può essere usato come underlay per Cisco SD-WAN. Gli utenti possono creare policy compatibili con le applicazioni SD-WAN e instradare le applicazioni critiche tramite connessione diretta e reindirizzarle tramite Internet in caso di violazione degli accordi sui livelli di servizio (SLA, Service Level Agreement).

Problema

AWS Direct Connect non fornisce funzionalità SD-WAN native. Le domande tipiche da parte degli utenti SD-WAN aziendali sono:

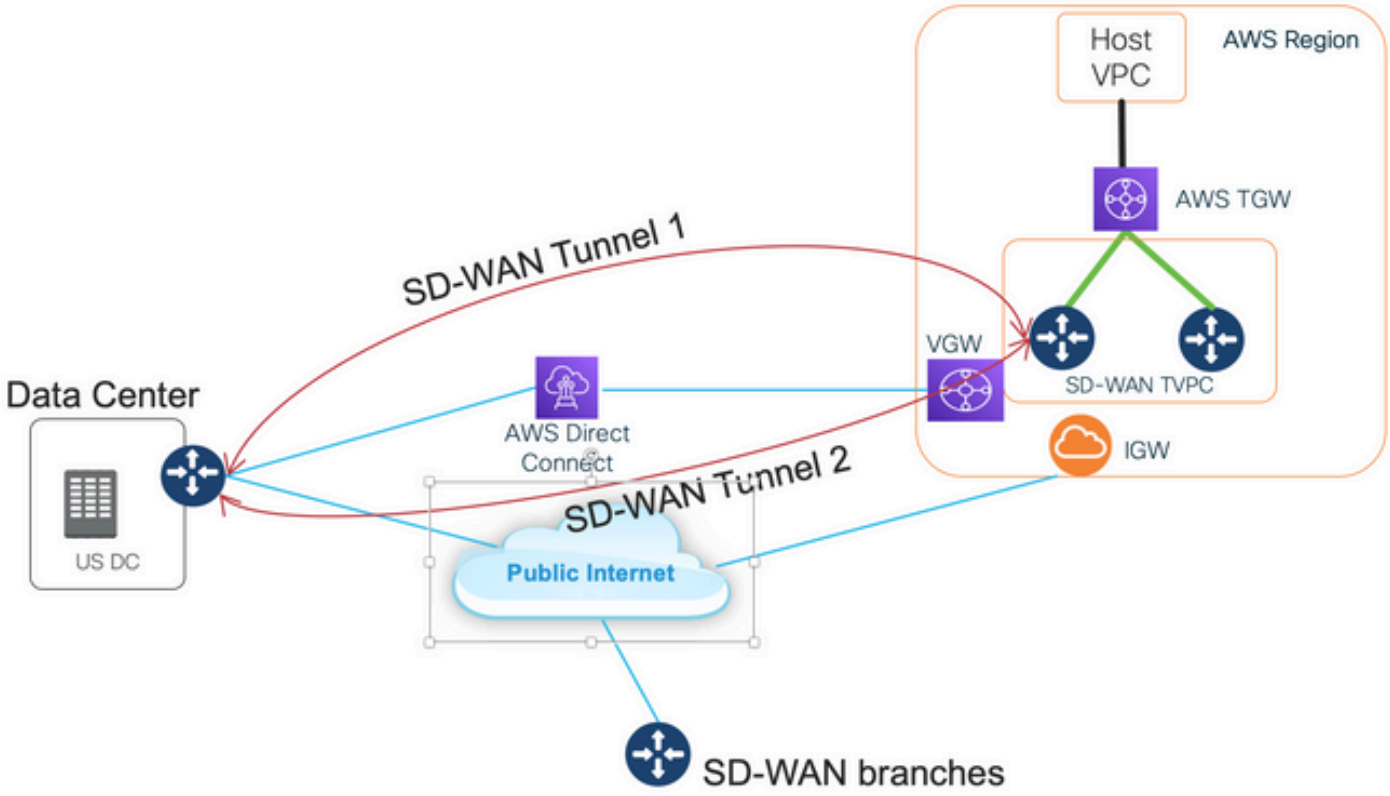
- Posso utilizzare AWS Direct Connect come underlay per Cisco SD-WAN?

- Come posso interconnettere AWS Direct Connect e Cisco SD-WAN?
- Come creare soluzioni resilienti, sicure e scalabili?

Soluzione

Panoramica della progettazione

Il punto di progettazione chiave è la connessione del centro dati tramite AWS Direct Connect a Virtual Gateway (VGW) in SD-WAN Transit Virtual Private Cloud (VPC), come mostrato nell'immagine.



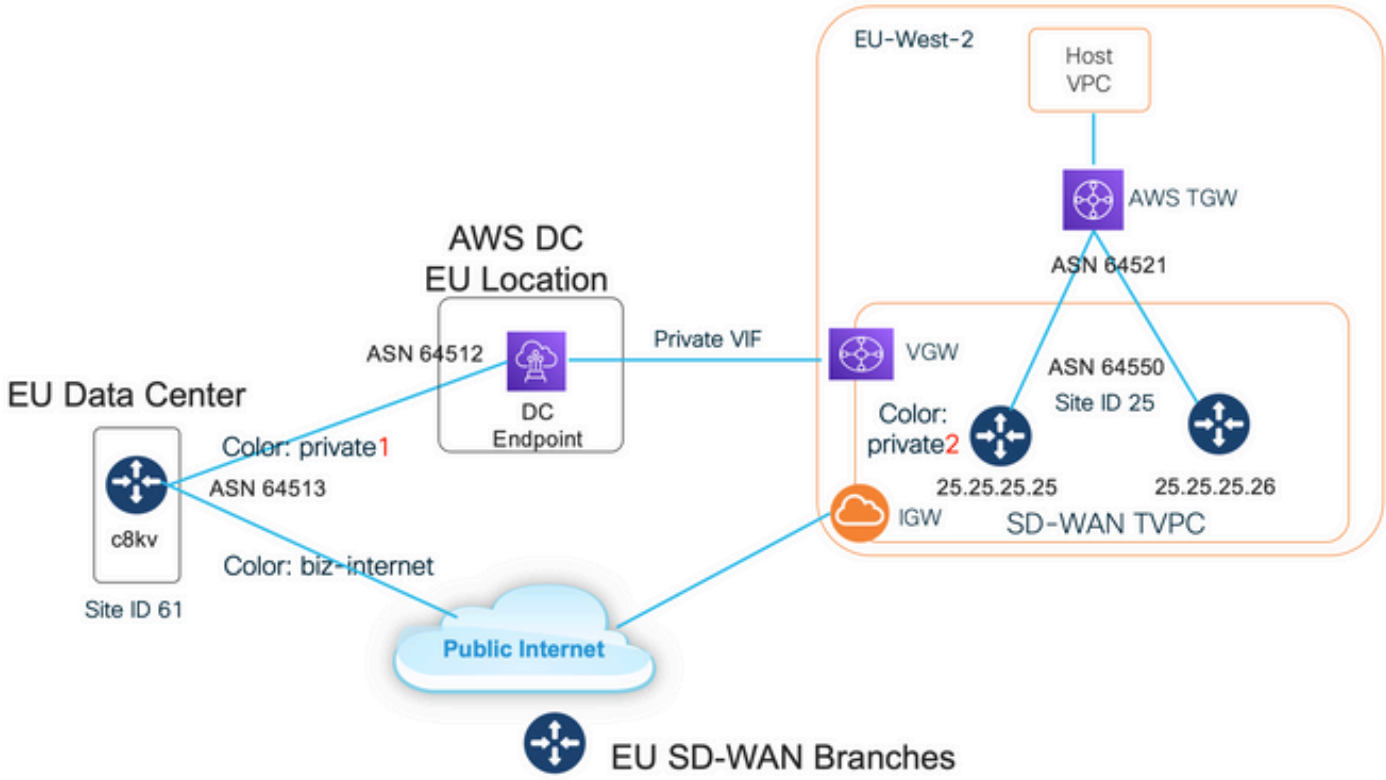
I vantaggi di questa soluzione sono:

- Completamente automatico: Cisco Cloud onRamp per automazione multicolore può essere utilizzato per installare VPC di transito SD-WAN con due router SD-WAN e un nuovo AWS Transit Gateway (TGW). I VPC host possono essere rilevati come parte di Cloud onRamp e mappati su reti SD-WAN con un solo clic.
- Full SD-WAN over Direct Connect: AWS Direct Connect è solo un altro trasporto SD-WAN. Tutte le funzioni SD-WAN, quali le policy compatibili con le applicazioni, la crittografia e così via, possono essere utilizzate in modo nativo sul tunnel SD-WAN su AWS Direct Connect.
- La progettazione proposta evita i limiti AWS del numero di prefissi su una connessione diretta AWS (20/100).

Dettagli della soluzione

Questa immagine mostra una regione AWS e un centro dati connessi tramite connessione diretta a VGW (colore privato1) in VPC di transito SD-WAN e tramite Internet pubblico (colore biz-internet). Notare che i router AWS SD-WAN c8kv utilizzano il colore SD-WAN private2 per la

connessione a Internet.



Passaggio 1. Preparazione

Verificare che Cisco vManage abbia un account AWS attivo definito e che le impostazioni globali di Cloud onRamp siano configurate correttamente.

Definire anche un account partner di interconnessione in vManage. In questo blog, Megaport è usato come partner di interconnessione, quindi è possibile definire un account appropriato e le impostazioni globali.

Passaggio 2. Configurazione router SD-WAN per data center

L'interfaccia Gigabit Ethernet1 viene utilizzata per la connettività Internet pubblica con biz-internet a colori, mentre l'interfaccia Gigabit Ethernet1.1352 viene utilizzata per AWS Direct Connect con color private1.

Si tenga presente che i router AWS SD-WAN dispongono di **private color private2** per la connettività Internet e la connettività tramite connessione diretta. I tunnel SD-WAN sono formati su Internet con indirizzi IP pubblici e tunnel SD-WAN sono stabiliti (con la stessa interfaccia) sui circuiti di connessione diretta con indirizzi IP privati a un DC/Sito. Ciò significa che il router del data center (colore biz-internet) stabilisce una connessione ai router AWS SD-WAN (colore private2) via Internet con indirizzi IP pubblici e tramite il suo colore privato su IP privato.

Informazioni generiche sui colori SD-WAN:

I Transport Locator (TLOC) si riferiscono alle interfacce di trasporto WAN (VPN 0) tramite le quali i router SD-WAN si connettono alla rete sottostante. Ogni TLOC viene identificato univocamente tramite una combinazione dell'indirizzo IP di sistema del router SD-WAN, del colore dell'interfaccia WAN e dell'incapsulamento del trasporto (GRE o IPsec). Il protocollo OMP (Cisco Overlay

Management Protocol) viene utilizzato per distribuire TLOC (noti anche come route TLOC), prefissi di overlay SD-WAN (noti anche come route OMP) e altre informazioni tra router SD-WAN. È attraverso le route TLOC che i router SD-WAN sanno come raggiungere gli altri router e stabilire i tunnel VPN IPsec tra loro.

I router e/o i controller SD-WAN (vManage, vSmart o vBond) possono supportare dispositivi NAT (Network Address Translation) all'interno della rete. Quando un router SD-WAN esegue l'autenticazione a un controller vBond, il controller vBond apprende sia l'indirizzo IP privato/numero di porta che l'indirizzo IP pubblico/numero di porta del router SD-WAN al momento dello scambio. I controller vBond fungono da utility di ritorno della sessione per i server NAT (STUN) e consentono ai router SD-WAN di rilevare gli indirizzi IP mappati e/o tradotti e i numeri di porta delle proprie interfacce di trasporto WAN.

Sui router SD-WAN, ogni trasporto WAN è associato a una coppia di indirizzi IP pubblici e privati. L'indirizzo IP privato viene considerato l'indirizzo precedente al NAT. L'indirizzo IP assegnato all'interfaccia WAN del router SD-WAN. Sebbene sia considerato un indirizzo IP privato, questo indirizzo IP può essere parte dello spazio di indirizzi IP instradabile pubblicamente o parte dello spazio di indirizzi IP instradabile non pubblicamente dell'IETF RFC 1918. L'indirizzo IP pubblico viene considerato l'indirizzo post-NAT. Questo viene rilevato dal server vBond quando il router SD-WAN inizialmente comunica e si autentica con il server vBond. L'indirizzo IP pubblico può anche far parte dello spazio degli indirizzi IP instradabile pubblicamente o dello spazio degli indirizzi IP non instradabile pubblicamente della RFC 1918 dell'IETF. In assenza di NAT, sia gli indirizzi IP pubblici che privati dell'interfaccia di trasporto SD-WAN sono gli stessi.

I colori TLOC sono parole chiave definite in modo statico usate per identificare i singoli trasporti WAN su ciascun router SD-WAN. Ogni trasporto WAN su un router SD-WAN specificato deve avere un colore univoco. I colori vengono inoltre utilizzati per identificare un singolo trasporto WAN come pubblico o privato. I colori metro-ethernet, Mpls e private1, private2, private3, private4, private5 e private6 sono considerati colori privati. Sono destinati all'utilizzo in reti private o in luoghi in cui non esiste un NAT. I colori sono 3g, biz-internet, blu, bronzo, custom1, custom2, custom3, default, oro, verde, lte, public-internet, rosso e argento sono considerati colori pubblici. Sono destinati ad essere utilizzati in reti pubbliche o in luoghi con indirizzamento IP pubblico delle interfacce di trasporto WAN, in modo nativo o tramite NAT.

Il colore determina l'utilizzo di indirizzi IP pubblici o privati quando comunicano tramite i piani dati e di controllo. Quando due router SD-WAN tentano di comunicare tra loro, entrambi utilizzano interfacce di trasporto WAN con colori privati, ciascun router tenta di connettersi all'indirizzo IP privato del router remoto. Se uno o entrambi i dispositivi utilizzano colori pubblici, ciascun dispositivo tenterà di connettersi all'indirizzo IP pubblico del router remoto. Un'eccezione a questa regola è costituita dal fatto che gli ID di sito di due dispositivi sono gli stessi. Quando gli ID del sito sono uguali, ma i colori sono pubblici, gli indirizzi IP privati vengono utilizzati per la comunicazione. Ciò può verificarsi per i router SD-WAN che tentano di comunicare con un controller vManage o vSmart situato nello stesso sito. Si noti che, per impostazione predefinita, i router SD-WAN non stabiliscono tunnel VPN IPsec tra loro quando hanno gli stessi ID sito.

```
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#
```

Configurazione Border Gateway Protocol (BGP) sul router SD-WAN del data center per 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
```

Il router SD-WAN del data center apprende il prefisso IP 10.211.1.0/24 dal VPC di transito SD-WAN. Ha un router AWS Direct Connect con indirizzo IP 198.18.0.6 come hop successivo - fare riferimento alla riga 7 qui:

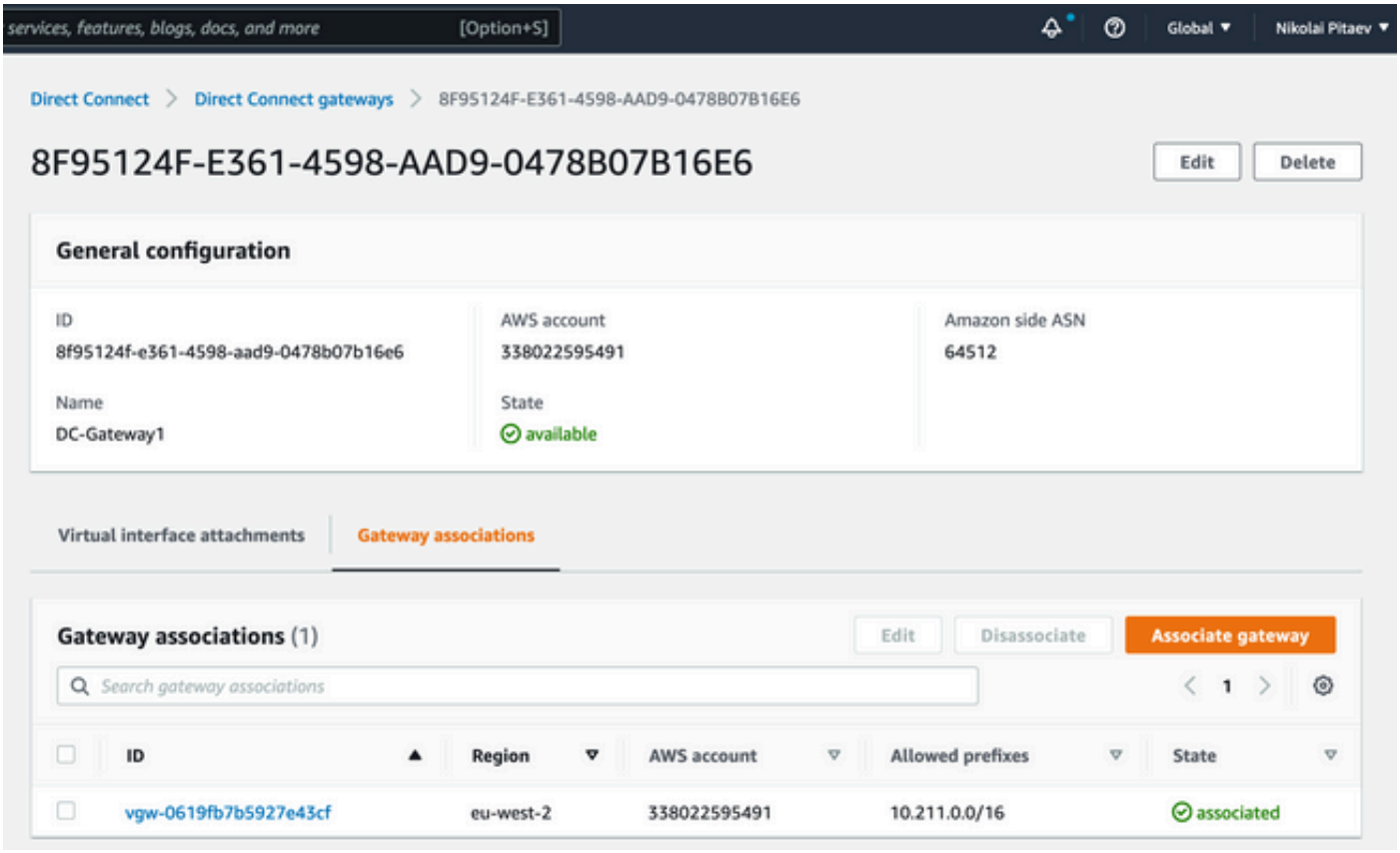
```
DC-MP-CGW1#sh ip ro ... Gateway of last resort is 162.43.145.2 to network 0.0.0.0 S* 0.0.0.0/0
[1/0] via 162.43.145.2 10.0.0.0/24 is subnetted, 1 subnets B 10.211.1.0 [20/0] via 198.18.0.6,
09:15:27 162.43.0.0/16 is variably subnetted, 2 subnets, 2 masks C 162.43.145.2/31 is directly
connected, GigabitEthernet1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

Passaggio 3. Configurazione router AWS-TVPC SD-WAN

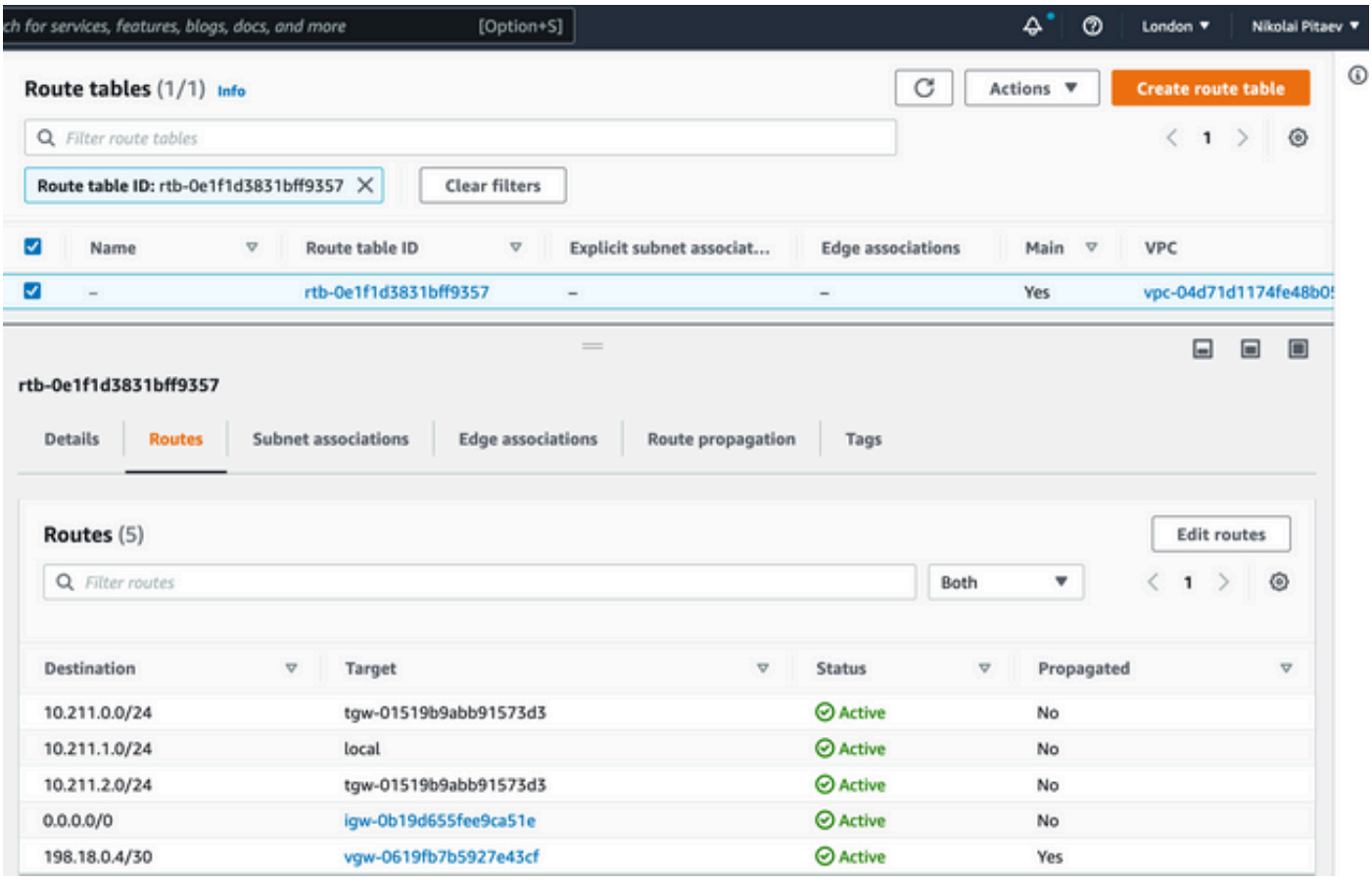
Entrambi i router SD-WAN in AWS Transit VPC sono creati con Cloud onRamp per l'automazione multicolore con modelli vManage predefiniti. Entrambi i router c8kv utilizzano il colore private2 per la connettività Internet pubblica.

Passaggio 4. Configurazione AWS Direct Connect

VGW deve essere creato e associato a VPC di transito SD-WAN nella console AWS o con qualsiasi strumento di automazione cloud. La stessa VGW deve essere associata alla connessione diretta come mostrato di seguito. Notare il prefisso 10.211.0.0/16 del TVPC SD-WAN nei **prefissi consentiti**.



La propagazione della route per il VGW deve essere abilitata nella tabella di routing AWS per il VPC di transito SD-WAN. Vedere l'ultimo percorso per 198.18.0.4/30 in questa immagine. La propagazione route annuncia il DC TLOC alla tabella route VPC in transito.



L'output di **show sdwan bfd session** CLI qui è stato preso da uno dei router SD-WAN c8kv in Transit VPC e mostra due tunnel SD-WAN:

1. Il primo tunnel (vedere linea 5) va via Internet da c8kv in AWS TVPC a Data Center: color private2 > biz-internet. Prendere nota dell'indirizzo IP di destinazione, ovvero l'indirizzo IP pubblico 192.0.2.0 del router del data center. Vedere la configurazione del router nella sezione precedente.
2. Il secondo tunnel (vedere la linea 6) passa attraverso AWS Direct Connect: dal colore private2 al privato1 con 198.18.0.5 come indirizzo IP di destinazione.

```
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#
```

Sicurezza con firewall in Shared Services VPC e AWS GWLB

Un requisito molto comune è quello di ispezionare il traffico est-ovest e nord-sud. In genere, il traffico tra diversi VPC host e/o VPN SD-WAN è soggetto a ispezione del firewall. I firewall virtuali vengono eseguiti in VPC di Shared Services e il bilanciamento del carico può essere implementato con GWLB (AWS Gateway Load Balancer).

Il design descritto funziona molto bene con l'ispezione centralizzata - vedere .

Impostazione per Proof of Concept

Le immagini seguenti vengono utilizzate per creare un'impostazione di prova per Proof of of Concept (PoC):

- vManage: 192.0.2.1R. Non c'è bisogno di questa immagine ingegneristica, deve anche funzionare con 20.6
- c8kv per AWS e Megaport (simulazione connessione diretta/data center):17,4 o 17,5
- AWS Direct Connect è stato simulato con Megaport

Connessione diretta con il provider SDCI Megaport o Equinix

Non è facile ottenere una connessione diretta AWS reale per un ambiente lab. Normalmente è necessario un partner AWS Direct Connect, operazione costosa e che può richiedere tempo.

Tuttavia, se disponi di un account Megaport o Equinix, puoi usarlo per creare un gateway AWS Direct Connect in pochi minuti con Cisco Cloud onRamp per l'automazione multicolore!

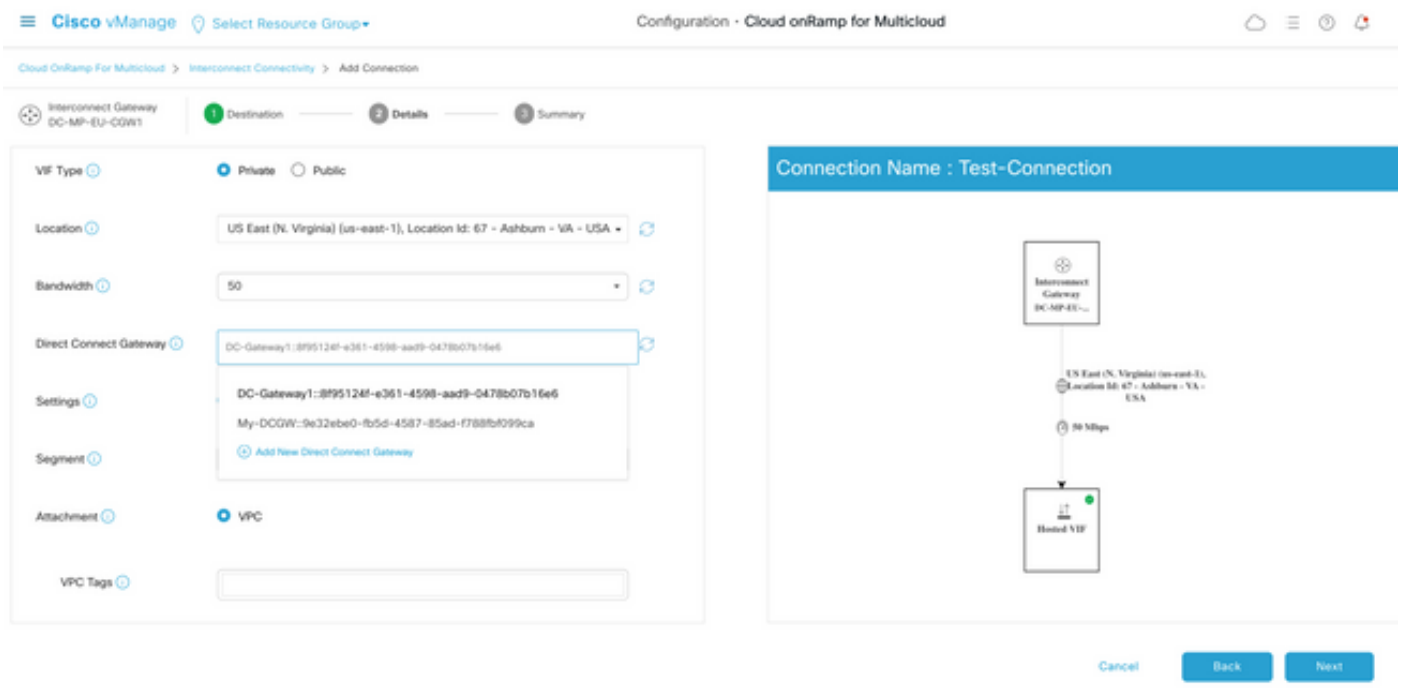
Di seguito è riportato un riepilogo dei passaggi principali, se si dispone già delle credenziali SDCI (Data Center Interconnect) e AWS definite dal software configurate in vManage:

1. Se non si dispone già di due c8kv che agiscono come Cloud Gateway in Transito VPC su AWS, usare Cloud onRamp (CoR) per il flusso di lavoro Multicast per AWS e crearlo nell'area AWS desiderata con il modello di router AWS CoR predefinito con qualsiasi colore privato.
2. In vManage, passare a CoR per la configurazione di interconnessione multicolore e creare un gateway di interconnessione (c8kv) nell'area SDCI desiderata con il modello di router del

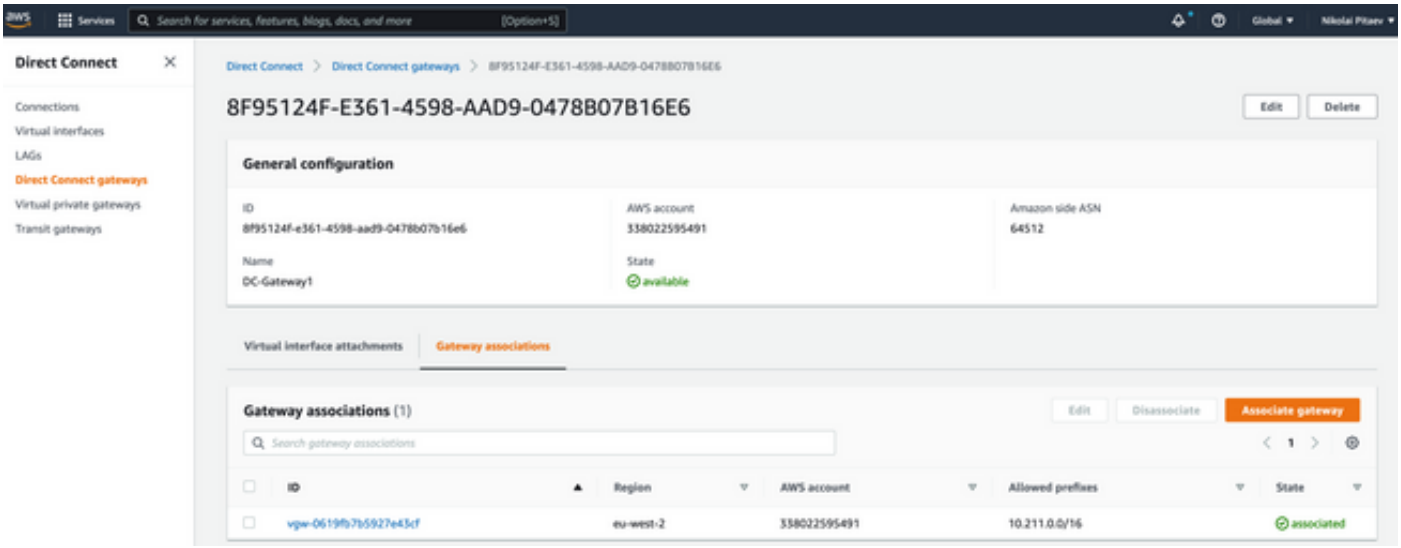
provider SDCI predefinito.

3. Nella pagina Configurazione di interconnessione multicolore di CoR in vManage creare un nuovo tipo di connessione Cloud con interfaccia virtuale privata (VIF). Al momento di questo flusso di lavoro di configurazione, è possibile creare un nuovo gateway AWS Direct Connect e collegarvi un VPC host. Verificare quindi di disporre di un VPC host "fittizio" per questa operazione.
4. Per il nuovo c8kv creato nel passaggio 2, passare dalla modalità di configurazione vManage alla modalità CLI e spostare il tunnel dal lato del servizio alla VPN0 (rimuovere l'istruzione di inoltro vrf). Verificare la connessione BGP e accertarsi di disporre dell'istruzione di rete nella configurazione BGP: network 198.18.0.4 mask 255.255.255.252. Vedere la configurazione completa del router per il data center e i router AWS collegati.
5. In AWS Management Console selezionare il VGW appropriato (o crearne uno nuovo) e abilitare la propagazione della route nelle impostazioni della tabella di route di AWS. Verificare inoltre di aver configurato **i prefissi consentiti** nella sezione Connessione diretta. Fare riferimento all'immagine più avanti in questo capitolo.

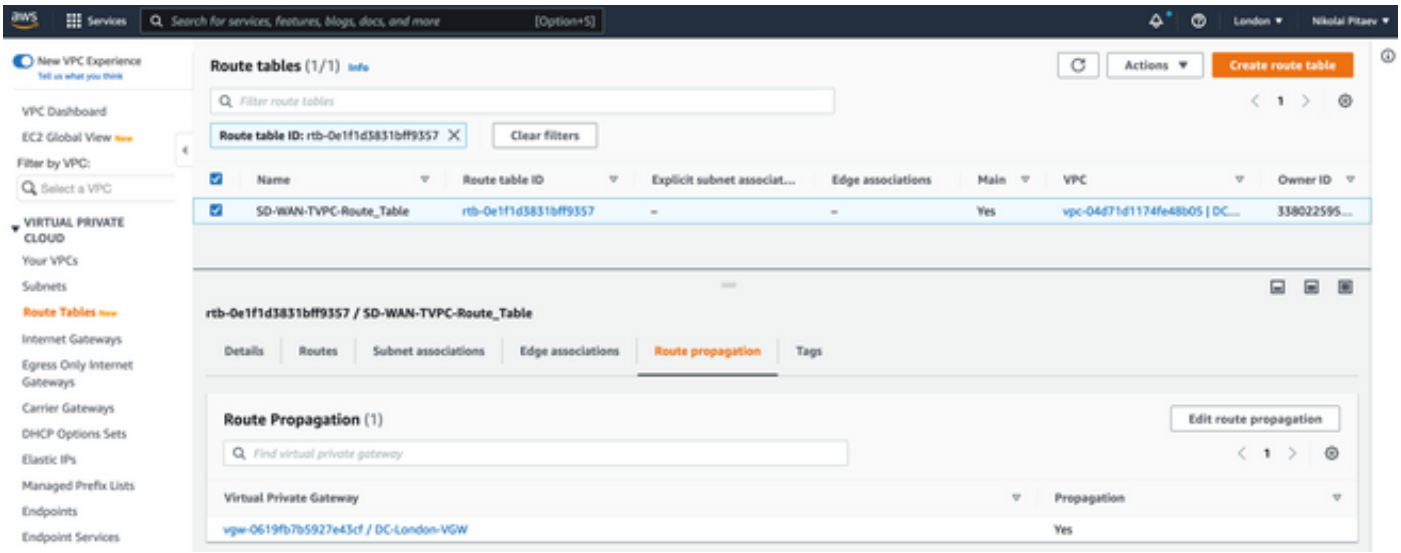
Nell'immagine è illustrata la creazione di una connessione diretta dal passaggio 3.



Come risultato finale, verrà visualizzato un nuovo gateway Direct Connect nella console di gestione AWS, come mostrato di seguito. Notare il campo dei prefissi consentiti, che ha il blocco CIDR del VPC SD-WAN in transito.



Verificare la tabella di routing per il VPC di transito SD-WAN. Deve avere la propagazione con la VGW corretta abilitata, come mostrato nell'immagine.



Fare riferimento a questa sezione per la configurazione completa del router e mostrare gli output.

```
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#
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).