

# Configuration du routeur de périphérie SD-WAN pour le déploiement en ligne

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer Cisco SD-WAN Edge avec le transport MPLS pour accéder aux contrôleurs Cisco SD-WAN sur Internet via la périphérie WAN CC en ligne.

## Conditions préalables

### Exigences

Cisco recommande de connaître les sujets suivants :

- Réseau étendu défini par logiciel Cisco (SD-WAN)
- Routage

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco vManage version 20.6.5.2
- Routeur Cisco WAN Edge version 17.06.05

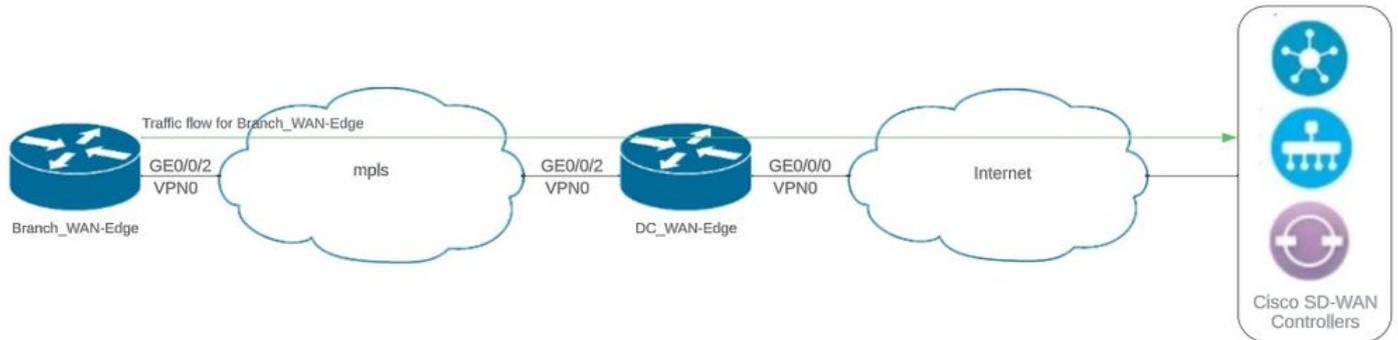
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Dans un déploiement de périphérie WAN DC en ligne, le trafic de contrôle entrant du MPLS doit atteindre les contrôleurs SD-WAN sur Internet. Le trafic peut être routé entre MPLS et Internet dans VPN 0.

Dans ce cas, la configuration du tunnel doit être supprimée des interfaces physiques MPLS et Internet et placée sur deux interfaces de bouclage distinctes.

## Diagramme du réseau



Topologie du réseau

## Configurations

Dans ce déploiement, le périphérique de périphérie WAN de la filiale doit accéder aux contrôleurs via la périphérie WAN du data center. Dans ce scénario, une interface physique supplémentaire est ajoutée dans le VPN 0 sur la périphérie WAN CC et les tunnels sont déplacés de l'interface physique vers l'interface de bouclage.

Le déplacement du tunnel de l'interface physique à l'interface de bouclage permet au routeur de périphérie WAN CC d'agir comme un transit pour le trafic de la périphérie WAN CC et du routeur de périphérie WAN de filiale. Il doit y avoir une connectivité entre les adresses IP de bouclage et les contrôleurs pour former le plan de contrôle et de données.

Cette sortie capture la configuration de l'interface WAN de périphérie CC :

```
interface GigabitEthernet0/0/0
 ip address 10.201.186.175 255.255.255.224
 no shutdown
!
interface GigabitEthernet0/0/2
 description connection to Branch_WAN-Edge
 ip address 192.168.20.21 255.255.255.252
 no shutdown
!
interface Loopback1
 description wan_color_green
 ip address 192.168.20.2 255.255.255.255
 no shutdown
!
interface Loopback2
 description wan_color_custom2
```

```
ip address 192.168.20.10 255.255.255.255
no shutdown
!
```

Le résultat suivant capture la configuration du tunnel de périphérie WAN CC :

```
DC_WAN-Edge#sh sdwan running-config sdwan
```

```
sdwan
interface Loopback1
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color green
  no last-resort-circuit
  no low-bandwidth-link
  max-control-connections 1
  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
  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
interface Loopback2
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color custom2 restrict
  no last-resort-circuit
  no low-bandwidth-link
  max-control-connections 1
  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
  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
!
```

Le résultat suivant capture la configuration du tunnel Branch\_WAN-Edge :

```
Branch_WAN-Edge#sh sdwan run sdwan
sdwan
interface GigabitEthernet0/0/2
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color custom2
  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
  no 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 http
  no allow-service snmp
  no allow-service bfd
exit
exit
!
```

## Vérification

Le résultat suivant capture la connectivité du plan de contrôle pour DC\_WAN-Edge.

```
DC_WAN-Edge#sh sdwan control connections
```

```

PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT ORGANIZATION LOCAL COLOR PROXY STATE UPTIME ID
-----
vsmart dtls 10.10.10.2 1 1 10.201.186.172 12346 10.201.186.172 12346 rch_sdwan_lab custom2 No up 0:00:00
vsmart dtls 10.10.10.2 1 1 10.201.186.172 12346 10.201.186.172 12346 rch_sdwan_lab green No up 0:00:00
vmanage dtls 10.10.10.1 1 0 10.201.186.171 12746 10.201.186.171 12746 rch_sdwan_lab green No up 0:00:00

```

Le résultat suivant capture la connectivité du plan de contrôle pour Branch\_WAN-Edge.

```

Branch_WAN-Edge#show sdwan control connections
PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR PROXY STATE UPTIME ID
-----
vsmart dtls 10.10.10.2 1 1 10.201.186.172 12346 10.201.186.172 12346 custom2 No up 0:00:00:20 0
vmanage dtls 10.10.10.1 1 0 10.201.186.171 12346 10.201.186.171 12346 custom2 No up 0:00:00:22 0

```

Le résultat suivant capture la connectivité du plan de données pour DC\_WAN-Edge. La couleur locale verte crée une session BFD avec les périphériques de périphérie distants.

```

DC_WAN-Edge#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec) UPTIME TRANSITIONS
-----
10.10.10.60 60 up green biz-internet 192.168.20.2 10.201.186.167 12346 ipsec 7 1000 0:00:06:37 6
10.10.10.20 20 up green biz-internet 192.168.20.2 10.201.186.180 12346 ipsec 7 1000 0:00:06:37 6
10.10.10.5 5 up green default 192.168.20.2 10.201.186.181 12346 ipsec 7 1000 0:00:06:37 6
10.10.10.10 10 up green gold 192.168.20.2 10.201.186.182 12346 ipsec 7 1000 0:00:06:37 6

```

Le résultat suivant capture la connectivité du plan de données pour Branch\_WAN-Edge. La couleur locale custom2 crée une session BFD avec des périphériques de périphérie distants.

```

Branch_WAN-Edge#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec) UPTIME TRANSITIONS
-----
10.10.10.5 5 up custom2 default 192.168.20.22 10.201.186.181 12346 ipsec 7 1000 0:00:07:37 2
10.10.10.10 10 up custom2 gold 192.168.20.22 10.201.186.182 12346 ipsec 7 1000 0:00:07:37 2
10.10.10.20 20 up custom2 biz-internet 192.168.20.22 10.201.186.180 12346 ipsec 7 1000 0:00:07:37 2
10.10.10.60 60 up custom2 biz-internet 192.168.20.22 10.201.186.167 12346 ipsec 7 1000 0:00:07:37 2

```

## Informations connexes

- [Guide de conception SD-WAN de Cisco](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.