Número de dirección del límite de túnel del plano de datos en el Data Center

Contenido

Introducción

Este documento describe una solución para abordar los problemas de escalado en las aristas SD-WAN del Data Center a medida que se acercan a sus límites de túnel del plano de datos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos de SD-WAN.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador SD-WAN versión 20.6.3.0.54 (ES)
- Cisco IOS® XE (ejecución en modo de controlador) 17.06.03a.0.2 (ES)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

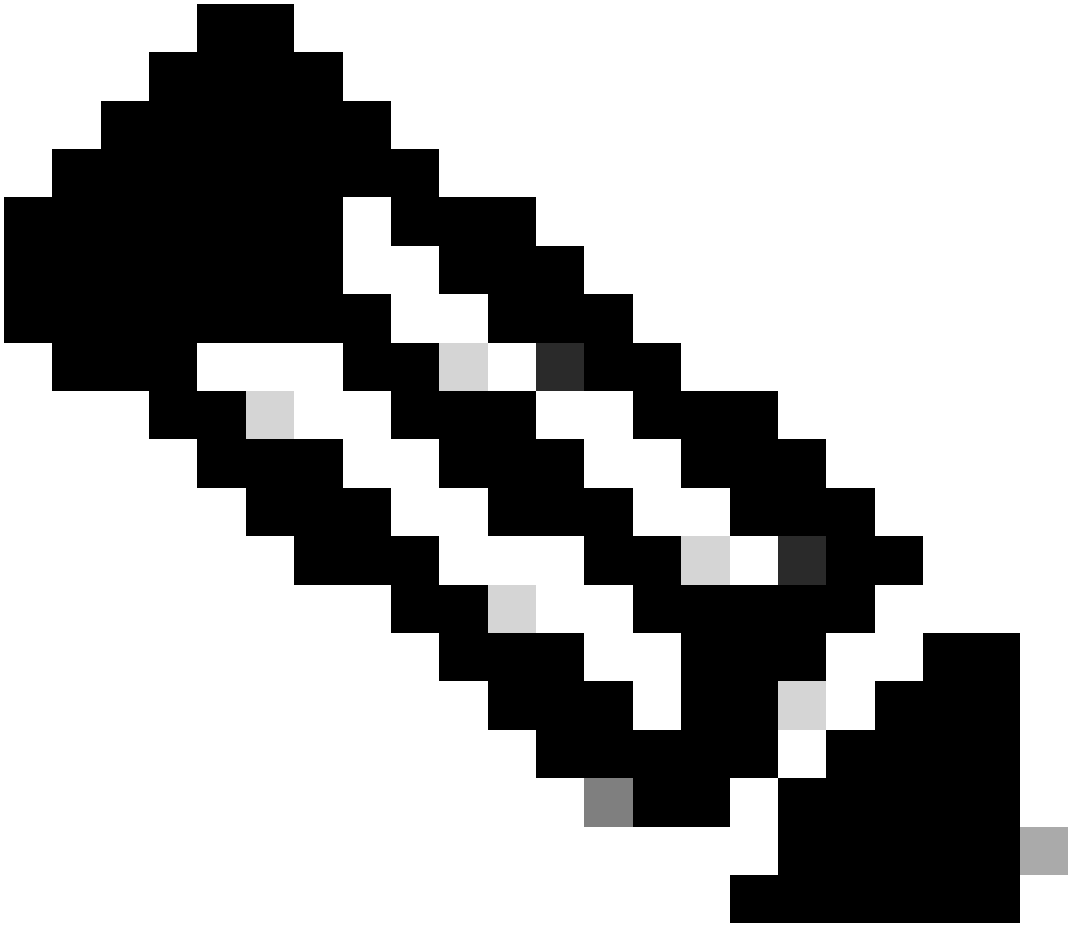
Antecedentes

Descripción general del diseño de red:

- VPN: VPN 10, VPN 20
- Enlaces de transporte: Multiprotocol Label Switching (MPLS), LTE, Internet
- Detalles del router:
    - Router principal: 2 en cada Data Center
      - Modelo: ASR1002-HX
      - Versión del software Cisco IOS XE: 17.06.03a.0.2
    - Router secundario: 1 en cada Data Center
      - Modelo: ISR4451-X
      - Versión del software Cisco IOS XE: 17.06.03a.0.22
- Protocolo de routing: el protocolo de gateway fronterizo (BGP) se utiliza en el lado de la LAN del Data Center

Problema

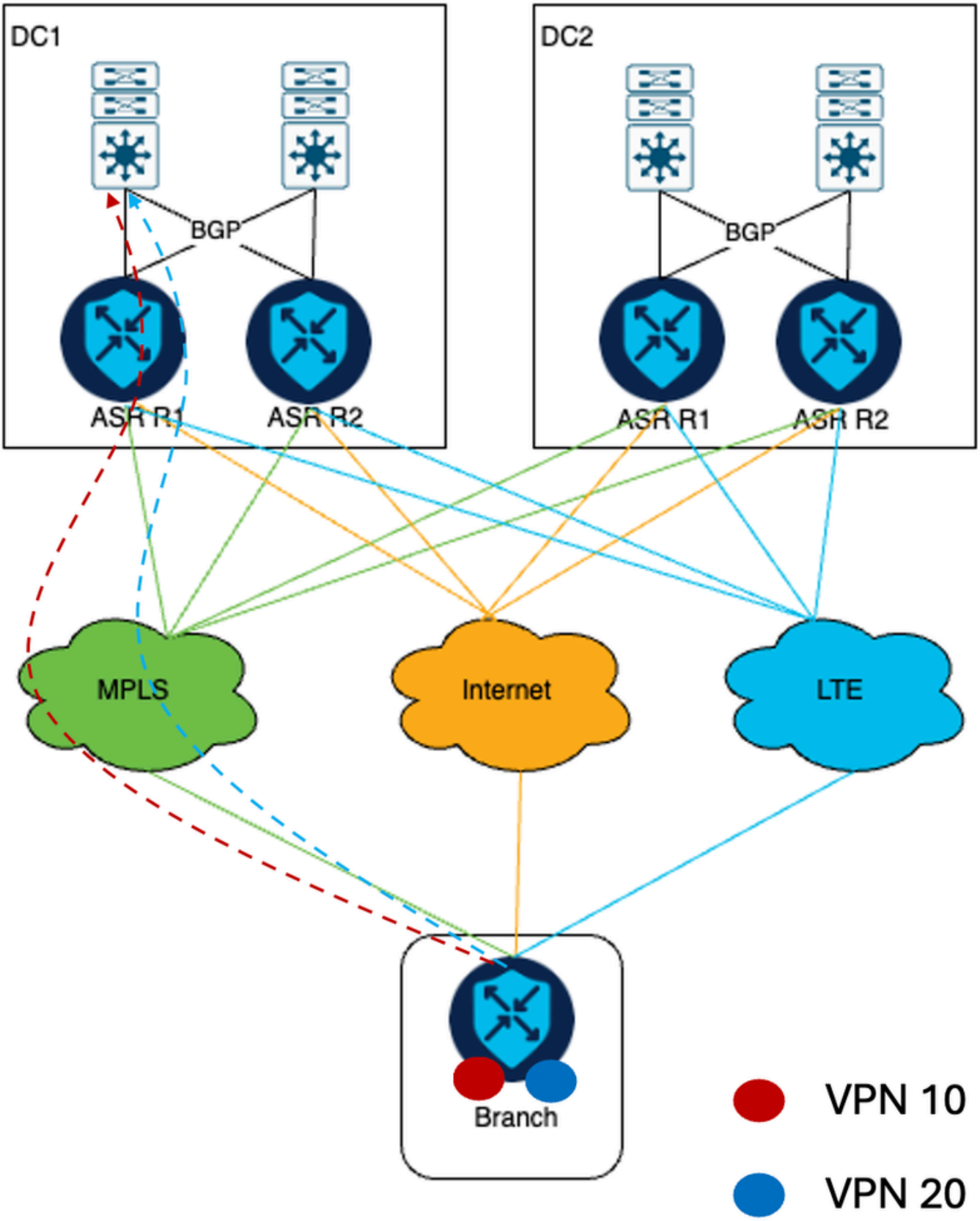
En este documento se describe el caso práctico de un cliente en el que, una vez mostrada la topología, la infraestructura de red del cliente consta de dos Data Centers, cada uno con dos ASR1002-HX SD-WAN cEdge implementados. Esta arquitectura de red pretende incorporar aproximadamente 3000 ubicaciones de tienda en la superposición de SD-WAN, aprovechando la disponibilidad de tres enlaces de transporte distintos.



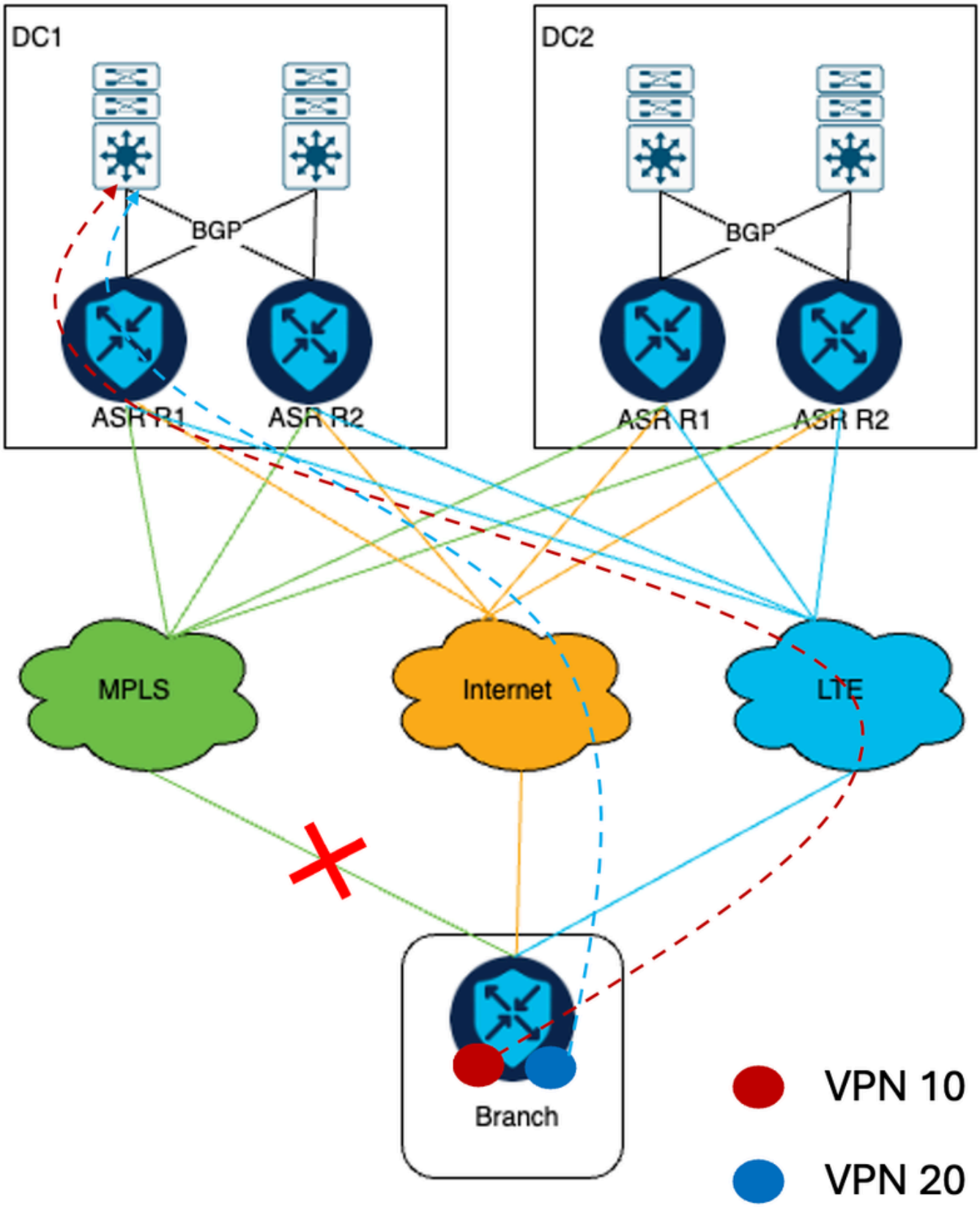
Nota: se ha implementado la topología de hub y radio. Los bordes DC1 y DC2 son hubs. Todas las sucursales remotas forman túneles IPsec a través de tres transportes disponibles con DC Edges.

Saliendo del diagrama de red

Todo el tráfico de VPN 10 y VPN 20 pasa a través del transporte MPLS.



Si el enlace MPLS deja de funcionar, el tráfico VPN 10 se traslada al transporte LTE y el tráfico VPN 20 se traslada al transporte de Internet.

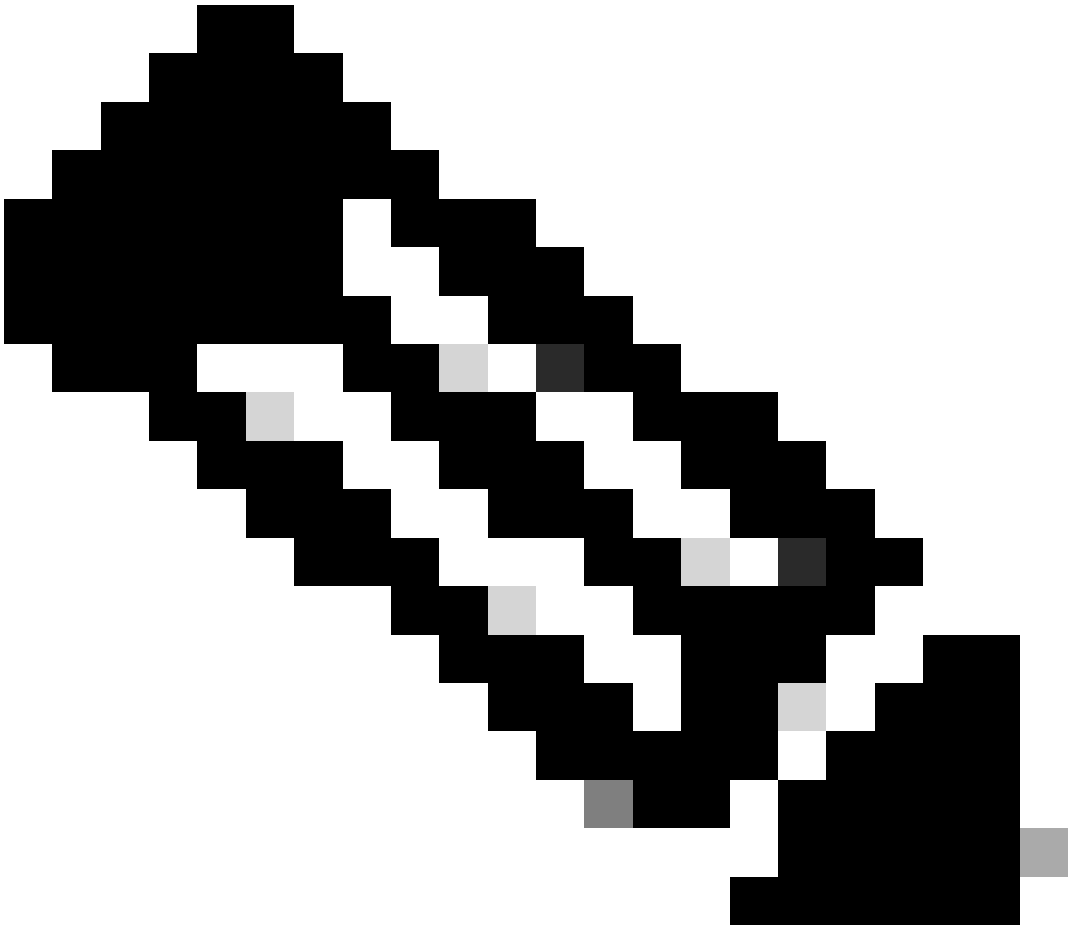


El desafío técnico en esta situación surge de la escala y los requisitos específicos de una implementación de red de clientes. Teniendo en cuenta la implementación de 3000 routers SD-WAN que establecen túneles IPSec a través de tres tipos de transporte al router del Data Center, el recuento total de túneles IPSec formados en routers de cabecera principales ASR1002-HX alcanza los 9000. Sin embargo, ASR1002-HX está limitado a 8000 túneles IPSec (fuente: ASR1K

Datasheet).

Solución

Para solucionar este problema, el cliente decidió añadir un dispositivo cEdge ISR4451-X en cada DC según los requisitos de escalabilidad futuros del cliente.



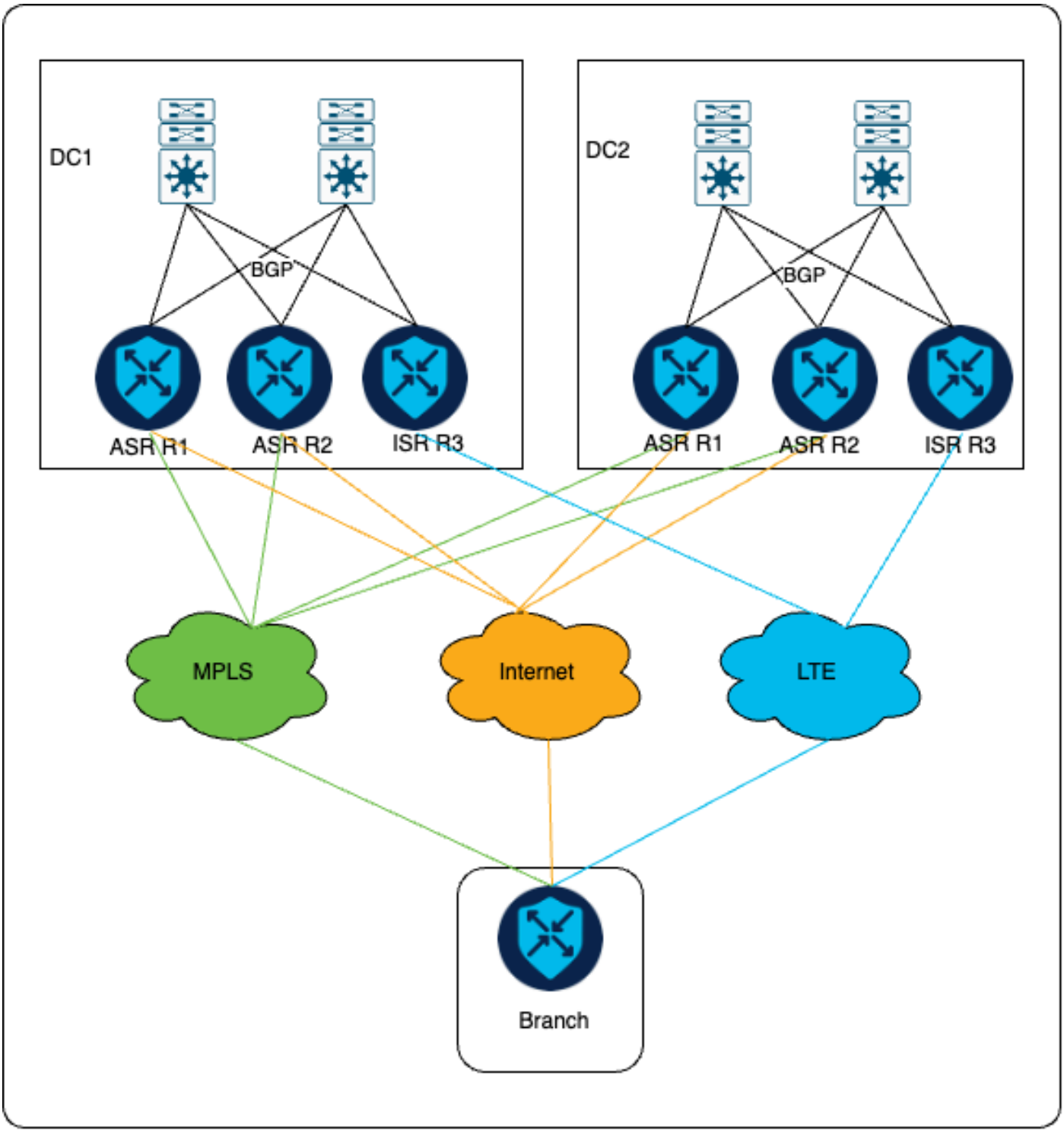
> Nota: Decida un modelo de dispositivo adicional en función de los requisitos de escalabilidad del cliente.

Topología de red

Como parte de la solución, los extremos del router de servicios de agregación (ASR) principal siguen formando un túnel IPSec sobre MPLS y transporte de Internet, y los extremos del router de servicios integrados (ISR) recién instalado forman un túnel IPsec solo a través del transporte LTE.

Como se muestra en el diagrama, los túneles IPSec se establecen entre la cabecera ASR y la

sucursal a través de MPLS e Internet, mientras que entre ISR y la sucursal, los túneles IPSec se establecen únicamente a través de LTE.



El requisito del cliente es que, en circunstancias normales, todo el tráfico VPN 10 y VPN 20 utilice transporte MPLS para la comunicación. Sin embargo, en caso de que se produzca un fallo en el enlace MPLS, el tráfico VPN 20 se vuelve a enrutar a través del transporte de Internet, mientras que el tráfico VPN 10 se redirige a través del transporte LTE, comportamiento similar al anterior a la adición de cEdge adicional.

Configurar

Se utilizan políticas centralizadas y localizadas para garantizar que el tráfico se envía a través del transporte correcto según las preferencias del cliente. El tráfico que llega desde la sucursal a través del link de Internet y el link LTE está etiquetado. Estas etiquetas se utilizan para garantizar que los switches LAN del terminal principal envíen correctamente mensajes de respuesta para VPN 10 al router ISR y que el tráfico VPN 20 se envíe a los dispositivos de terminal ASR.

Configuración de políticas centralizadas

Esta es la política preparada para cumplir los requisitos del cliente. Para el tráfico que llega a través del enlace de Internet, se asigna una etiqueta OMP de 200. Por otro lado, al tráfico que llega a través del link LTE se le asigna una etiqueta 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>
```

En DC, mientras se reenvía el tráfico de los routers SD-WAN a los switches de núcleo, el campo AS-PATH se manipula cuando se anuncia la ruta en BGP en el lado LAN. Se aplica un route map en la configuración BGP en el momento de la redistribución de las rutas OMP en BGP.

Cuando el link MPLS está operativo, solamente los bordes primarios redistribuyen las rutas en BGP ya que no se recibe tráfico a través de LTE. Sin embargo, en caso de que se produzca un fallo en un enlace MPLS:

- Para VPN 10, ASR Edges redistribuye las rutas anexando el campo AS-PATH cuatro veces, mientras que ISR cEdge lo redistribuye anexando el campo AS-PATH tres veces. Esta configuración garantiza que ISR cEdge es el preferido para enviar respuestas.

- De manera similar, para VPN 20, ASR Edges redistribuye los prefijos sin anexar ningún AS-PATH, e ISR cEdge redistribuye los prefijos anexando el campo AS-PATH tres veces. Esto garantiza que se prefieran las aristas ASR.

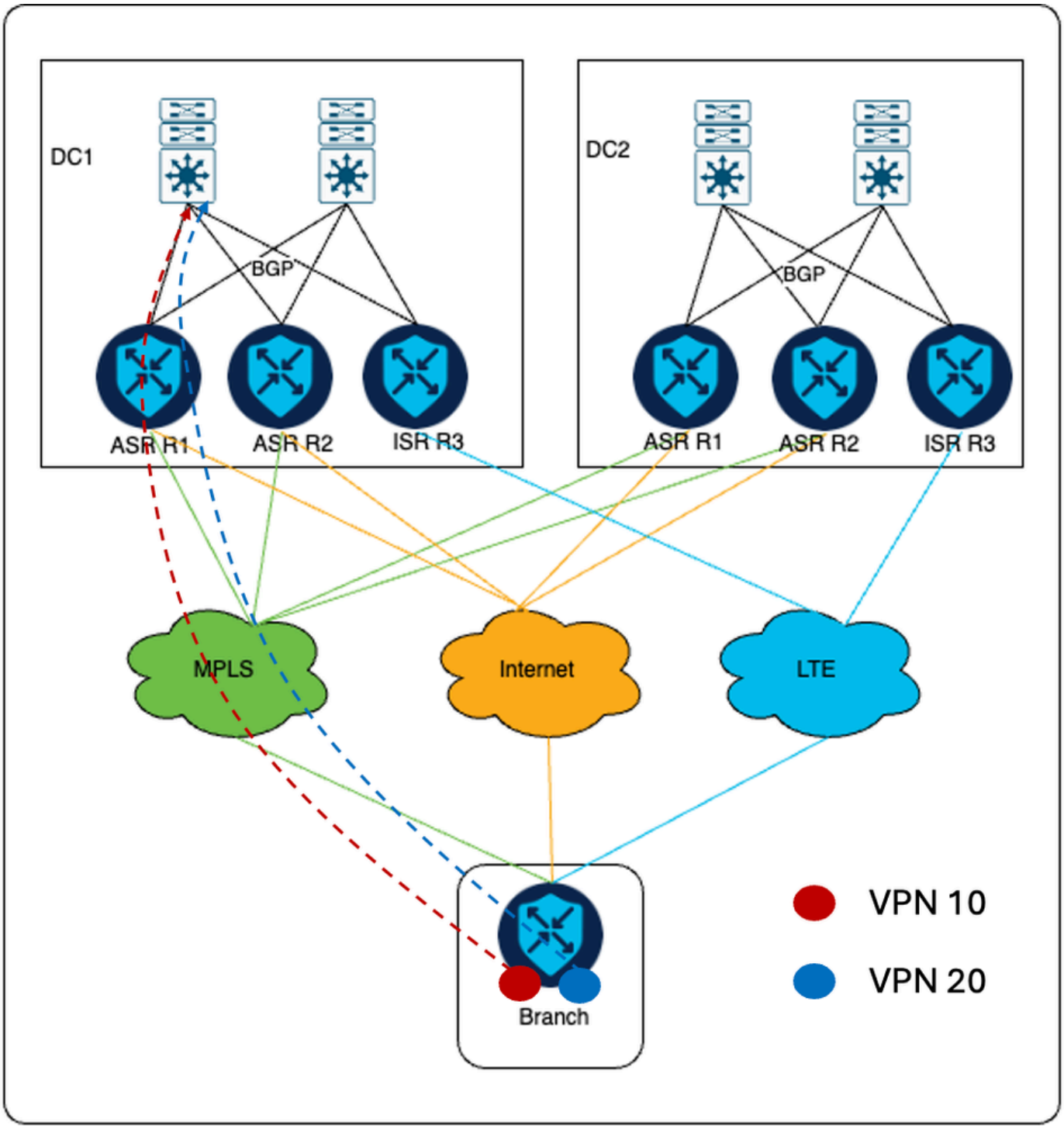
Configuración de política localizada

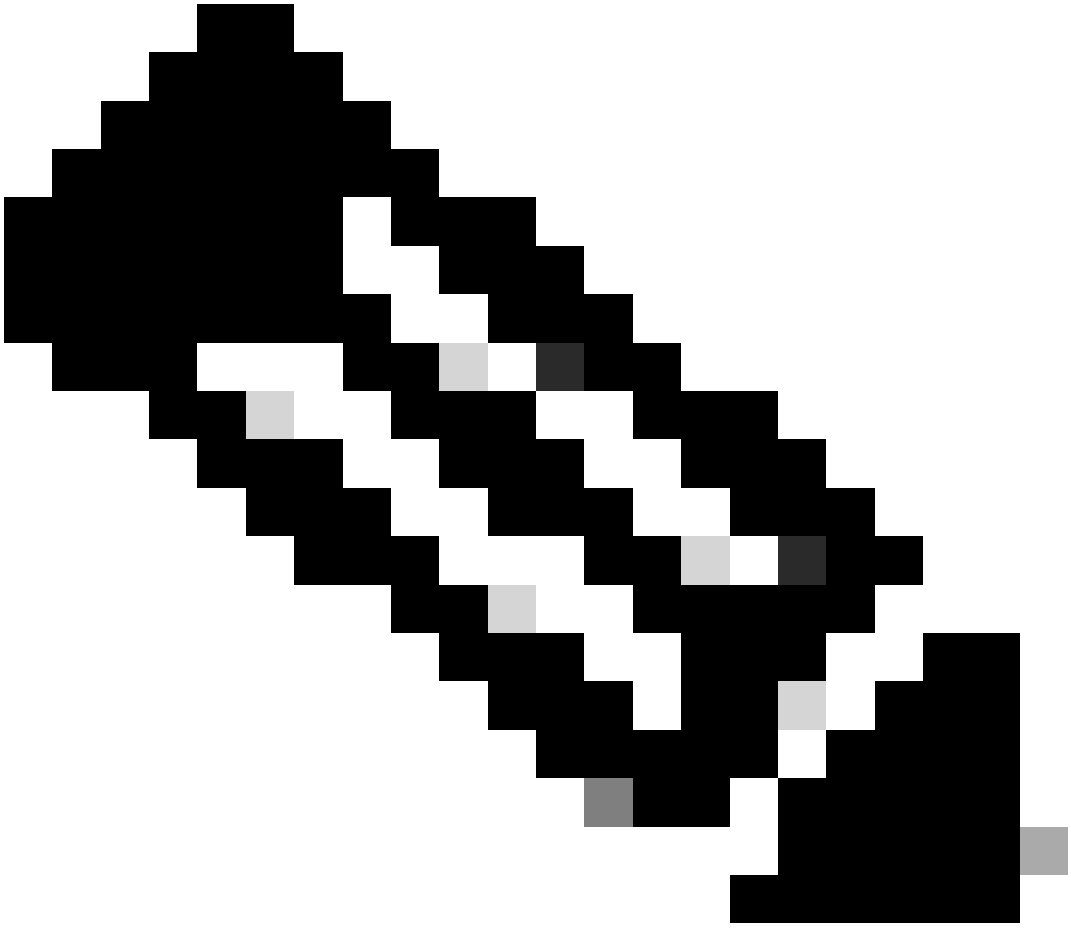
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

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
```

Flujo de tráfico

Escenario normal

Cuando el enlace MPLS está activo, todo el tráfico de VPN 10 y VPN 20 pasa a través del transporte MPLS.

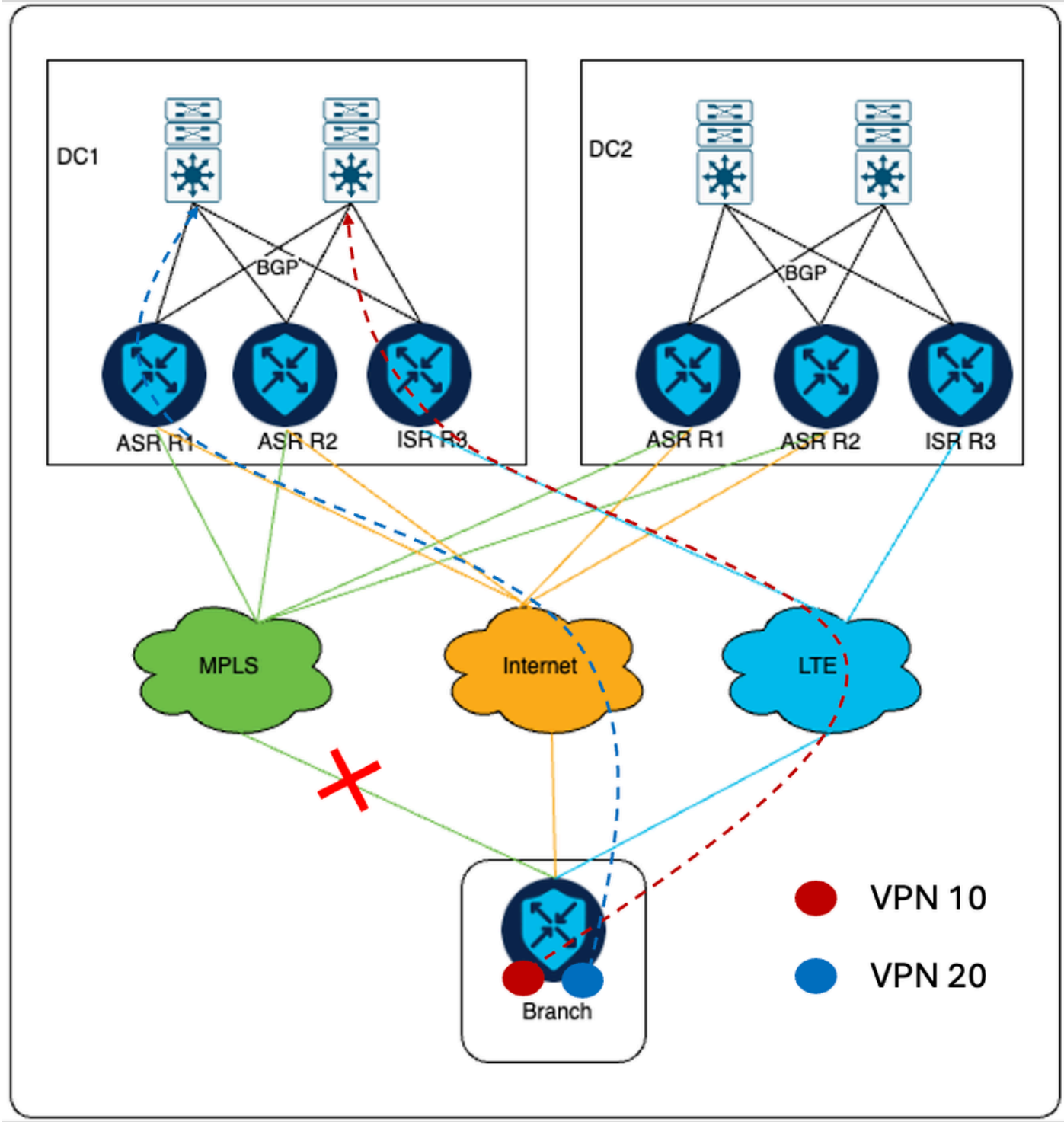

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



Nota: DC1 es el DC primario.

Escenario de Failover

En caso de fallo del enlace MPLS, el tráfico VPN 10 pasa a través del transporte LTE hacia ISR Edge. Donde el tráfico de AS VPN 20 se envía a través del transporte de Internet al dispositivo ASR cEdge.



Para el tráfico de retorno de los switches de núcleo, para el tráfico VPN 10 se envía al ISR cEdge ya que la longitud de AS-PATH es menor a través de ISR en comparación con ASR, como se especifica en la sección de políticas localizadas. Del mismo modo, el tráfico VPN 20 se envía hacia los extremos ASR, ya que AS-PATH es más pequeño a través de ASR en comparación con ISR.

Additional Information

En la configuración anterior, todos los bordes de cada DC están conectados a controladores SD-WAN solo a través del transporte de Internet. Por lo tanto, los routers ISR tienen un túnel de

Internet configurado. El requisito es garantizar que ISR cEdge forme un túnel IPsec a las sucursales remotas solo a través del transporte LTE y, para lograr el requisito dado, el color del túnel en el transporte de Internet de ISR debe configurarse con un color público que no se utilice en la configuración del cliente.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).