클릭 한 번으로 AWS Direct Connect를 SD-WAN을 통한 전송으로 구성

목차

소개
배경 정보
문제
솔루션
설계 개요
솔루션 세부사항
1단계. 준비
2단계. 데이터 센터 SD-WAN 라우터 컨피그레이션
3단계. AWS TVPC SD-WAN 라우터 컨피그레이션
4단계. AWS Direct Connect 컨피그레이션
Shared Services VPC 및 AWS GWLB의 방화벽을 통한 보안
개념 증명 설정
SDCI 공급자 메가포트 또는 Equinix와 직접 연결

소개

이 문서에서는 Amazon Web Services(AWS) Direct Connect를 SD-WAN(Software-defined Wide Area Network) 전송으로 사용하는 방법에 대해 설명합니다.

배경 정보

Cisco SD-WAN을 위한 또 다른 전송으로서 AWS Direct Connect의 주요 이점은 다음과 같은 전반적인 전송에 SD-WAN 정책을 사용할 수 있다는 것입니다

AWS Direct Connect.

AWS에서 워크로드를 보유한 엔터프라이즈 사용자는 데이터 센터 또는 허브 연결을 위해 AWS Direct Connect를 사용합니다. 또한 공용 인터넷 연결은 데이터 센터에서 매우 일반적이며 다른 위치와의 SD-WAN 연결을 위한 언더레이로 사용됩니다. 이 문서에서는 AWS Direct Connect를 Cisco SD-WAN의 언더레이로 사용하는 방법에 대해 설명합니다. 사용자는 SD-WAN 애플리케이션 인식 정책을 생성하고 Direct Connect를 통해 중요한 애플리케이션을 라우팅하고 SLA(Service Level Agreement) 위반 시 공용 인터넷을 통해 다시 라우팅할 수 있습니다.

문제

AWS Direct Connect는 기본 SD-WAN 기능을 제공하지 않습니다. 엔터프라이즈 SD-WAN 사용자의 일반적인 질문은 다음과 같습니다.

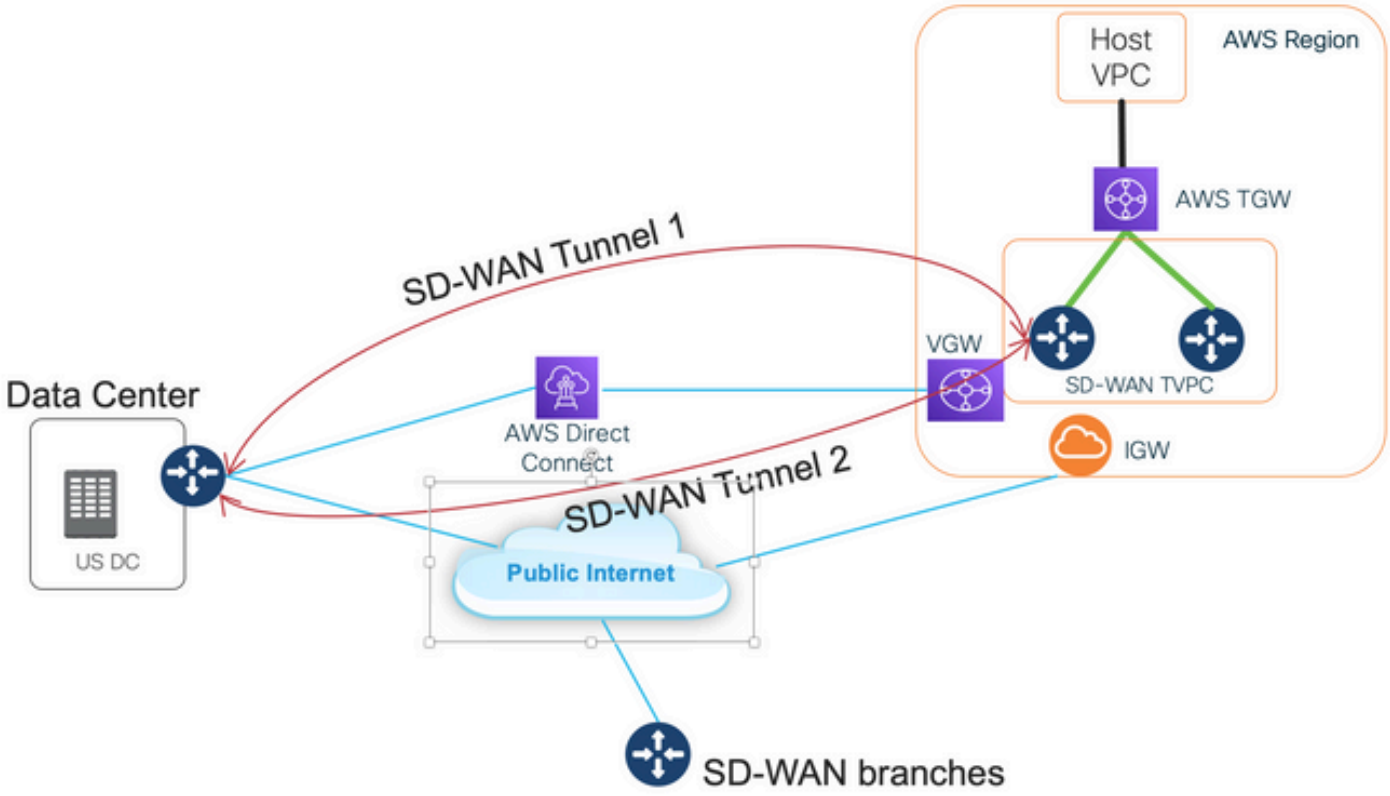
- AWS Direct Connect를 Cisco SD-WAN의 언더레이로 사용할 수 있습니까?
- AWS Direct Connect와 Cisco SD-WAN을 상호 연결하려면 어떻게 해야 합니까?

- 복원력, 보안, 확장성을 갖춘 솔루션을 만들려면 어떻게 해야 합니까?

솔루션

설계 개요

핵심 설계 포인트는 이미지에 표시된 대로 SD-WAN Transit Virtual Private Cloud(VPC)에서 AWS Direct Connect를 통해 VGW(Virtual Gateway)에 데이터 센터를 연결하는 것입니다.

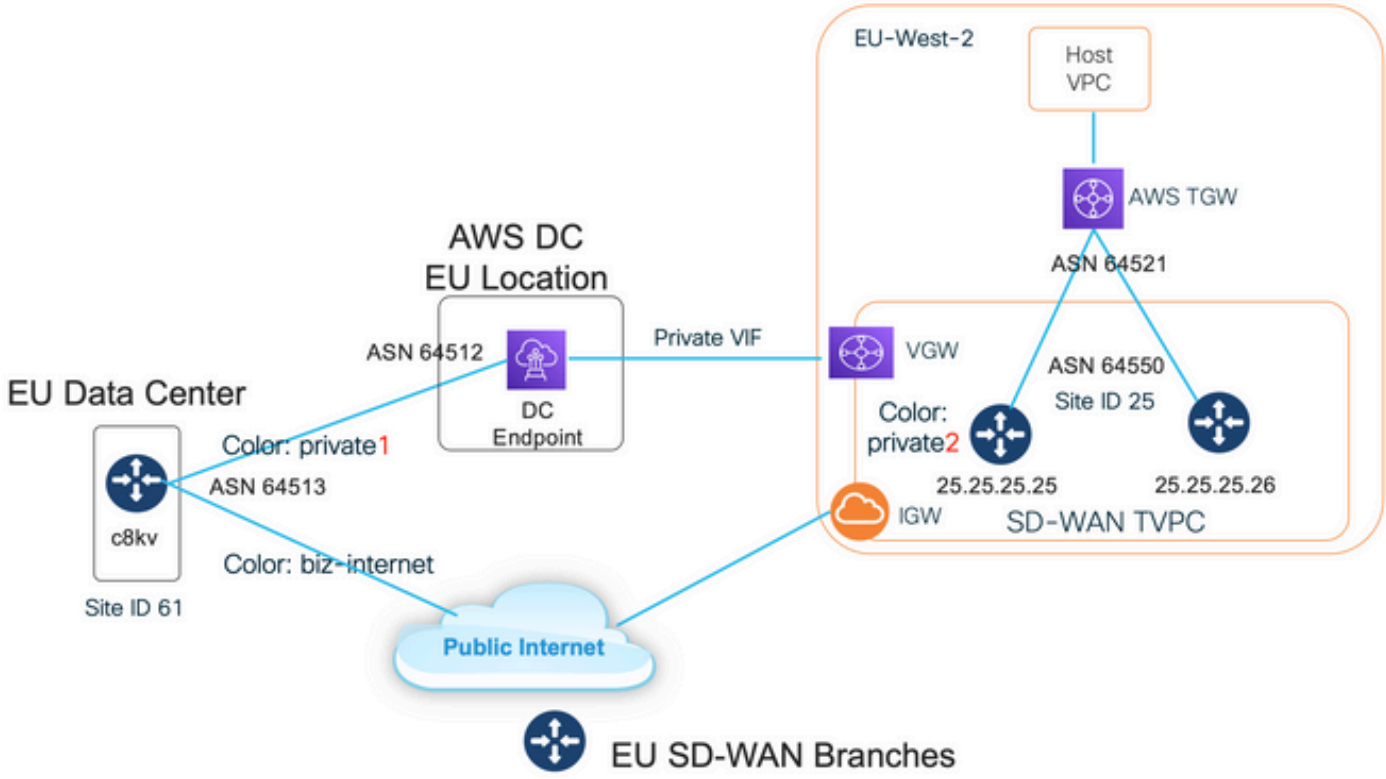


이 솔루션의 이점은 다음과 같습니다.

- 완전 자동: Cisco Cloud onRamp for Multicloud 자동화를 통해 SD-WAN 라우터 2개 및 새로운 AWS TGW(Transit Gateway)가 포함된 SD-WAN 트랜짓 VPC를 구축할 수 있습니다. 호스트 VPC는 Cloud onRamp의 일부로 검색되고 클릭 한 번으로 SD-WAN 네트워크에 매핑될 수 있습니다.
- Full SD-WAN over Direct Connect: AWS Direct Connect는 또 다른 SD-WAN 전송일 뿐입니다. 애플리케이션 인식 정책, 암호화 등의 모든 SD-WAN 기능은 AWS Direct Connect를 통한 SD-WAN 터널에서 기본적으로 사용할 수 있습니다.
- 제안된 설계에서는 AWS Direct Connect(20/100)보다 많은 접두사 수의 AWS 제한을 방지합니다.

솔루션 세부사항

이 그림에서는 SD-WAN 트랜짓 VPC에서 VGW에 직접 연결(color private1)을 통해 그리고 공용 인터넷(color biz-internet)을 통해 연결된 AWS 리전 및 데이터 센터 하나를 보여 줍니다. AWS SD-WAN c8kv 라우터는 인터넷 연결에 SD-WAN color private2를 사용합니다.



1단계. 준비

Cisco vManage에 활성 AWS 계정이 정의되어 있고 Cloud onRamp Global Settings가 올바르게 구성되어 있는지 확인합니다.

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

2단계. 데이터 센터 SD-WAN 라우터 컨피그레이션

인터페이스 GigabitEthernet1은 컬러 비즈-인터넷과의 공용 인터넷 연결에 사용되며 인터페이스 GigabitEthernet1.1352는 컬러 private1을 사용하는 AWS Direct Connect에 사용됩니다.

AWS SD-WAN 라우터에는 인터넷 연결뿐만 아니라 직접 **연결을** 통한 연결을 위해 **프라이빗 컬러** 프라이빗**2**가 있습니다. SD-WAN 터널은 공용 IP 주소로 인터넷을 통해 형성되고 SD-WAN 터널은 사설 IP 주소가 있는 직접 연결 회로를 통해 DC/사이트에 설정됩니다(동일한 인터페이스로). 즉, 데이터 센터 라우터(biz-internet 색상)가 공용 IP 주소를 사용하는 인터넷과 사설 IP를 사용하는 사설 색상을 통해 AWS SD-WAN 라우터(private2 색상)에 대한 연결을 설정합니다.

SD-WAN 색상에 대한 일반 정보:

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

SD-WAN 라우터 및/또는 컨트롤러(vManage, vSmart 또는 vBond)는 네트워크 내 NAT(Network Address Translation) 디바이스 뒤에 있을 수 있습니다. SD-WAN 라우터가 vBond 컨트롤러에 인증

되면 vBond 컨트롤러는 SD-WAN 라우터의 사설 IP 주소/포트 번호 및 공용 IP 주소/포트 번호 설정을 교환 시 학습합니다. vBond 컨트롤러는 NAT(STUN) 서버에 대한 세션 접근 유틸리티의 역할을 하며 SD-WAN 라우터가 WAN 전송 인터페이스의 매핑된 IP 주소 및/또는 변환된 IP 주소와 포트 번호를 검색할 수 있도록 합니다.

SD-WAN 라우터에서 모든 WAN 전송은 퍼블릭 및 프라이빗 IP 주소 쌍과 연결됩니다. 프라이빗 IP 주소는 사전 NAT 주소로 간주됩니다. SD-WAN 라우터의 WAN 인터페이스에 할당된 IP 주소입니다. 이 주소는 사설 IP 주소로 간주되지만, 이 IP 주소는 공개적으로 라우팅 가능한 IP 주소 공간의 일부 또는 IETF RFC 1918 non-public 라우팅 가능한 IP 주소 공간의 일부가 될 수 있습니다. 공용 IP 주소는 사후 NAT 주소로 간주됩니다. 이는 SD-WAN 라우터가 vBond 서버와 처음 통신하고 인증할 때 vBond 서버에서 탐지됩니다. 공용 IP 주소는 또한 공개적으로 라우팅 가능한 IP 주소 공간의 일부 또는 IETF RFC 1918 non-public 라우팅 가능한 IP 주소 공간의 일부일 수 있습니다. NAT가 없을 경우 SD-WAN 전송 인터페이스의 공용 IP 주소와 사설 IP 주소가 모두 동일합니다.

TLOC 색상은 각 SD-WAN 라우터에서 개별 WAN 전송을 식별하는 데 사용되는 정적으로 정의된 키워드입니다. 지정된 SD-WAN 라우터의 각 WAN 전송에는 고유한 색상이 있어야 합니다. 색깔은 개별 WAN 전송을 공용 또는 전용으로 식별하는 데에도 사용됩니다. metro-ethernet, Mpls 및 private1, private2, private3, private4, private5 및 private6 색상은 전용 색상으로 간주됩니다. 전용 네트워크 또는 NAT가 없는 곳에서 사용하도록 만들어졌습니다. 색상은 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, public-internet, red 및 silver이며 공용 색상으로 간주됩니다. 이 인터페이스는 공용 네트워크 또는 WAN 전송 인터페이스의 공용 IP 주소 지정이 있는 장소에서 기본적으로 또는 NAT를 통해 사용됩니다.

색은 제어 및 데이터 평면을 통해 통신할 때 프라이빗 또는 퍼블릭 IP 주소의 사용을 나타냅니다. 두 SD-WAN 라우터가 서로 통신하려고 할 때 두 라우터는 모두 전용 색상으로 된 WAN 전송 인터페이스를 사용하며, 각 라우터는 원격 라우터의 전용 IP 주소에 연결을 시도합니다. 한 쪽 또는 양쪽에서 공용 색상을 사용하는 경우 각 쪽은 원격 라우터의 공용 IP 주소에 연결을 시도합니다. 단, 두 디바이스의 사이트 ID가 동일한 경우는 예외입니다. 사이트 ID는 동일하지만 색상이 공용인 경우 통신에 사설 IP 주소가 사용됩니다. 이는 동일한 사이트 내에 있는 vManage 또는 vSmart 컨트롤러와 통신을 시도하는 SD-WAN 라우터에 대해 발생할 수 있습니다. SD-WAN 라우터는 동일한 사이트 ID를 가질 때 기본적으로 서로 간에 IPsec VPN 터널을 설정하지 않습니다.

```
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#
```

AWS Direct Connect용 Data Center SD-WAN 라우터의 BGP(Border Gateway Protocol) 구성:

```
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
```

데이터 센터 SD-WAN 라우터는 SD-WAN 트랜짓 VPC에서 IP 접두사 10.211.1.0/24을 학습합니다. IP 주소 198.18.0.6을 next-hop으로 사용하는 AWS Direct Connect Router가 있습니다. 여기서 7번

행을 참조하십시오.

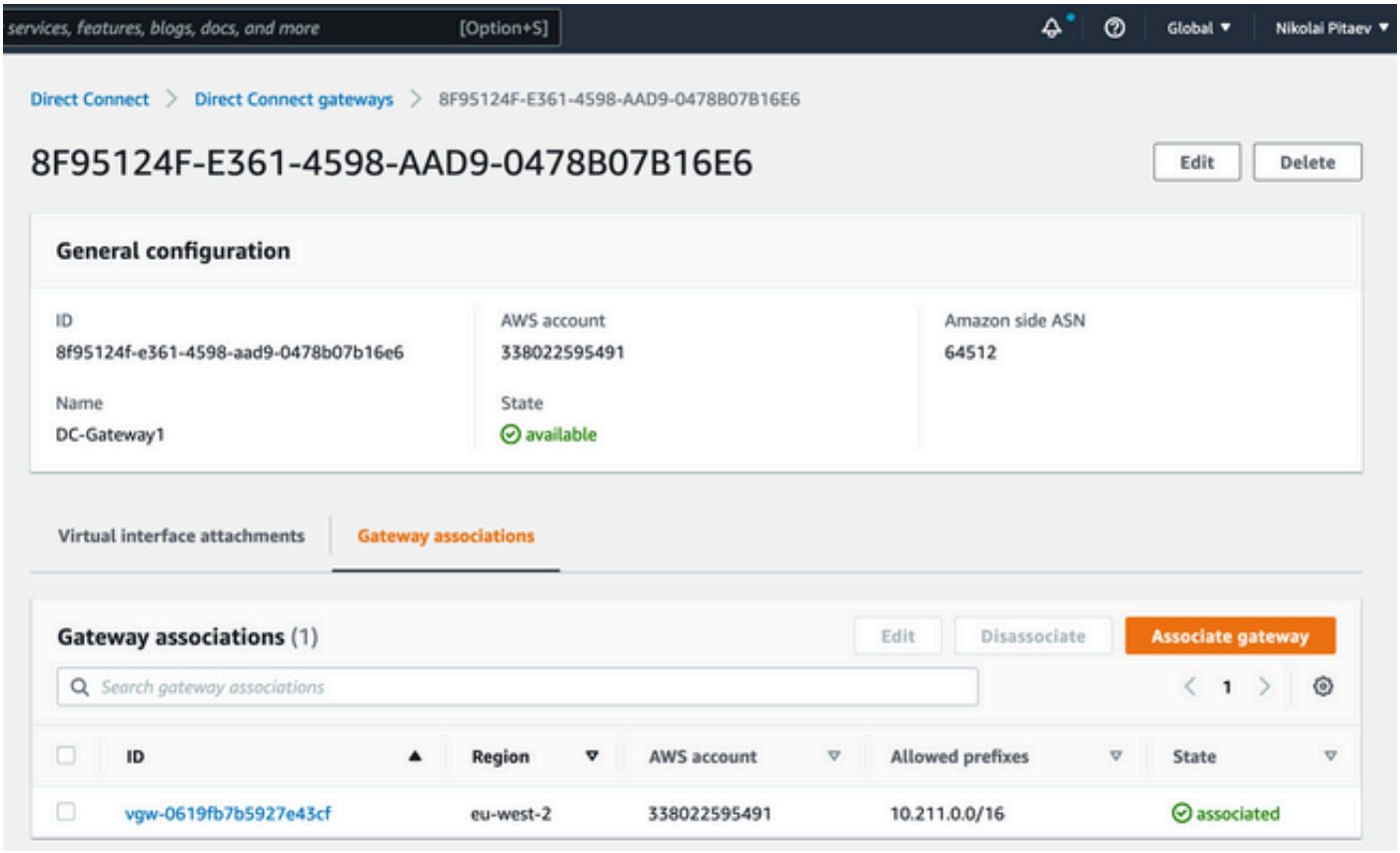
```
DC-MP-CGW1#sh ip ro ... Gateway of last resort is 162.43.145.2 to network 0.0.0.0 S* 0.0.0.0/0
[1/0] via 162.43.145.2 10.0.0.0/24 is subnetted, 1 subnets B 10.211.1.0 [20/0] via 198.18.0.6,
09:15:27 162.43.0.0/16 is variably subnetted, 2 subnets, 2 masks C 162.43.145.2/31 is directly
connected, GigabitEthernet1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

3단계. AWS TVPC SD-WAN 라우터 컨피그레이션

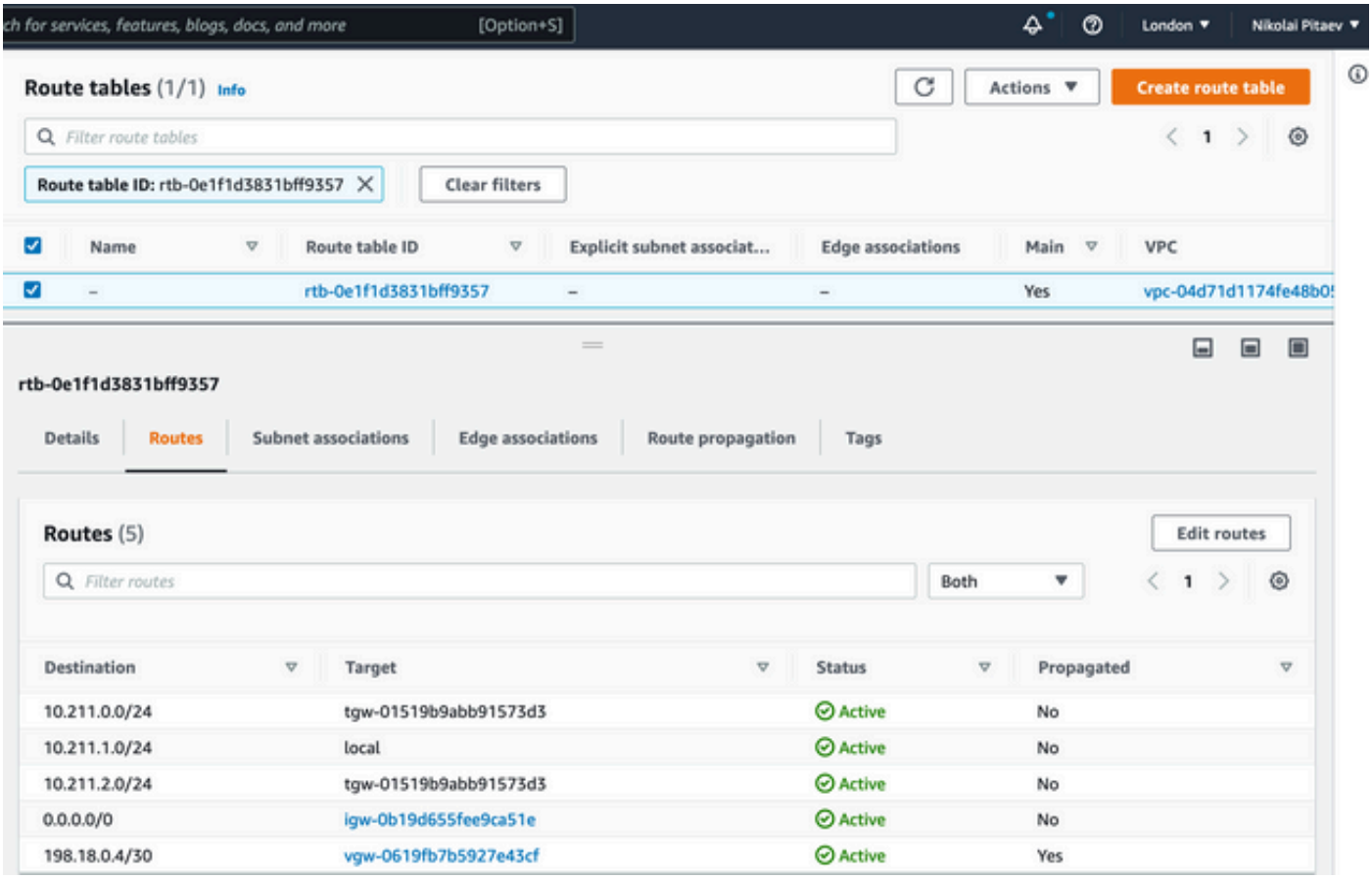
AWS Transit VPC의 두 SD-WAN 라우터는 모두 기본 vManage 템플릿을 사용하는 멀티클라우드 자동화를 위한 Cloud onRamp로 생성됩니다. 두 c8kv 라우터 모두 공용 인터넷 연결에 private2 색상을 사용합니다.

4단계. AWS Direct Connect 컨피그레이션

VGW는 AWS 콘솔에서 SD-WAN 트랜짓 VPC를 생성하고 연결하거나 클라우드 자동화 툴과 연결해야 합니다. 동일한 VGW를 여기에 표시된 대로 Direct Connect와 연결해야 합니다. 허용되는 접두사 아래에 SD-WAN TVPC 접두사 10.211.0.0/16을 **기록해 두십시오**.



VGW의 경로 전파는 SD-WAN 트랜짓 VPC의 AWS 경로 테이블에서 활성화되어야 합니다. 이 이미지의 198.18.0.4/30에 대한 마지막 경로를 참조하십시오. 경로 전파는 트랜짓 VPC 경로 테이블에 DC TLOC를 다시 광고합니다.



여기서 **show sdwan bfd sessions CLI**의 출력은 Transit VPC의 c8kv SD-WAN 라우터 중 하나에서 가져왔으며 두 개의 SD-WAN 터널을 보여줍니다.

1. 첫 번째 터널(5행 참조)은 인터넷을 통해 AWS TVPC의 c8kv에서 데이터 센터: color private2 > biz-internet으로 이동합니다. 대상 IP 주소(데이터 센터 라우터의 공용 IP 주소 192.0.2.0)를 확인합니다. 이전 섹션의 라우터 컨피그레이션을 참조하십시오.
2. 두 번째 터널(6번 행 참조)은 AWS Direct Connect를 통해 컬러 private2에서 목적지 IP 주소로 198.18.0.5를 사용하는 private1로 이동합니다.

```
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#
```

Shared Services VPC 및 AWS GWLB의 방화벽을 통한 보안

매우 일반적인 요구 사항은 동-서 및 남북 트래픽을 검사하는 것입니다. 일반적으로 서로 다른 호스트 VPC 및/또는 SD-WAN VPN 간의 모든 트래픽은 방화벽 검사의 대상이 됩니다. 가상 방화벽은 Shared Services VPC에서 실행되고 로드 밸런싱은 AWS GWLB(Gateway Load Balancer)를 사용하여 구현할 수 있습니다.

설명된 설계는 중앙 집중식 검사에서 매우 잘 작동합니다. 을/를 참조하십시오.

개념 증명 설정

다음 이미지는 PoC(개념 증명)를 위한 테스트 설정을 만드는 데 사용됩니다.

- vManage: 192.0.2.1R 이 엔지니어링 이미지는 필요 없으며 20.6과 함께 작동해야 합니다.
- c8kv for AWS and Megaport (Direct Connect / Data Center 시뮬레이션):17.4 또는 17.5
- AWS Direct Connect를 Megaport로 시뮬레이션했습니다.

SDCI 공급자 메가포트 또는 Equinix와 직접 연결

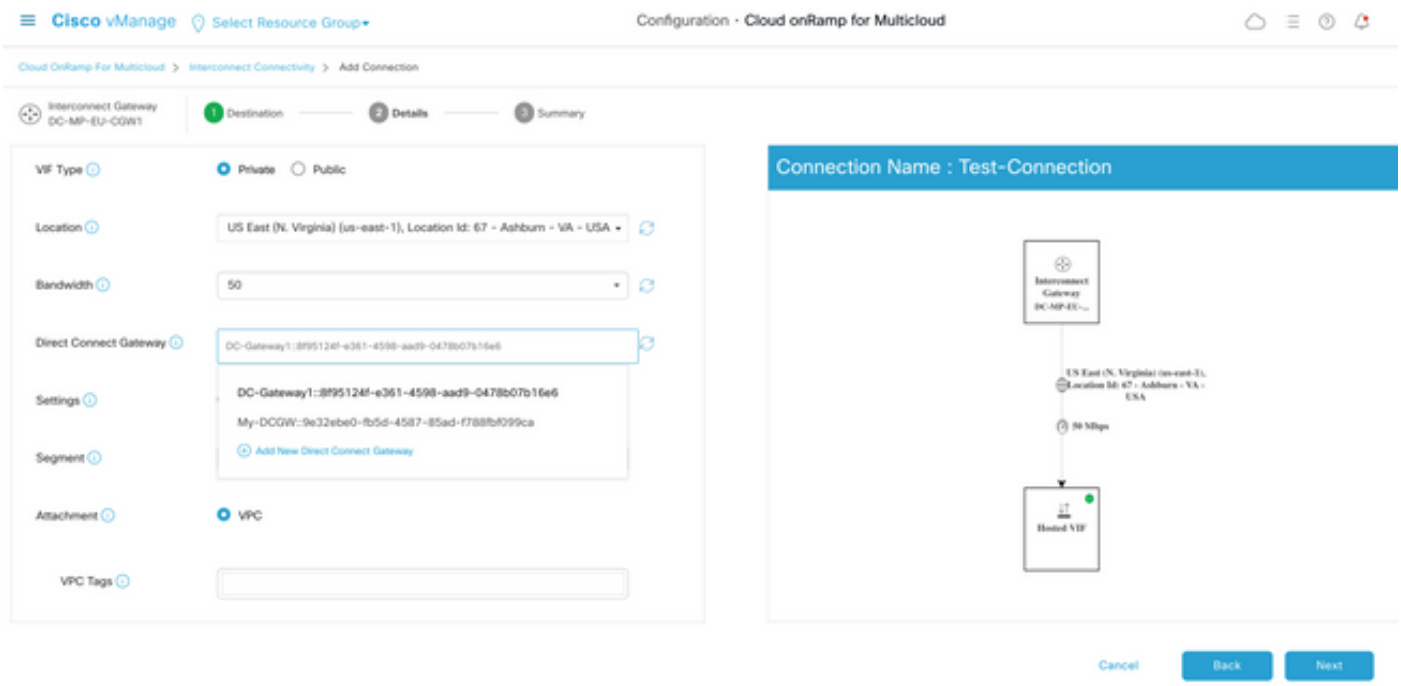
실습 환경에서 실제 AWS Direct Connect를 사용하는 것은 쉽지 않습니다. 일반적으로 AWS Direct Connect 파트너가 필요하므로 많은 비용과 시간이 소요됩니다.

그러나 Megaport 또는 Equinix 계정이 있는 경우, 이를 사용하여 Cisco Cloud onRamp for Multicloud 자동화를 통해 몇 분 내에 AWS Direct Connect 게이트웨이를 만들 수 있습니다!

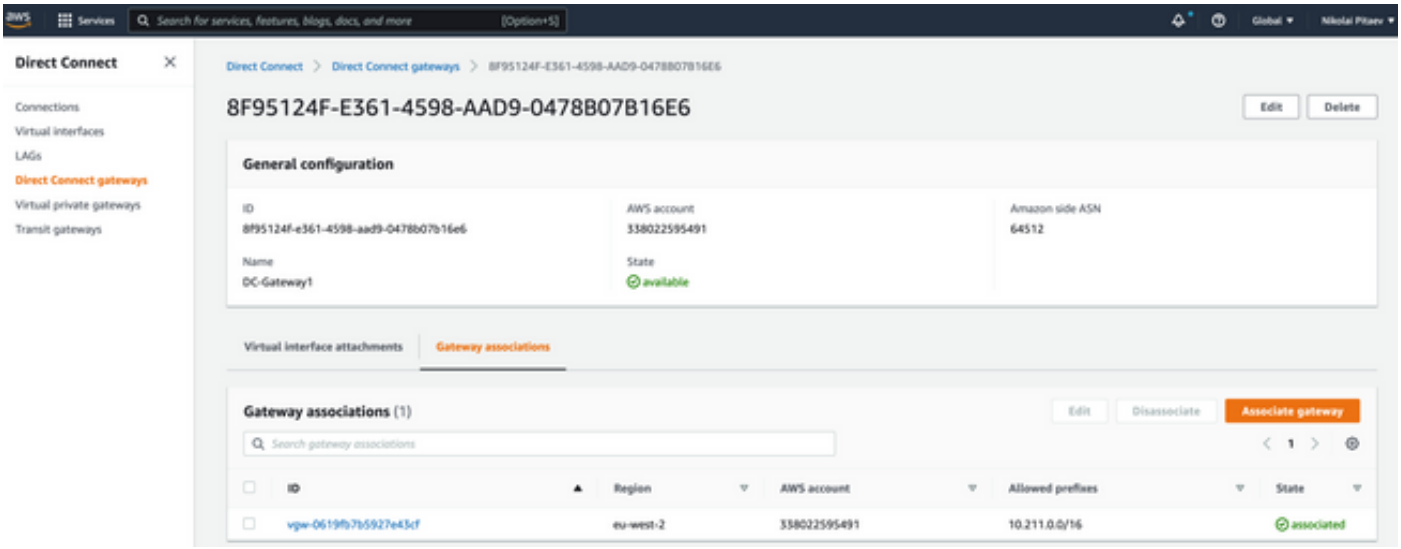
vManage에 SDCI(Software-defined Data Center Interconnect) 및 AWS 자격 증명이 구성되어 있는 경우, 주요 단계를 요약하면 다음과 같습니다.

1. AWS의 트랜짓 VPC에서 클라우드 게이트웨이 역할을 하는 2개의 c8kv가 없는 경우, AWS용 Multicloud 워크플로용 Cloud onRamp(CoR)를 사용하고 프라이빗 컬러의 기본 AWS CoR 라우터 템플릿으로 원하는 AWS 리전에서 생성하십시오.
2. vManage에서 Multicoloud Interconnect 컨피그레이션에 대한 CoR로 이동하고 기본 SDCI 제공자 라우터 템플릿을 사용하여 원하는 SDCI 영역에 Interconnect Gateway(c8kv)를 생성합니다.
3. vManage의 CoR Multicoloud Interconnect Configuration(CoR 멀티 클라우드 상호 연결 컨피그레이션) 페이지에서 VIF(Private Virtual Interface)를 사용하여 새 연결 유형 클라우드를 생성합니다. 이 컨피그레이션 워크플로를 진행할 때 새 AWS Direct Connect 게이트웨이를 생성하고 호스트 VPC를 연결하는 옵션이 있습니다. 따라서 이 단계에 대해 "더미" 호스트 VPC가 있는지 확인합니다.
4. 2단계에서 생성한 새 c8kv의 경우 vManage 컨피그레이션 모드에서 CLI 모드로 전환하고 서비스 측에서 VPN0으로 터널을 이동합니다(vrf forwarding statement 제거). BGP 연결을 확인하고 BGP 컨피그레이션에 network 명령문이 있는지 확인합니다. network 198.18.0.4 mask 255.255.252. 연결된 데이터 센터 및 AWS 라우터에 대한 전체 라우터 컨피그레이션을 참조하십시오.
5. AWS Management Console에서 적절한 VGW를 선택하거나 새 VGW를 생성하고 AWS Route Table 설정에서 경로 전파를 활성화합니다. 또한 Direct Connect 섹션에서 **허용된 접두사**를 구성했는지 확인합니다. 이 장의 뒷부분에 있는 이미지를 참조하십시오.

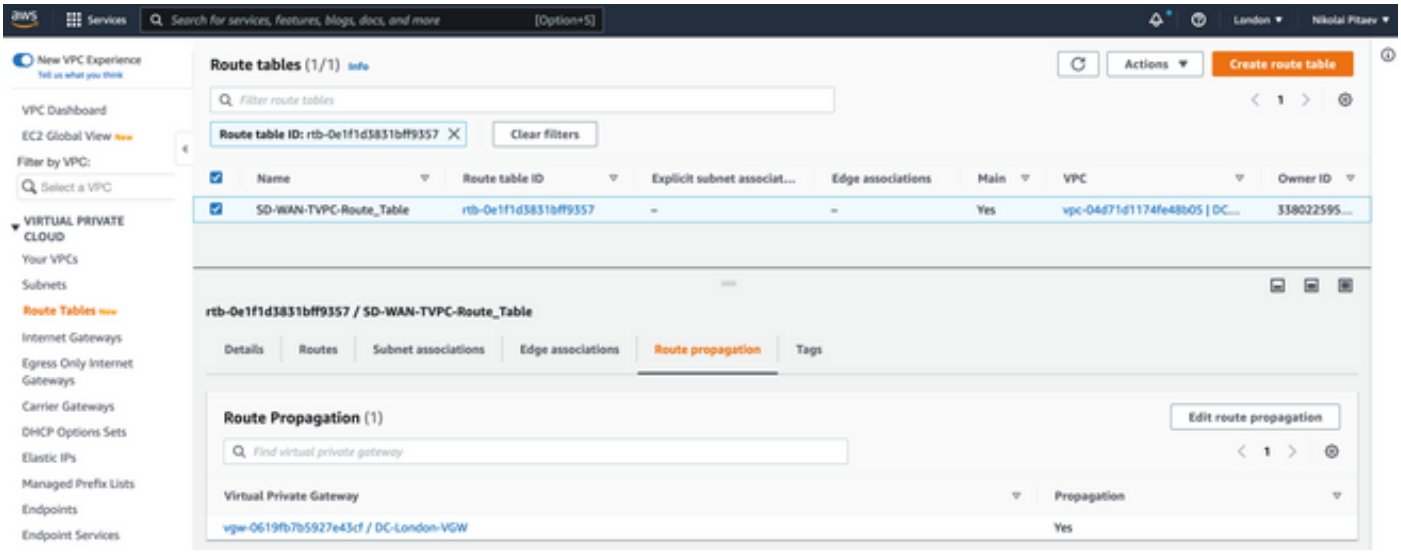
이 이미지는 3단계에서 직접 연결을 생성하는 방법을 보여줍니다.



결과적으로 여기에 표시된 것처럼 AWS Management Console에 새로운 Direct Connect 게이트웨이가 표시됩니다. 트랜짓 SD-WAN VPC의 CIDR 블록이 있는 허용되는 접두사 필드에 유의하십시오.



SD-WAN 트랜짓 VPC에 대한 경로 테이블을 다시 확인합니다. 이미지에 표시된 대로 올바른 VGW가 활성화된 전파가 있어야 합니다.



전체 라우터 컨피그레이션 및 표시 출력은 이 섹션을 참조하십시오.

```
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
```

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

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

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#

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.