Adresse Nombre de limites de tunnel du plan de données dans le centre de données

Table des matières

Introduction

Ce document décrit une solution permettant de résoudre les problèmes d'évolutivité des bords SD-WAN du centre de données à mesure qu'ils approchent des limites de leur tunnel de plan de données.

Conditions préalables

Exigences

Cisco recommande que vous ayez une bonne connaissance du SD-WAN.

Composants utilisés

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

- Contrôleur SD-WAN version 20.6.3.0.54 (ES)
- Cisco IOS® XE (exécution en mode contrôleur) 17.06.03a.0.2 (ES)

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.

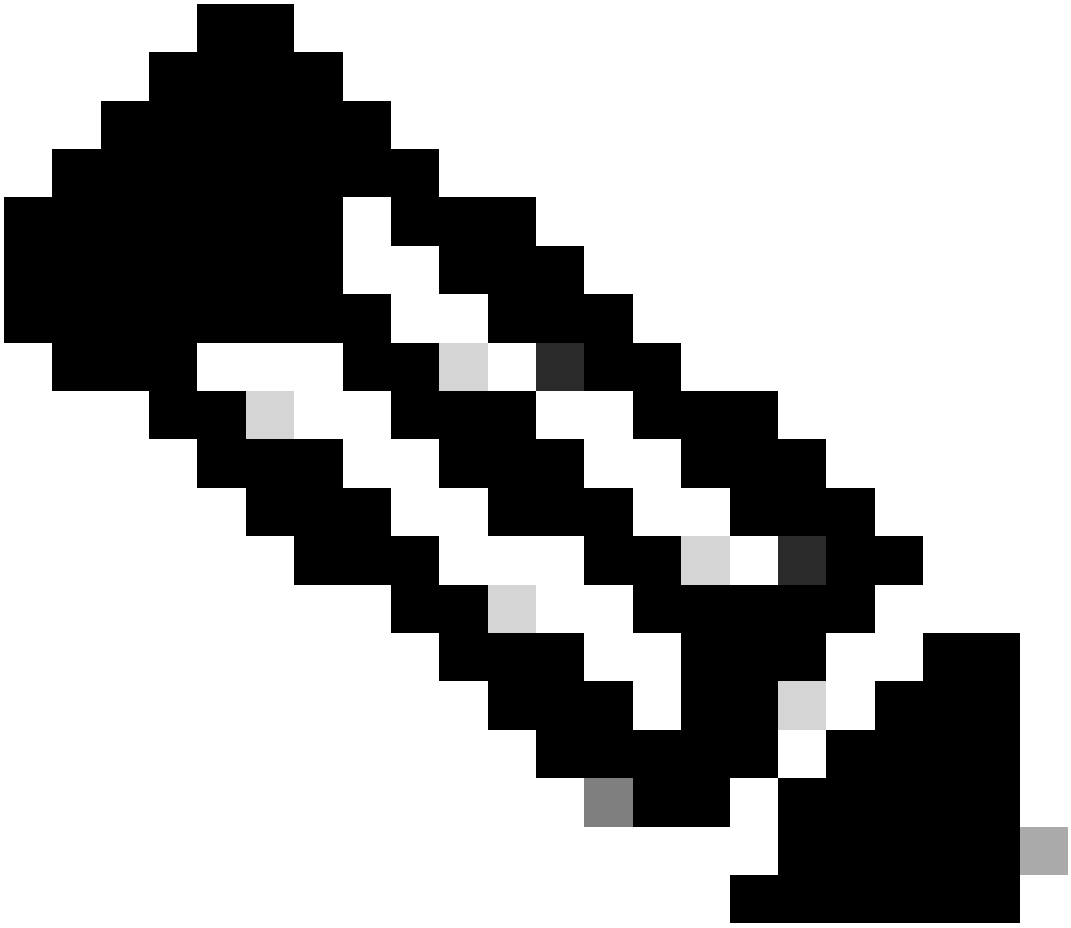
Informations générales

Présentation de la conception réseau :

- VPN : VPN 10, VPN 20
- Liaisons de transport : Multiprotocol Label Switching (MPLS), LTE, Internet
- Détail du routeur :
    - Routeur principal : 2 dans chaque data center
      - Modèle : ASR1002-HX
      - Version du logiciel Cisco IOS XE : 17.06.03a.0.2
    - Routeur secondaire : 1 dans chaque data center
      - Modèle : ISR4451-X
      - Version du logiciel Cisco IOS XE : 17.06.03a.0.22
- Protocole de routage : le protocole BGP (Border Gateway Protocol) est utilisé côté LAN du data center

Problème

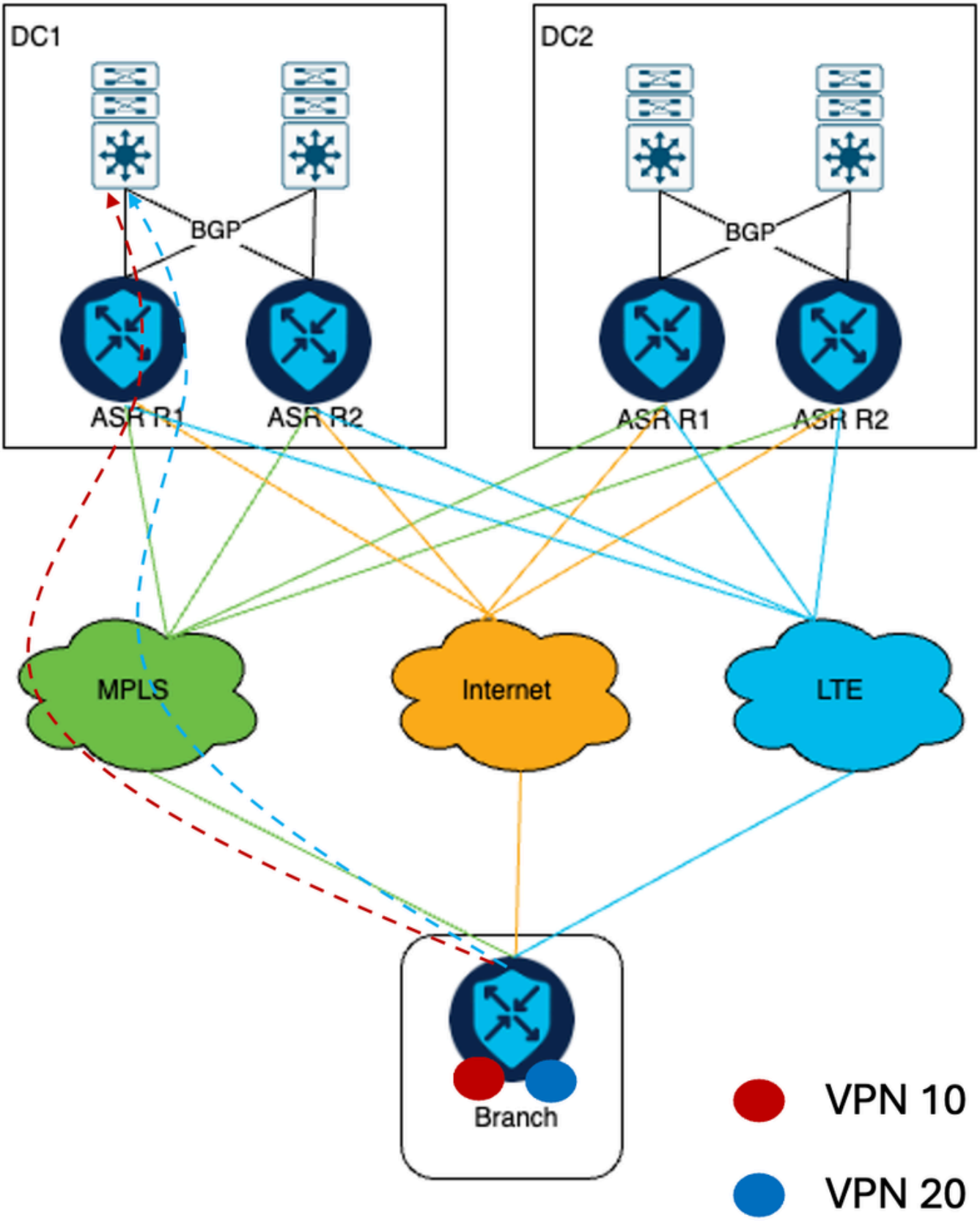
Ce document présente l'étude de cas du client présentant la topologie illustrée. L'infrastructure réseau du client comprend deux data centers, chacun ayant deux serveurs ASR1002-HX SD-WAN cEdge déployés. Cette architecture réseau vise à intégrer environ 3 000 emplacements de magasin sur la superposition SD-WAN, en tirant parti de la disponibilité de trois liaisons de transport distinctes.



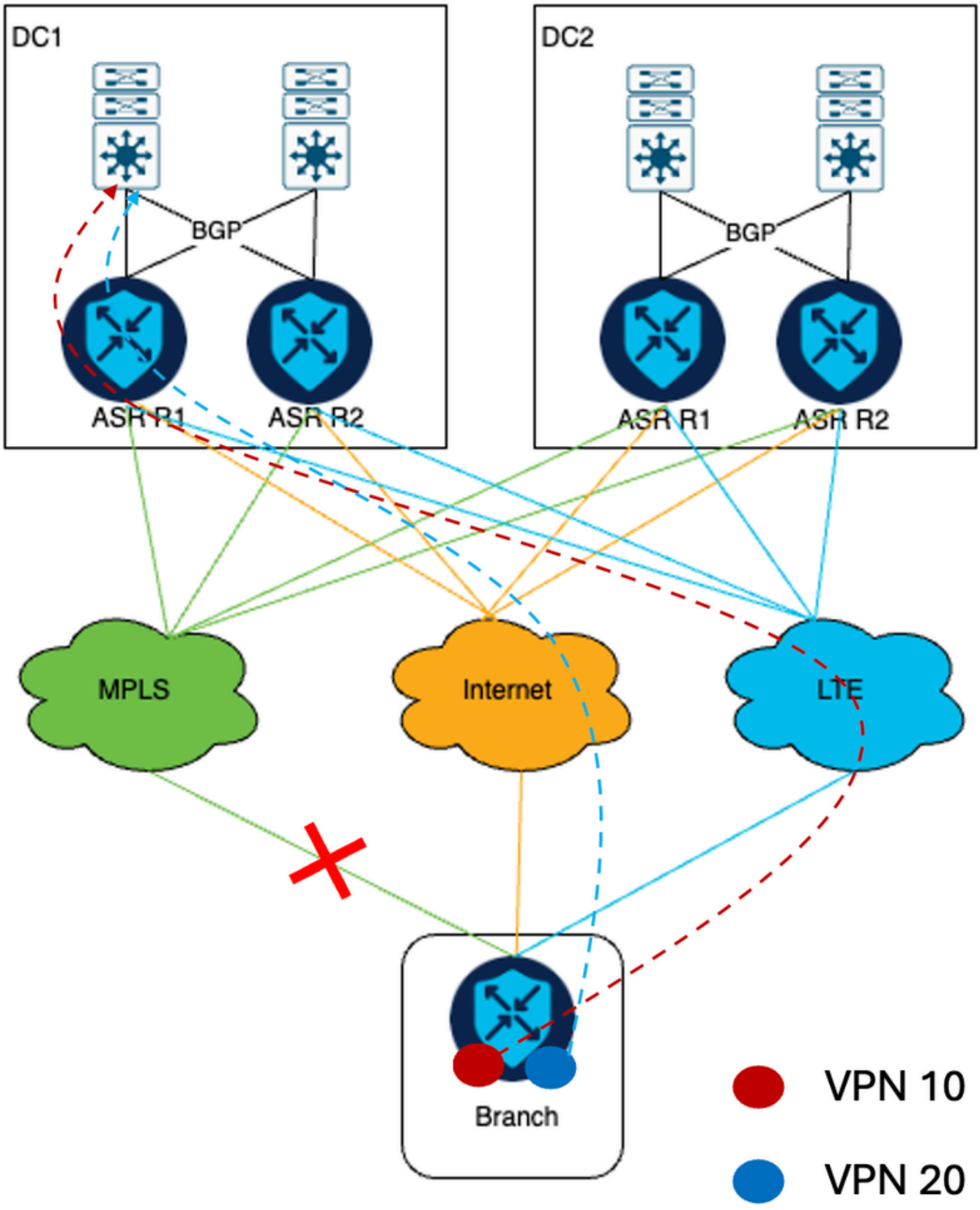
Remarque : la topologie Hub and Spoke est déployée. DC1 et DC2 Edge sont des concentrateurs. Toutes les filiales distantes forment des tunnels IPsec sur trois modes de transport disponibles avec DC Edge.

Diagramme de réseau sortant

Tout le trafic des réseaux VPN 10 et VPN 20 passe par le transport MPLS.



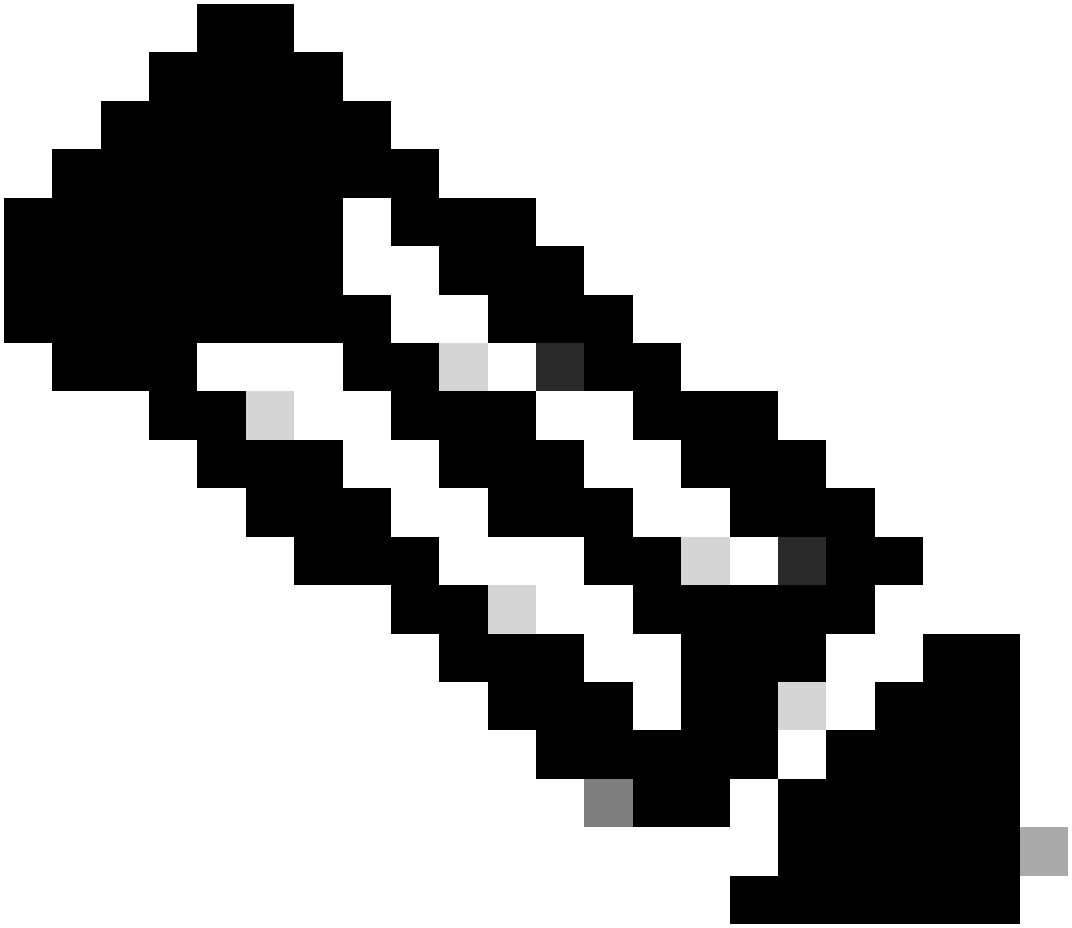
Si la liaison MPLS tombe en panne, le trafic VPN 10 passe au transport LTE et le trafic VPN 20 passe au transport Internet.



Dans ce scénario, le défi technique découle de l'échelle et des exigences spécifiques d'un déploiement réseau de clients. Compte tenu du déploiement de 3 000 routeurs SD-WAN établissant des tunnels IPSec via trois types de transport vers le routeur de data center, le nombre total de tunnels IPSec formés sur les routeurs de tête de réseau primaire ASR1002-HX atteint 9 000. Cependant, l'ASR1002-HX est limité à 8000 tunnels IPSec (source : fiche technique ASR1K).

Solution

Pour résoudre ce problème, le client a décidé d'ajouter un périphérique cEdge ISR4451-X dans chaque DC, en fonction de ses besoins futurs en matière d'évolutivité.



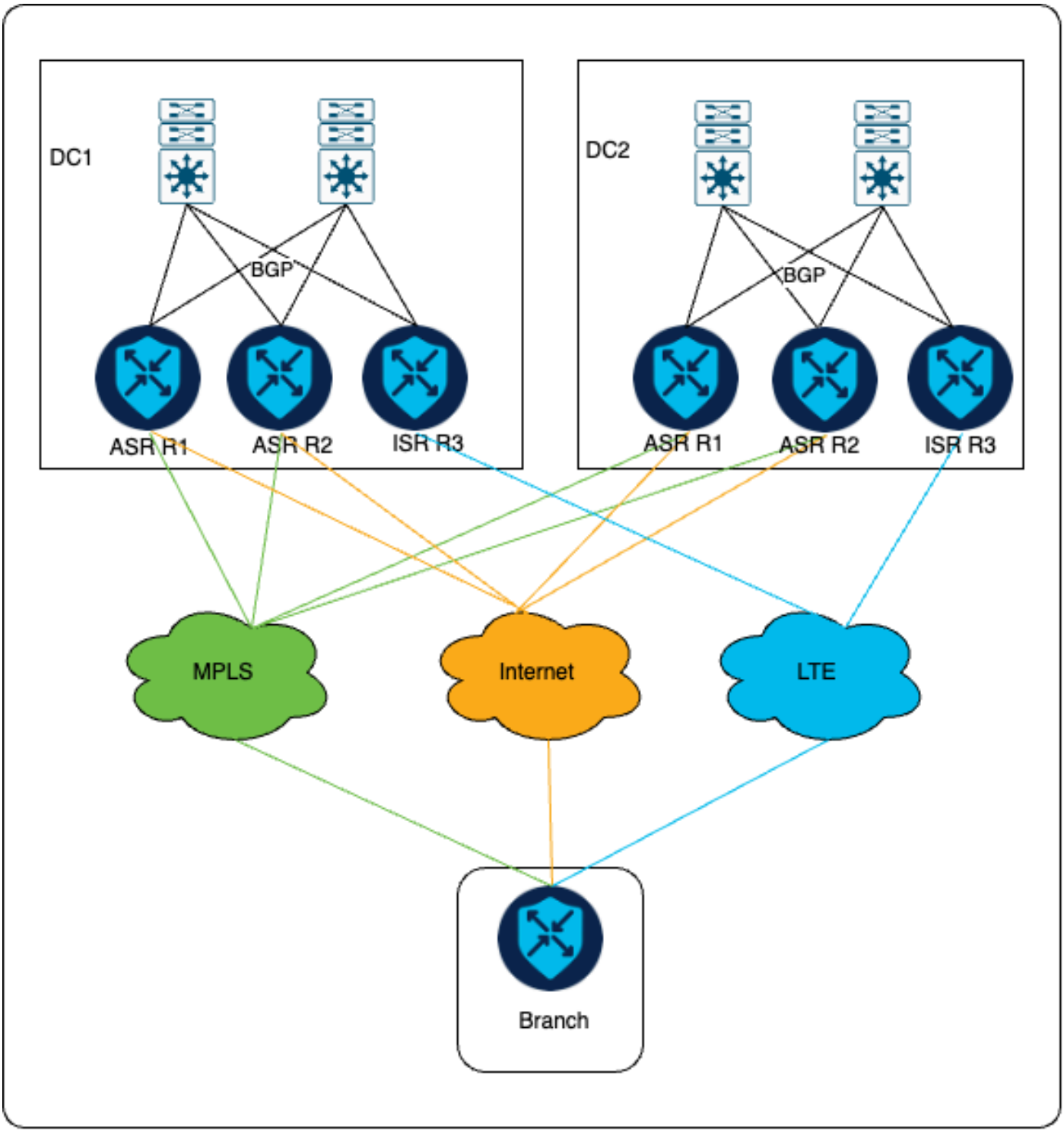
> Remarque : choisissez un modèle de périphérique supplémentaire en fonction des exigences d'évolutivité du client.

Topologie du réseau

Dans le cadre de la solution, les arêtes du routeur de services d'agrégation (ASR) principal continuent de former un tunnel IPSec sur MPLS et le transport Internet, et les arêtes du routeur de services intégrés (ISR) nouvellement installées forment un tunnel IPSec uniquement via le transport LTE.

Comme l'illustre le schéma, les tunnels IPSec sont établis entre la tête de réseau ASR et la

branche via MPLS et Internet, tandis qu'entre le routeur ISR et la branche, les tunnels IPSec sont établis uniquement via LTE.



Le client exige que, dans des circonstances normales, tout le trafic VPN 10 et VPN 20 utilise le transport MPLS pour la communication. Cependant, en cas de défaillance d'une liaison MPLS, le trafic VPN 20 est réacheminé via le transport Internet, tandis que le trafic VPN 10 est réacheminé via le transport LTE, comme avant l'ajout de cEdge supplémentaire.

Configurer

Des politiques centralisées et localisées sont utilisées afin de s'assurer que le trafic est envoyé via

le transport approprié selon la préférence du client. Le trafic provenant de la succursale via la liaison Internet et la liaison LTE est étiqueté. Ces balises sont utilisées pour garantir que les commutateurs LAN de la tête de réseau envoient correctement les messages de réponse pour VPN 10 au routeur ISR et que le trafic VPN 20 est envoyé aux périphériques de tête de réseau ASR.

Configuration de stratégie centralisée

Voici la politique préparée afin de répondre aux exigences du client. Pour le trafic arrivant via la liaison Internet, une balise OMP de 200 est attribuée. D'autre part, le trafic arrivant par la liaison LTE se voit attribuer une balise OMP de 100.

<#root>

Centralized Policy

```
control-policy DataCenter_Outbound_v001
<<omited>>
  sequence 10
   match route
    color-list MPLS
    site-list remote_branches
  vpn-list vpn-10
    prefix-list _AnyIpv4PrefixList
  !
   action accept
    set
     preference 1500
 !
 !
 sequence 20
    match route
      color-list LTE
      site-list remote_branches
      vpn-list vpn-10
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 1000
      omp-tag 100
    !
   !
  !
  sequence 30
    match route
      color-list Internet
      site-list remote_branches
      vpn-list vpn-10
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 500
      omp-tag 200
```

```
     !
    !
  !
  sequence 40
   match route
    color-list MPLS
    site-list remote_branches
    vpn-list vpn-20
    prefix-list _AnyIpv4PrefixList
   !
   action accept
    set
     preference 1500
   !
  sequence 50
    match route
      color-list LTE
      site-list remote_branches
      vpn-list vpn-20
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 500
      omp-tag 100
     !
    !
  !
  sequence 60
    match route
      color-list Internet
      site-list remote_branches
      vpn-list vpn-20
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 1000
      omp-tag 200
    !
   !
  !
<<omited>>
site-list remote_branches
site-id <specifiy site-id range for all remote branch sites>
```

Au niveau du DC, tout en transférant le trafic des routeurs SD-WAN vers les commutateurs principaux, le champ AS-PATH est manipulé lors de l'annonce de la route dans BGP côté LAN. Une carte de route est appliquée dans la configuration BGP au moment de la redistribution des routes OMP dans BGP.

Lorsque la liaison MPLS est opérationnelle, seuls les arêtes principales redistribuent les routes dans BGP car aucun trafic n'est reçu via LTE. Toutefois, en cas de défaillance d’une liaison MPLS :

- Pour le VPN 10, les arêtes ASR redistribuent les routes en ajoutant quatre fois le champ AS-PATH, tandis que l'arête ISR redistribue trois fois le champ AS-PATH. Cette configuration

garantit que le routeur de service intégré (ISR) cEdge est préféré pour l'envoi de réponses.

- De même, pour VPN 20, les périphériques ASR redistribuent les préfixes sans ajouter d'AS-PATH, et le routeur ISR cEdge redistribue les préfixes en ajoutant trois fois le champ AS-PATH. Cela permet de s'assurer que les arêtes ASR sont préférées.

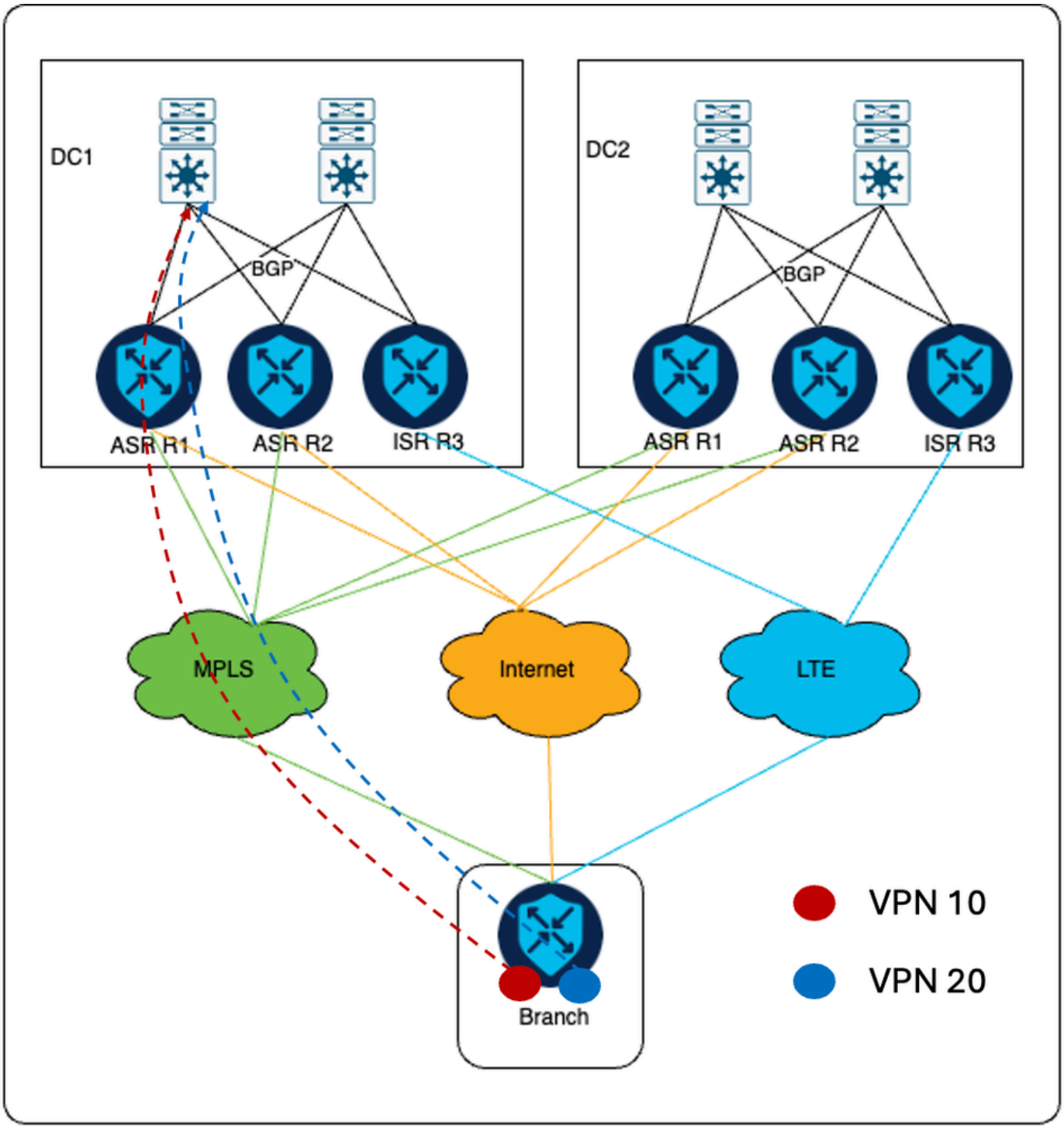
Configuration de stratégie localisée

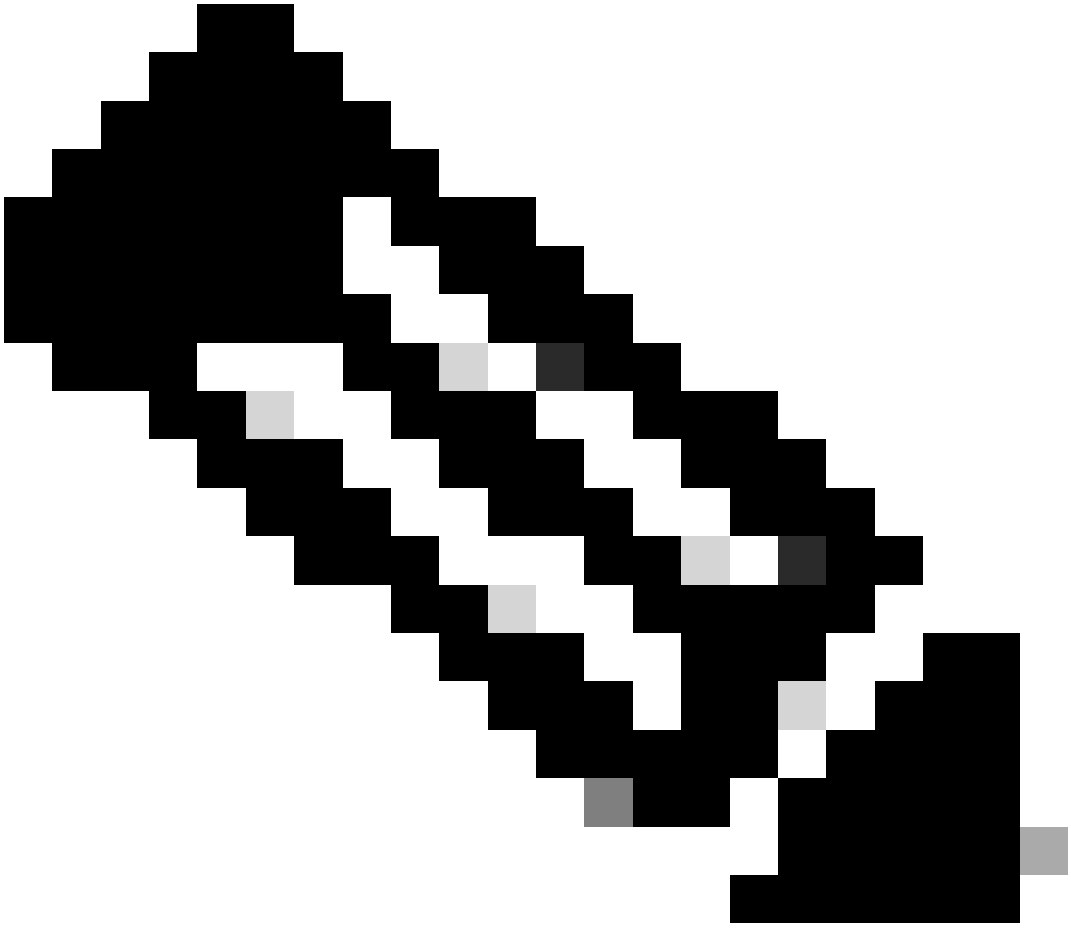
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

route-map DC2_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc2-asnum> <dc2-asnum> <dc2-asnum> <dc2-asnum>
route-map DC2_VPN-10_out_v001 permit 65535

route-map DC1_Backup_All_out_v001 permit 1
match omp-tag 100
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_Backup_All_out_v001 deny 65535

route-map DC2_Backup_All_out_v001 permit 1
match omp-tag 100
set as-prepend <dc2-asnum> <dc2-asnum> <dc2-asnum>
route-map DC2_Backup_All_out_v001 deny 65535
```

Flux de trafic

Scénario normal

Lorsque la liaison MPLS est active, tout le trafic provenant des VPN 10 et VPN 20 traverse le transport MPLS.

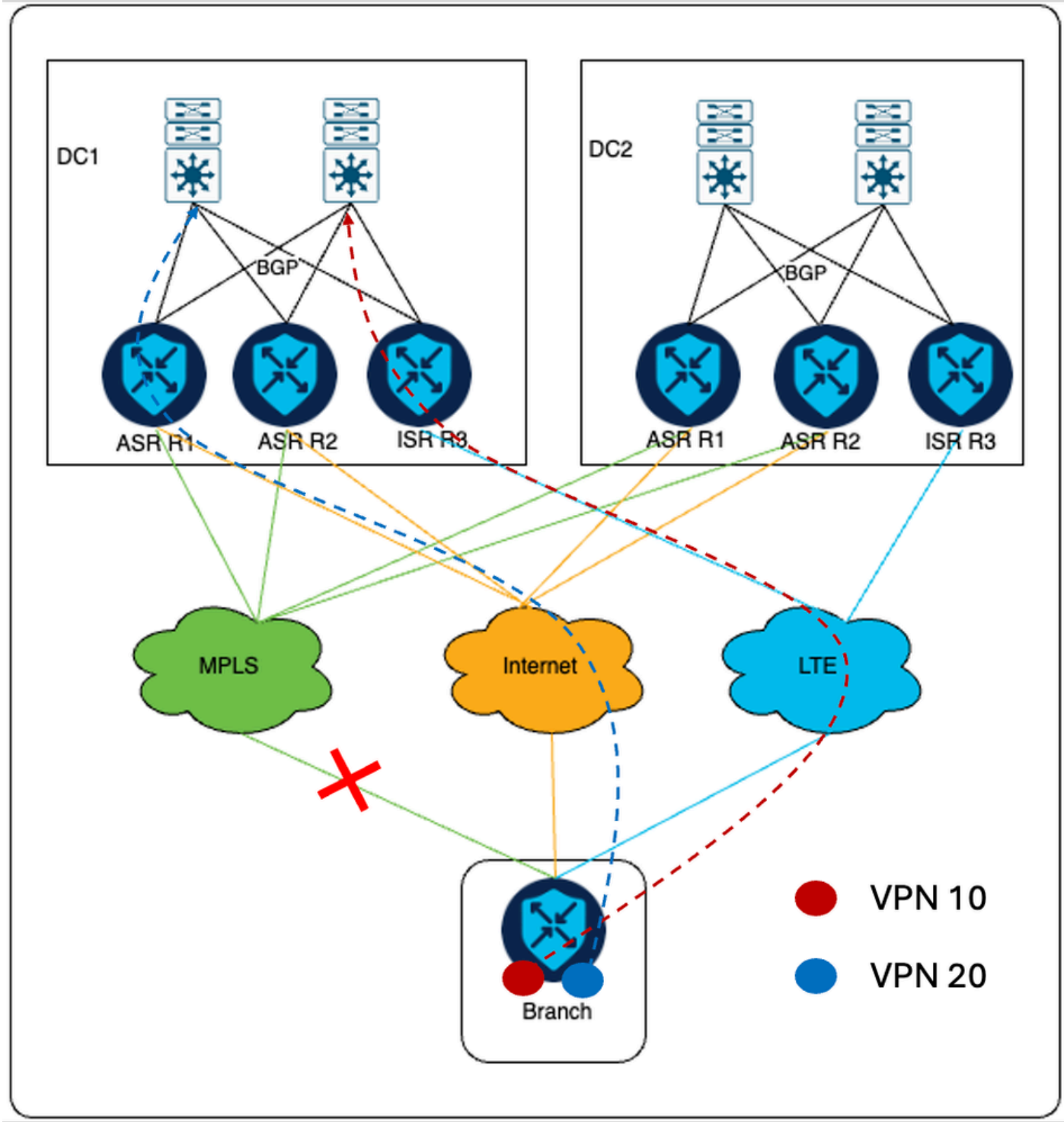

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



Remarque : DC1 est le DC principal.

Scénario de basculement

En cas de défaillance de la liaison MPLS, le trafic VPN 10 transite par le transport LTE vers ISR cEdge. Où le trafic VPN 20 est envoyé via le transport Internet vers le périphérique ASR cEdge.



Pour le trafic de retour des commutateurs principaux, pour le trafic VPN 10, il est envoyé au routeur ISR cEdge car la longueur AS-PATH est plus petite via le routeur ISR que celle du routeur ASR, comme indiqué dans la section relative à la stratégie localisée. De même, le trafic VPN 20 est envoyé vers les périphéries ASR, car AS-PATH est plus petit via ASR par rapport à ISR.

Additional Information

Dans la configuration précédente, tous les arêtes de chaque DC sont connectées aux contrôleurs SD-WAN uniquement via le transport Internet. Ainsi, les routeurs ISR ont un tunnel Internet configuré. L'objectif est de s'assurer que ISR cEdge forme un tunnel IPsec vers les filiales

distantes uniquement via le transport LTE et afin d'atteindre l'objectif donné, la couleur du tunnel sur le transport Internet d'ISR doit être configurée avec une couleur publique qui n'est pas utilisée dans la configuration du client.

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.