

# Adresnummer van tunnelgrens voor dataplane in datacenter

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Netwerkdigram afsluiten](#)

[Oplossing](#)

[Netwerktopologie](#)

[Configureren](#)

[Gecentraliseerde beleidsconfiguratie](#)

[Gelocaliseerde beleidsconfiguratie](#)

[Traffic Flow](#)

[Normaal scenario](#)

[failover-scenario](#)

[Aanvullende informatie](#)

---

## Inleiding

Dit document beschrijft een oplossing voor het aanpakken van schalingproblemen in datacenter SD-WAN randen aangezien deze zich in de buurt van de limieten van hun dataplatform bevinden.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van SD-WAN.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- SD-WAN controller versie 20.6.3.0.54 (ES)
- Cisco IOS® XE (uitgevoerd in controllermodus) 17.06.03a.0.2 (ES)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

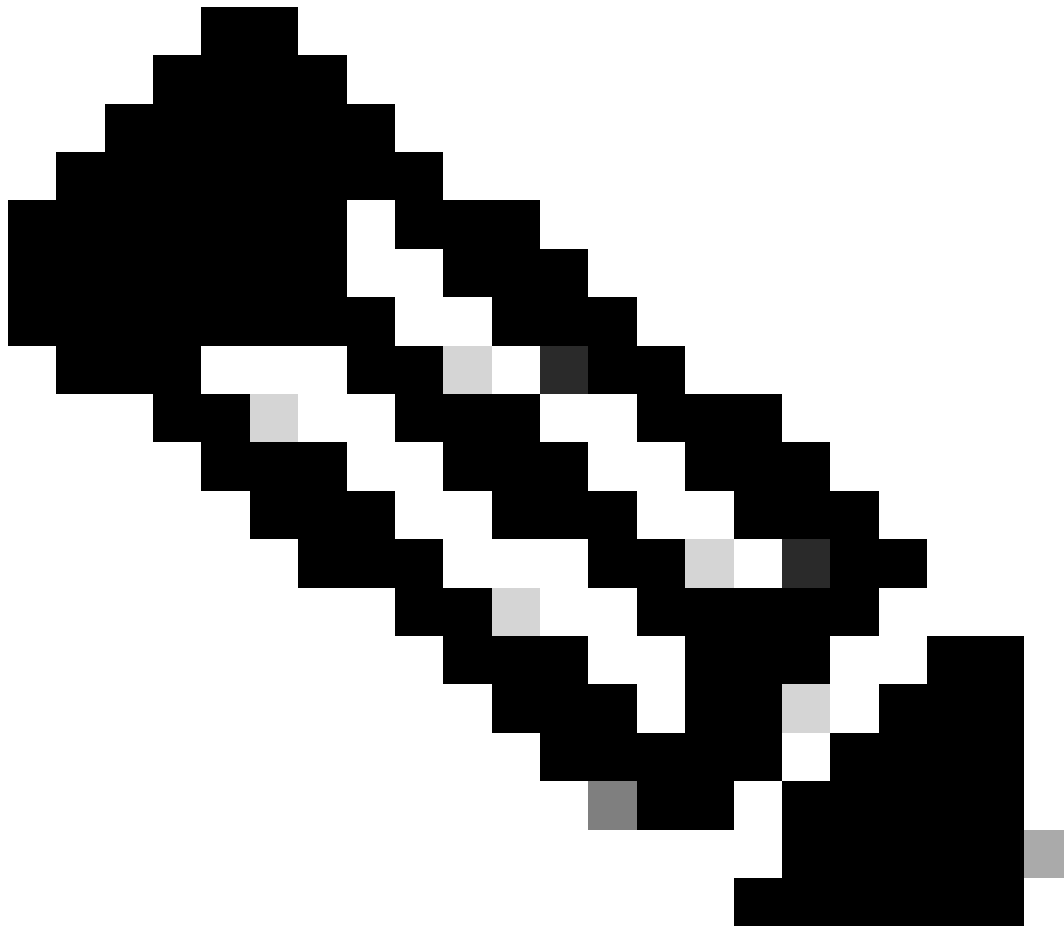
## Achtergrondinformatie

Overzicht van netwerkontwerp:

- VPN: VPN 10, VPN 20
- Transport links: Multiprotocol Label Switching (MPLS), LTE, Internet
- Routergegevens:
  - Primaire router: 2 in elk datacenter
    - Model ASR 1002-HX
    - Cisco IOS XE-softwareversie: 17.06.03a.0.2
  - Secundaire router: 1 in elk Datacenter
    - Model ISR4451-X
    - Cisco IOS XE-softwareversie: 17.06.03a.0.2
- Routing Protocol: BGP (Border Gateway Protocol) wordt gebruikt aan datacenter LAN-zijde

## Probleem

In dit document wordt de casestudy van de klant besproken met de getoonde topologie. De netwerkinfrastructuur van de klant bestaat uit twee datacenters, elk met twee ASR 1002-HX SD-WAN cEdge geïmplementeerd. Deze netwerkarchitectuur heeft als doel ongeveer 3000 opslaglocaties op de SD-WAN overlay te integreren, waarbij de beschikbaarheid van drie verschillende transportverbindingen wordt benut.

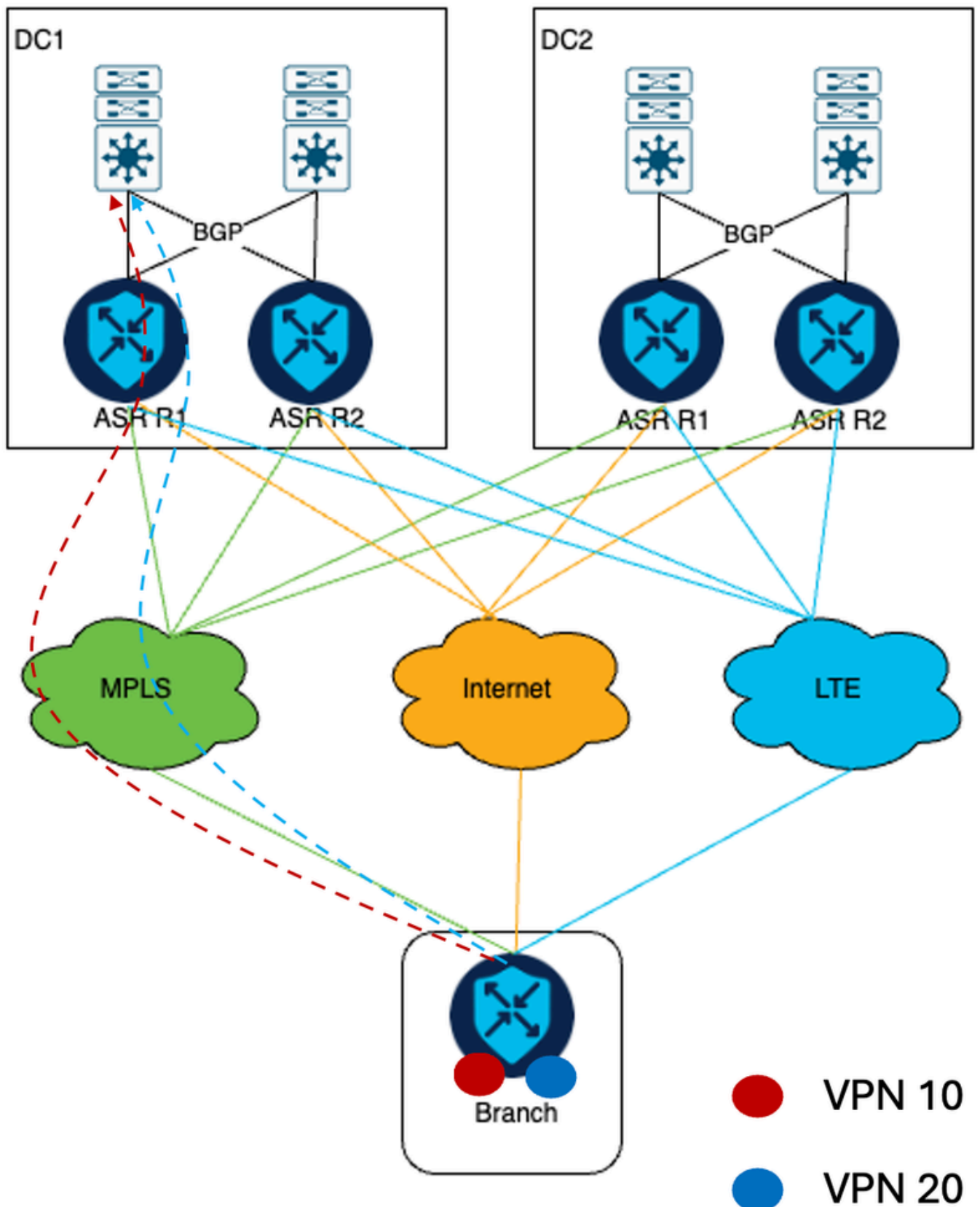


Opmerking: hub and Spoke-topologie wordt geïmplementeerd. DC1 en DC2 randen zijn hubs. Alle verafgelegen vertakkingen vormen IPsec-tunnels via drie beschikbare transportlijnen met DC-randen.

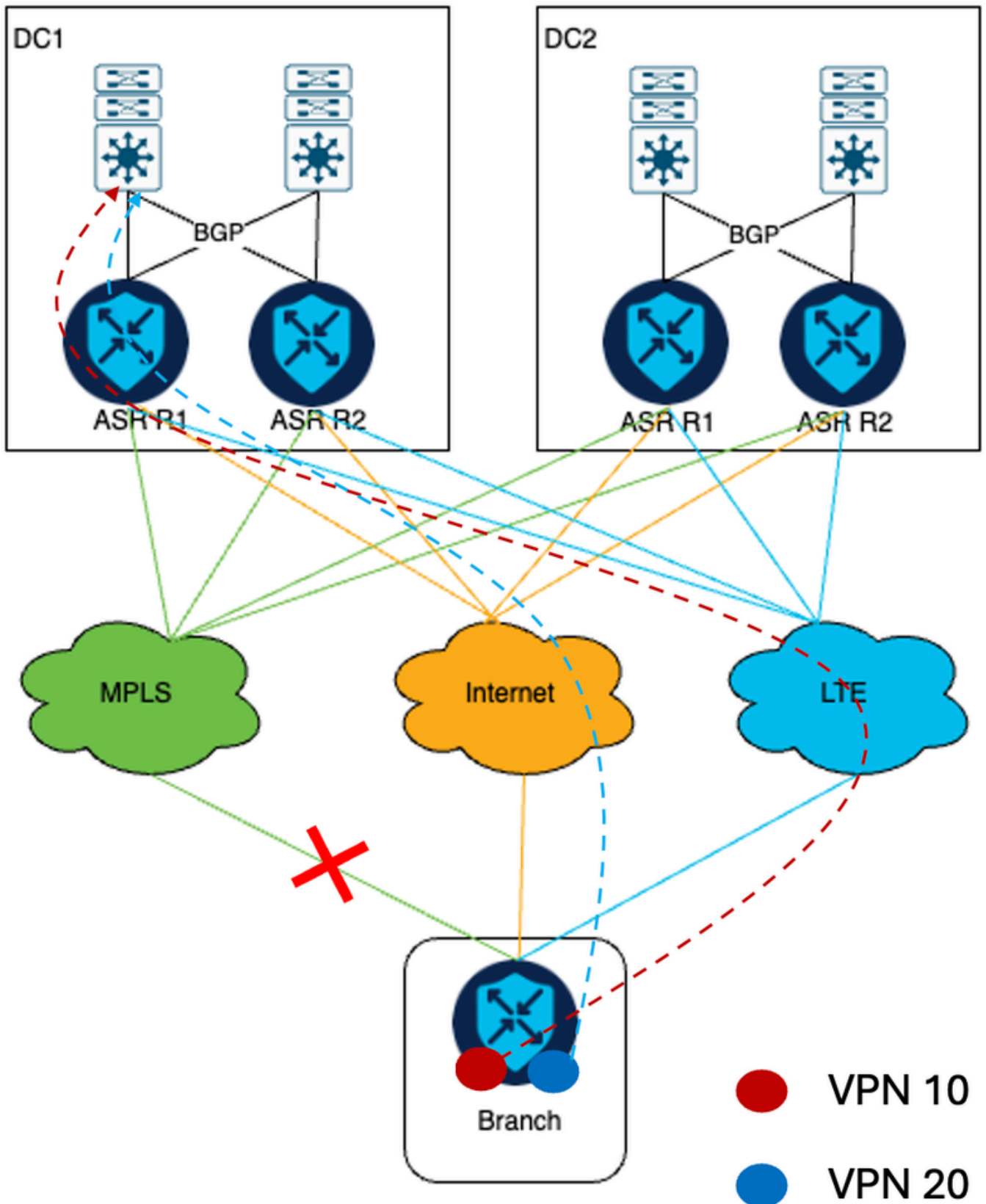
---

## Netwerkdigram afsluiten

Al het verkeer van VPN 10 en VPN 20 verloopt via MPLS-transport.



Als de MPLS-link naar beneden gaat, verschuift VPN 10 verkeer naar LTE-transport en VPN 20 verkeersverschuivingen naar internettransport.

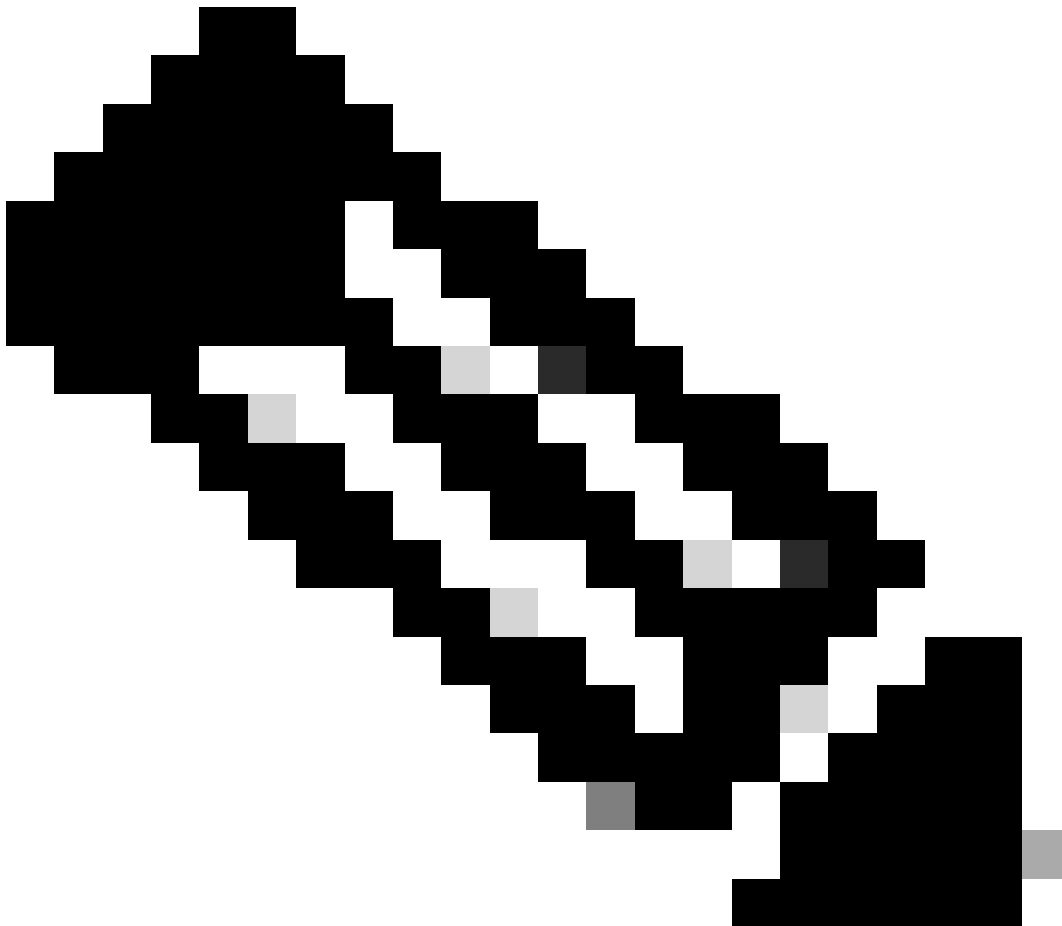


De technische uitdaging in dit scenario vloeit voort uit de schaal en de specifieke vereisten van een netwerkplaatsing van klanten. Gezien de plaatsing van 3000 SD-WAN routers die IPSec-tunnels via drie soorten transport naar de datacenterrouter opzetten, bedraagt het totale aantal IPSec-tunnels dat op ASR1002-HX primaire head-end routers wordt gevormd 9000. De ASR1002-HX is echter beperkt tot 8000 IPSec-tunnels (bron: [ASR1K Datasheet](#)).

# Oplossing

Om dit op te lossen heeft de klant besloten om in elke DC een ISR4451-X cEdge-apparaat toe te voegen volgens de toekomstige schaalbaarheidsvereiste van de klant.

---



Opmerking: kies een extra apparaatmodel op basis van de schaalbaarheidsvereiste van de klant.

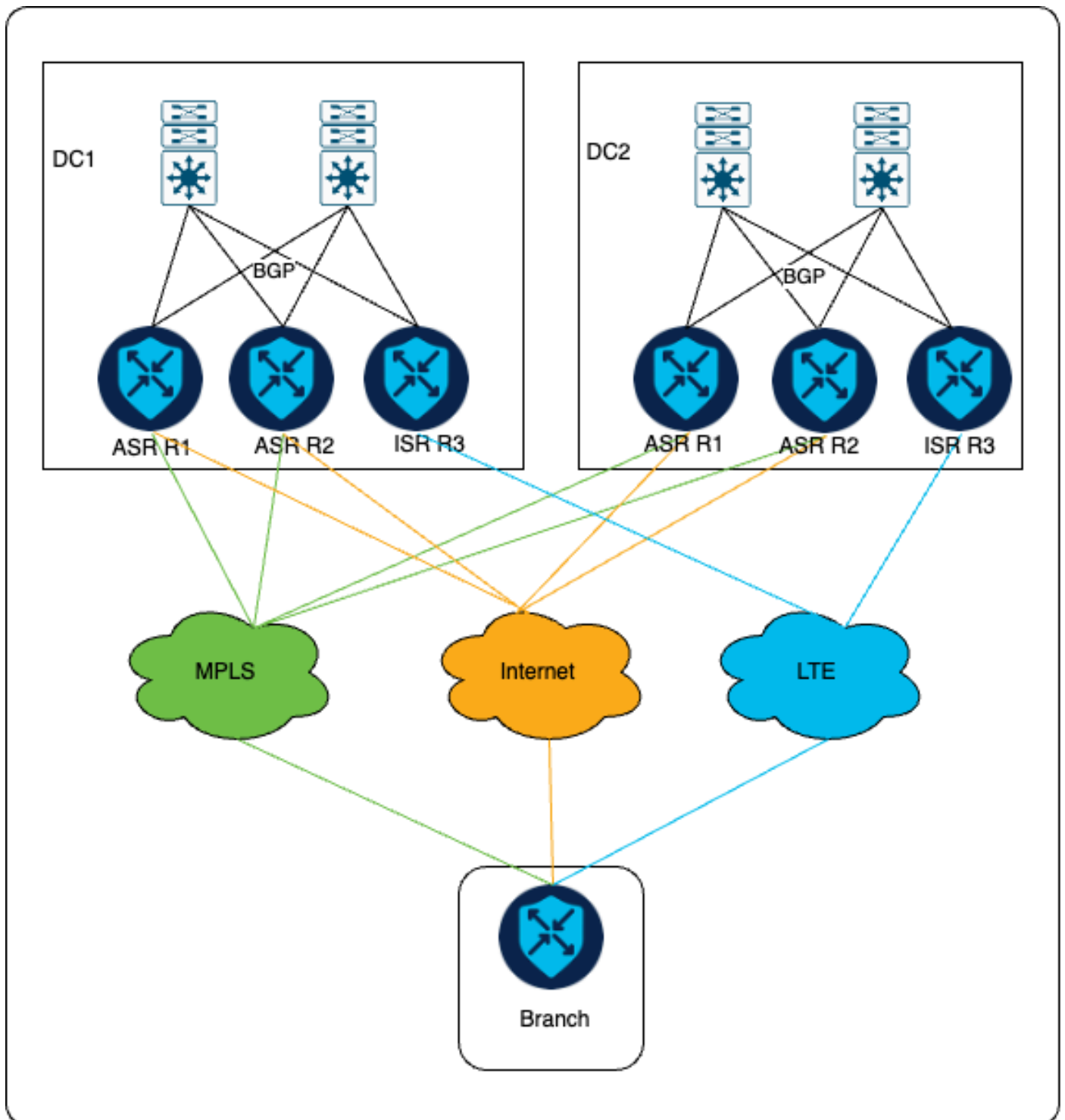
---

## Netwerktopologie

Als deel van de oplossing, blijven de primaire Randen van de Aggregation Services Router (ASR) een tunnel IPsec over MPLS en Internet vervoer vormen, en de onlangs geïnstalleerde Randen van de Geïntegreerde Dienst (ISR) vormen een tunnel IPsec slechts via LTE vervoer.

Zoals afgebeeld in het diagram, worden IPsec-tunnels ingesteld tussen de ASR-head-end en de aftakking via zowel MPLS als het internet, terwijl tussen de ISR en de aftakking IPsec-tunnels

uitsluitend via LTE worden opgezet.



Het klantenvereiste is dat, onder normale omstandigheden, al VPN 10 en VPN 20 verkeer MPLS vervoer voor mededeling gebruiken. In het geval van een MPLS-koppelingsfout wordt VPN 20-verkeer echter omgeleid via internettransport, terwijl VPN 10-verkeer omgeleid wordt via LTE-transport, zoals vóór het toevoegen van extra cEdge.

## Configureren

Gecentraliseerd en lokaal beleid wordt gebruikt om ervoor te zorgen dat verkeer wordt verzonden via het juiste transport per de voorkeur van de klant. Verkeer dat binnenkomt vanaf de locatie via

de internetlink en LTE link is gelabeld. Deze tags worden gebruikt om ervoor te zorgen dat LAN-switches op de head-end antwoordberichten voor VPN 10 correct naar de ISR-router sturen en dat VPN 20-verkeer naar ASR-head-end apparaten wordt verzonden.

## Gecentraliseerde beleidsconfiguratie

Hier is het beleid voorbereid om te voldoen aan de eisen van de klant. Voor verkeer dat via de internetlink aankomt, wordt een OMP-tag van 200 toegewezen. Aan de andere kant wordt verkeer dat aankomt via de LTE-link toegewezen aan een OMP-tag van 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 <specify site-id range for all remote branch sites>

```

Bij DC wordt het AS-PATH veld tijdens het doorsturen van verkeer van SD-WAN routers naar core switches gemanipuleerd bij het adverteren van de route naar BGP aan de LAN kant. Op het moment van herverdeling van OMP-routes in BGP wordt een routekaart toegepast in de BGP-configuratie.

Wanneer de MPLS-link operationeel is, herverdelen alleen de primaire randen routes in BGP, aangezien er geen verkeer via LTE wordt ontvangen. In het geval van een MPLS-koppelingfout:

- Voor VPN 10 herverdelen de ASR-randen routes door het veld AS-PATH vier keer toe te voegen, terwijl de ISR cEdge opnieuw wordt gedistribueerd door het veld AS-PATH drie keer toe te voegen. Deze configuratie zorgt ervoor dat de ISR cEdge de voorkeur verdient voor het verzenden van antwoorden.

- Op dezelfde manier herverdelen de ASR-randen voor VPN 20 prefixes zonder een AS-PATH toe te voegen, en herverdelen de ISR cEdge prefixes door het AS-PATH-veld drie keer toe te voegen. Dit waarborgt dat de ASR-randen de voorkeur krijgen.

## Gelocaliseerde beleidsconfiguratie

```
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
```

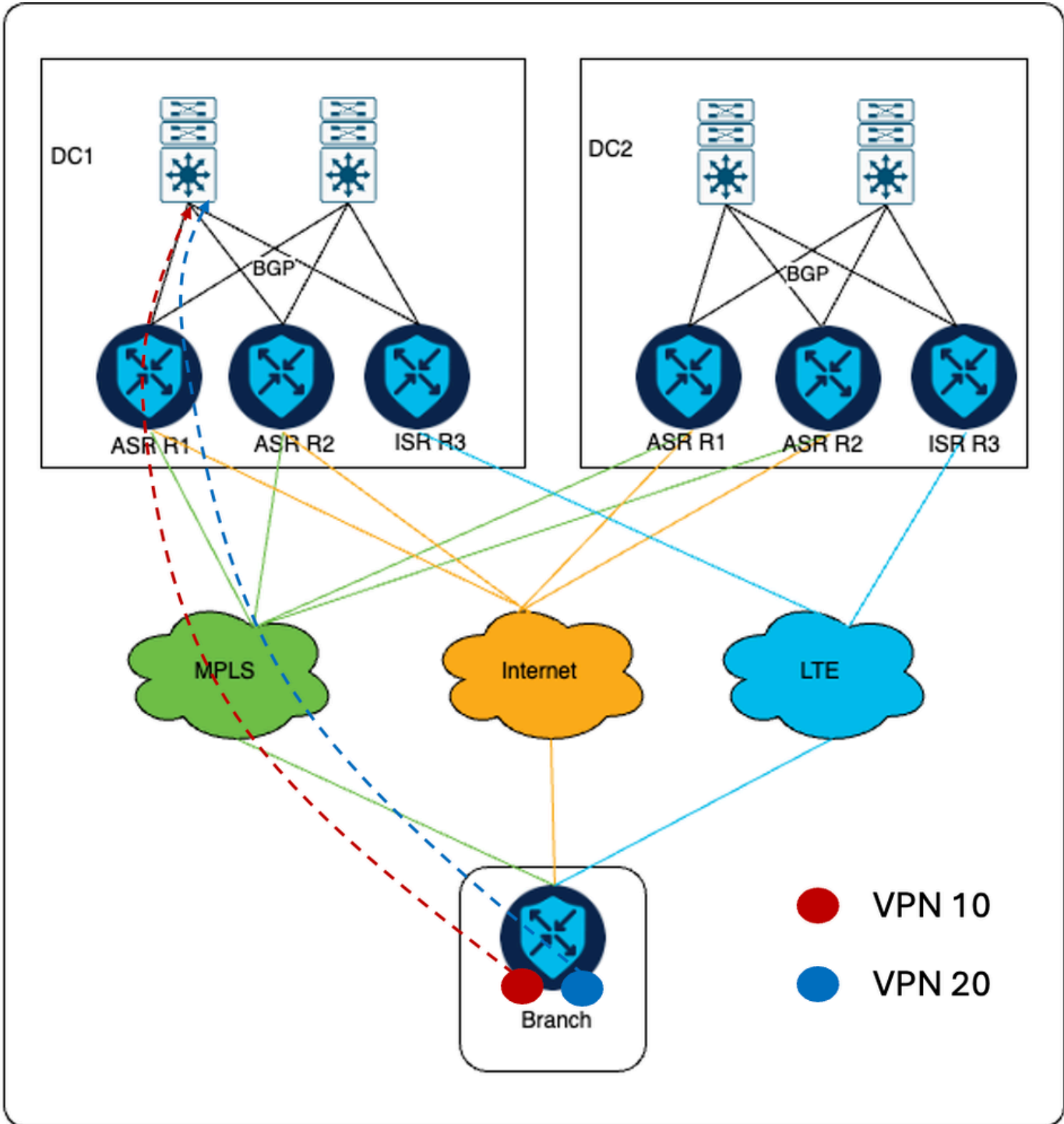
```
route-map DC1_Backup_All_out_v001 permit 1
match omp-tag 100
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_Backup_All_out_v001 deny 65535
```

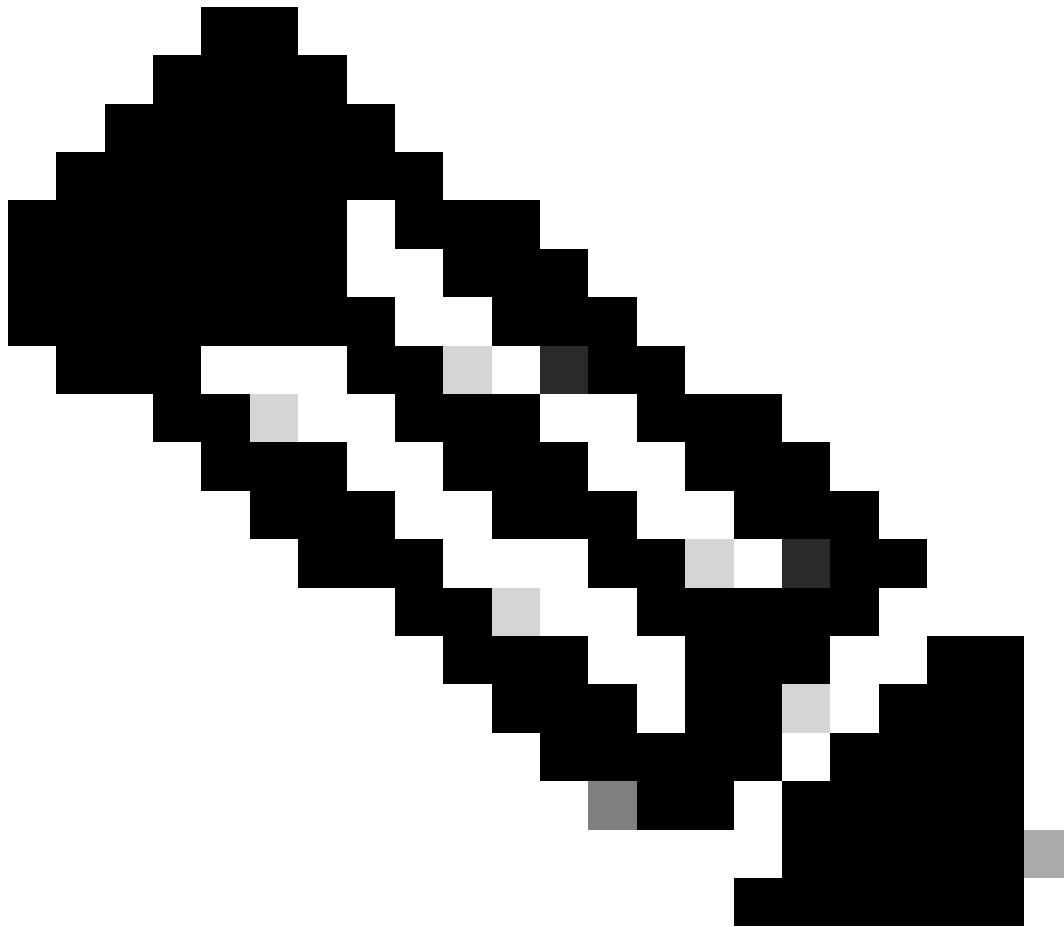
```
route-map DC2_Backup_All_out_v001 permit 1
match omp-tag 100
set as-prepend <dc2-asnum> <dc2-asnum> <dc2-asnum>
route-map DC2_Backup_All_out_v001 deny 65535
```

## Traffic Flow

### Normaal scenario

Wanneer de MPLS-link is geopend, wordt al het verkeer van VPN 10 en VPN 20 door het MPLS-transport geleid.



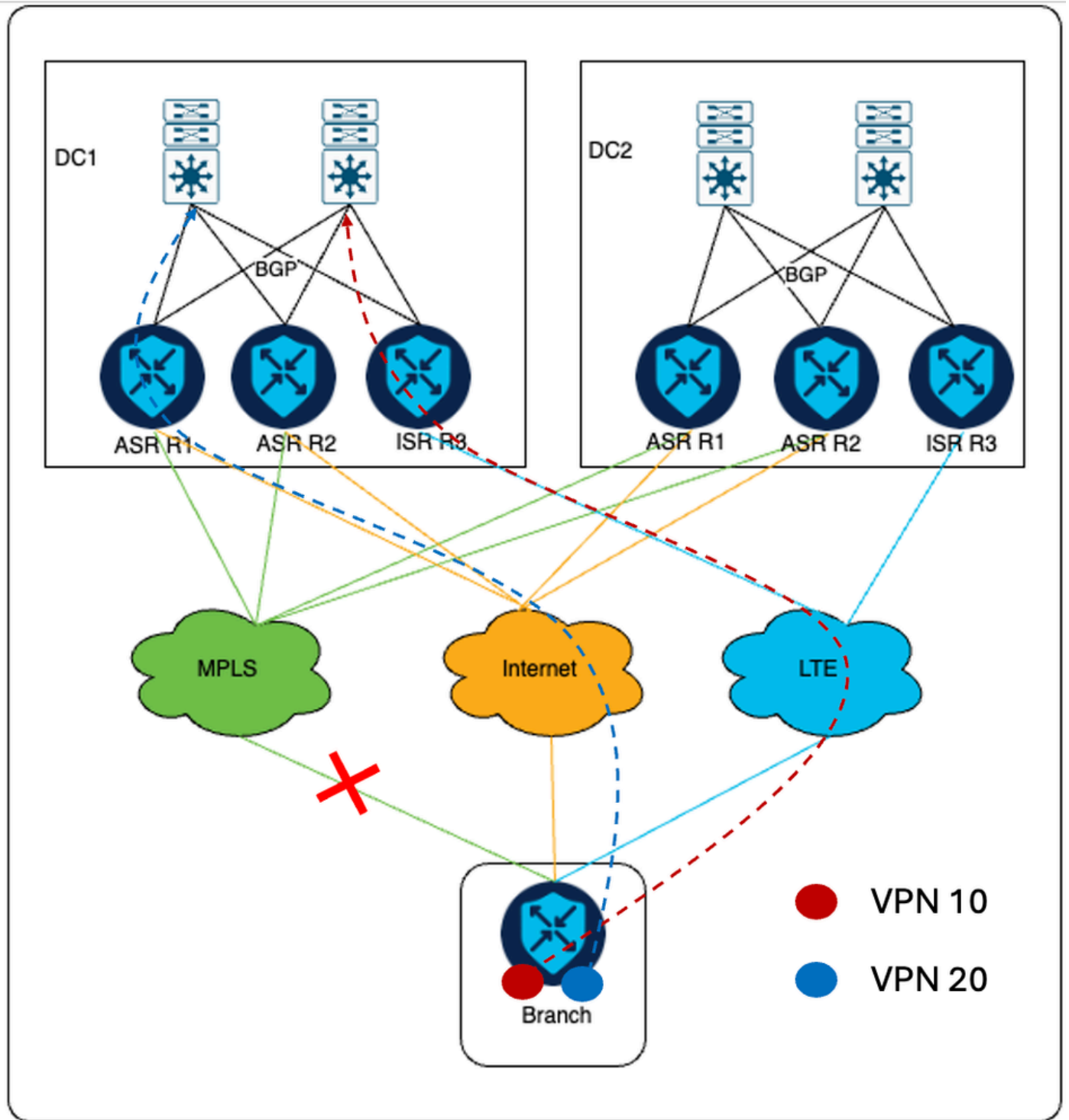


Opmerking: DC1 is de primaire DC.

---

#### failover-scenario

In het geval van een MPLS-koppelingfout leiden VPN 10-verkeersovergangen via LTE-transport naar ISR cEdge. Waar als VPN 20 verkeer via internettransport naar ASR cEdge-apparaat wordt verzonden.



Voor retourverkeer van core switches wordt voor VPN 10 verkeer naar de ISR cEdge verzonden omdat de AS-PATH-lengte kleiner is via ISR dan in ASR zoals gespecificeerd in de paragraaf over gelocaliseerd beleid. Op dezelfde manier wordt VPN 20 verkeer naar ASR-randen verzonden omdat AS-PATH via ASR kleiner is dan ISR.

## Aanvullende informatie

In de eerdere installatie zijn alle randen van elke DC alleen via internettransport verbonden met SD-WAN controllers. Aldus hebben de routers ISR de tunnel van Internet gevormd. Er moet voor worden gezorgd dat ISR cEdge alleen via LTE-transport een IPsec-tunnel naar verafgelegen

filialen vormt en om aan de gestelde eis te voldoen, moet de tunnelkleur op het internettransport van ISR worden geconfigureerd met een openbare kleur die niet in gebruik is bij de instelling van de klant.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.