Address Number of Data Plane Tunnel Limit in Data Center (Limite de túnel de plano de dados no data center)

Contents

Introdução

Este documento descreve uma solução para resolver problemas de dimensionamento nas bordas SD-WAN do data center à medida que elas se aproximam dos limites do túnel do plano de dados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento de SD-WAN.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador SD-WAN versão 20.6.3.0.54 (ES)
- Cisco IOS® XE (executado no modo controlador) 17.06.03a.0.2 (ES)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

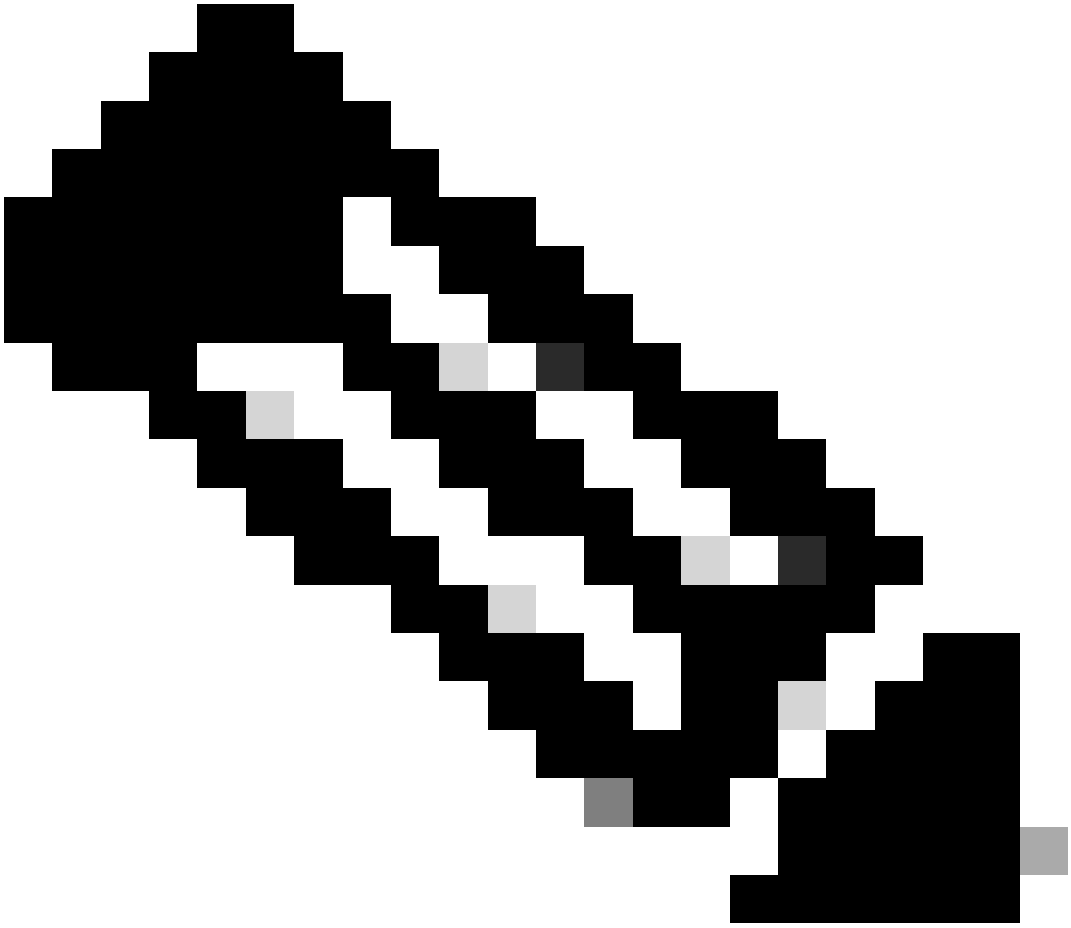
Informações de Apoio

Visão geral do projeto de rede:

- VPN: VPN 10, VPN 20
- Links de transporte: Multiprotocol Label Switching (MPLS), LTE, Internet
- Detalhes do roteador:
    - Roteador principal: 2 em cada data center
      - Modelo: ASR1002-HX
      - Versão do software Cisco IOS XE: 17.06.03a.0.2
    - Roteador secundário: 1 em cada data center
      - Modelo: ISR4451-X
      - Versão do software Cisco IOS XE: 17.06.03a.0.22
- Protocolo de roteamento: o BGP (Border Gateway Protocol) é usado no lado da LAN do data center

Problema

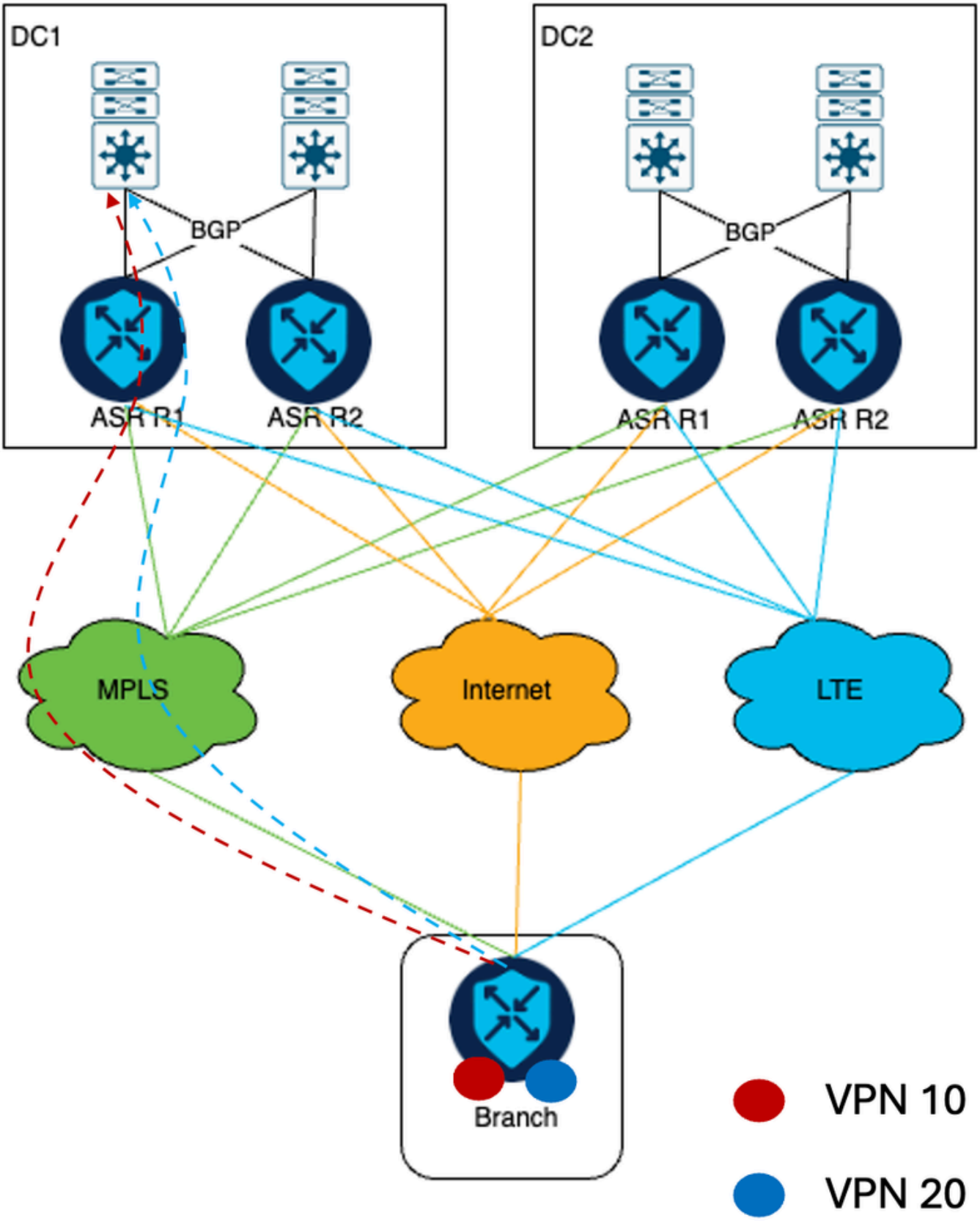
Este documento discute o estudo de caso do cliente com a topologia mostrada, a infraestrutura de rede do cliente compreende dois data centers, cada um com dois ASR1002-HX SD-WAN cEdge implantados. Essa arquitetura de rede tem como objetivo incorporar aproximadamente 3.000 locais de loja na sobreposição de SD-WAN, aproveitando a disponibilidade de três links de transporte distintos.



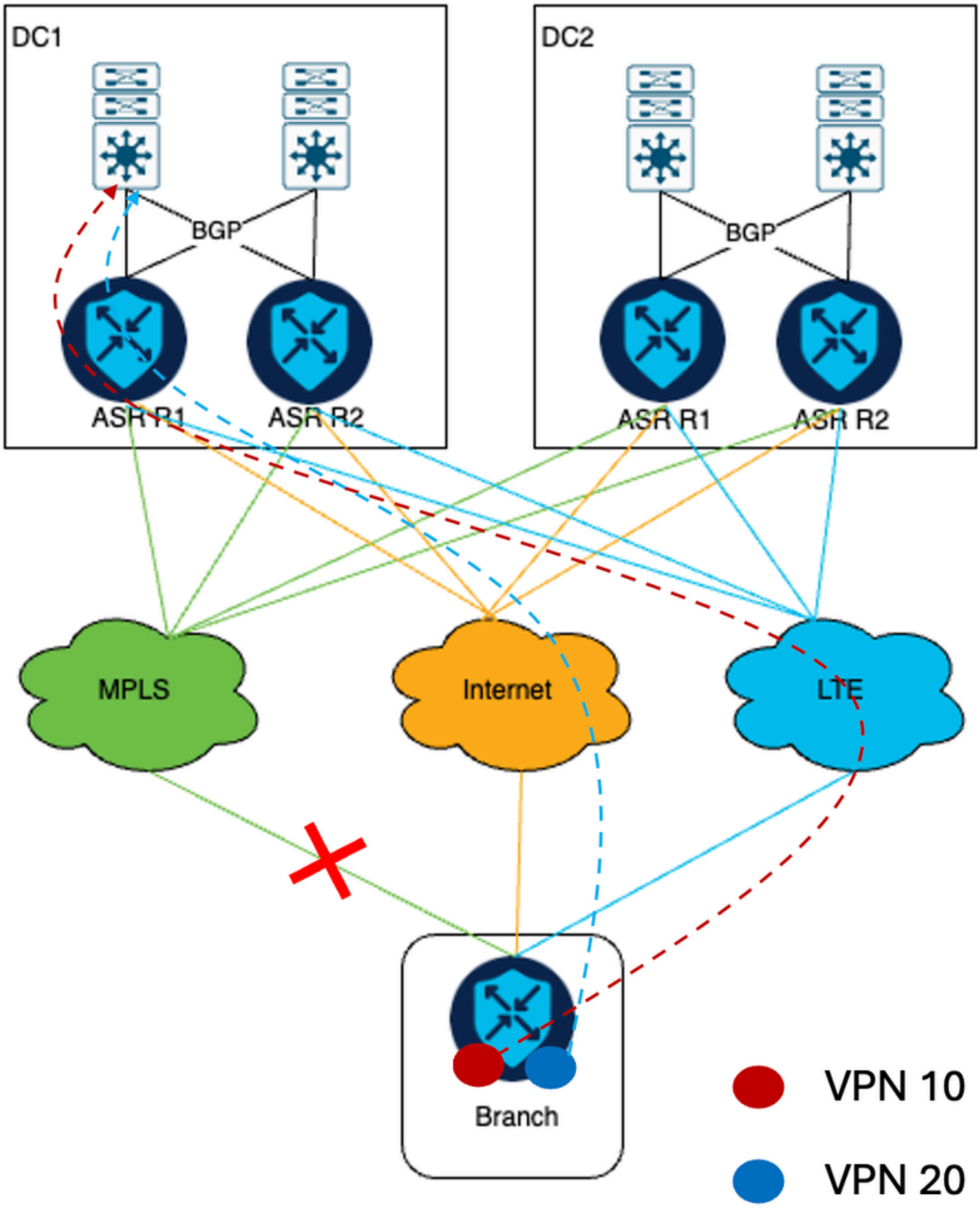
Observação: a topologia Hub and Spoke é implantada. As bordas DC1 e DC2 são hubs. Todas as filiais remotas formam túneis IPsec sobre três transportes disponíveis com DCedges.

Saindo do diagrama de rede

Todo o tráfego da VPN 10 e da VPN 20 passa pelo transporte MPLS.



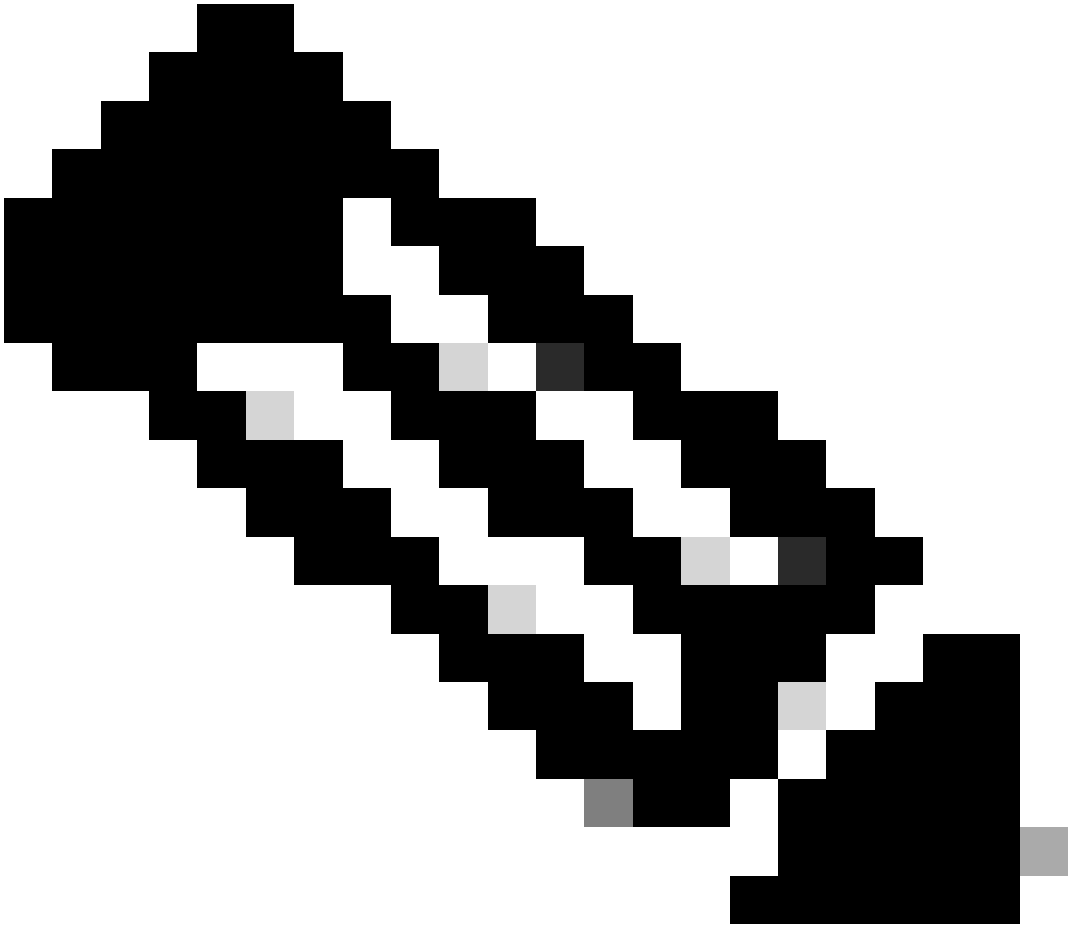
Se o link MPLS ficar inativo, o tráfego da VPN 10 será transferido para o transporte LTE e o tráfego da VPN 20 será transferido para o transporte da Internet.



O desafio técnico neste cenário surge da escala e dos requisitos específicos de uma implantação de rede de clientes. Considerando a implantação de 3.000 roteadores SD-WAN que estabelecem túneis IPSec através de três tipos de transporte para o roteador do data center, a contagem total de túneis IPSec formados nos roteadores de headend primário ASR1002-HX chega a 9.000. No entanto, o ASR1002-HX está limitado a 8.000 túneis IPSec (fonte: Ficha técnica do ASR1K).

Solução

Para resolver isso, o cliente decidiu adicionar um dispositivo ISR4451-X de borda central em cada DC de acordo com o requisito de escalabilidade futuro do cliente.



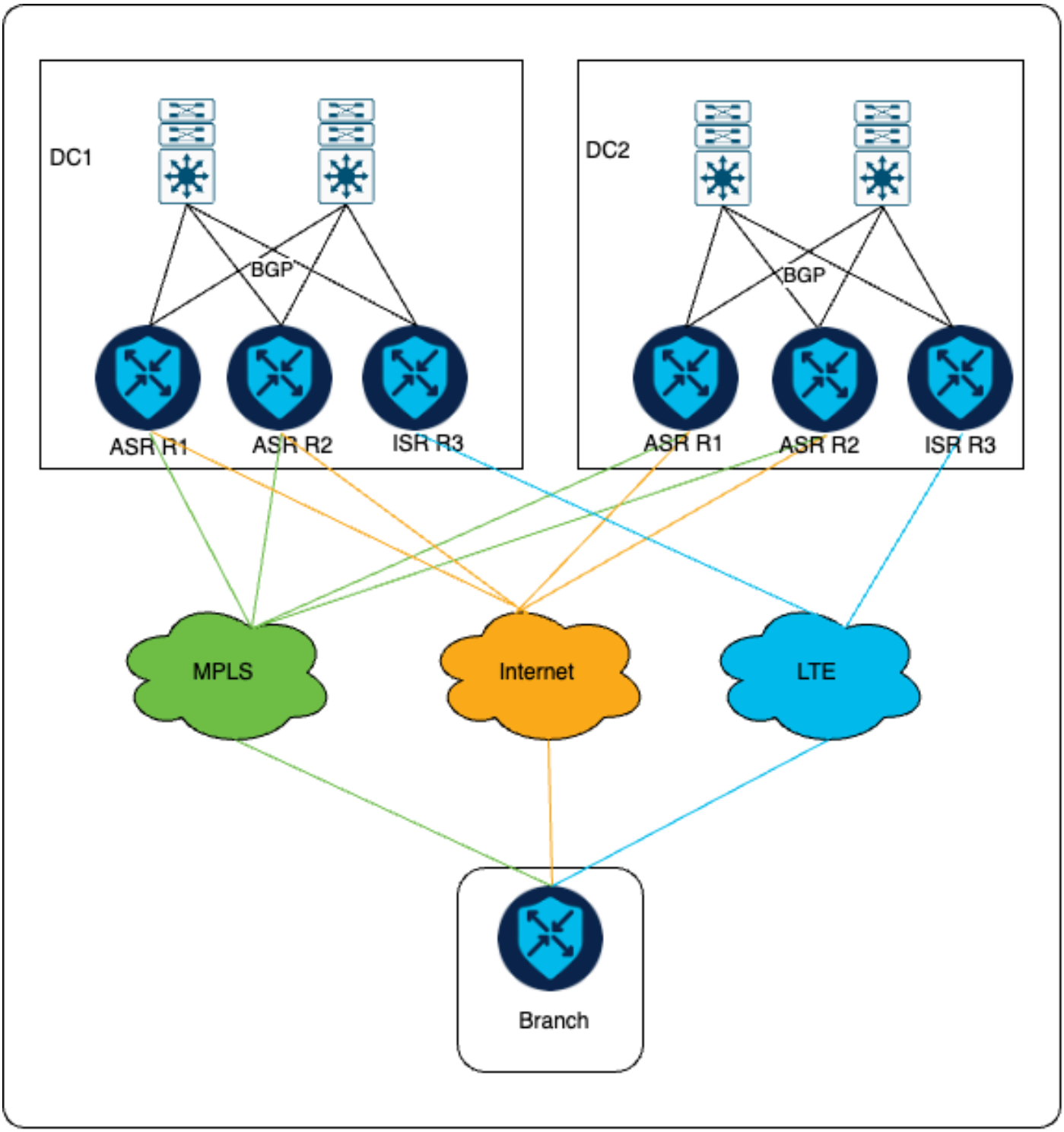
> Observação: escolha um modelo de dispositivo adicional com base no requisito de escalabilidade do cliente.

Topologia de rede

Como parte da solução, as Bordas do Roteador de Serviços de Agregação (ASR) principal continuam a formar um túnel IPSec sobre MPLS e transporte de Internet, e as Bordas do Roteador de Serviços Integrados (ISR) recém-instaladas formam um túnel IPsec somente através de transporte LTE.

Conforme descrito no diagrama, os túneis IPSec são estabelecidos entre o ponto inicial do ASR e

a filial através do MPLS e da Internet, enquanto entre o ISR e a filial, os túneis IPSec são estabelecidos exclusivamente através do LTE.



O requisito do cliente é que, em circunstâncias normais, todo o tráfego VPN 10 e VPN 20 utilize o transporte MPLS para comunicação. No entanto, no caso de uma falha de link MPLS, o tráfego VPN 20 é roteado novamente através do transporte de Internet, enquanto o tráfego VPN 10 é redirecionado através do transporte LTE, comportamento como antes de adicionar cEdge adicional.

Configurar

Políticas centralizadas e localizadas são usadas para garantir que o tráfego seja enviado através do transporte correto de acordo com a preferência do cliente. O tráfego que chega da filial pelo link da Internet e pelo link LTE é marcado. Essas tags são usadas para garantir que os switches LAN no headend enviem mensagens de resposta para a VPN 10 corretamente para o roteador ISR e que o tráfego da VPN 20 seja enviado para os dispositivos headend do ASR.

Configuração de política centralizada

Esta é a política preparada para atender aos requisitos do cliente. Para o tráfego que chega através do link de Internet, uma tag OMP de 200 é atribuída. Por outro lado, o tráfego que chega através do link LTE recebe uma marca 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>
```

No DC, ao encaminhar o tráfego dos roteadores SD-WAN para os switches centrais, o campo AS-PATH é manipulado ao anunciar a rota no BGP no lado da LAN. Um mapa de rotas é aplicado na configuração do BGP no momento da redistribuição das rotas OMP no BGP.

Quando o link MPLS está operacional, somente as Bordas primárias redistribuem rotas no BGP, pois nenhum tráfego é recebido via LTE. No entanto, no caso de uma falha de link de MPLS:

- Para a VPN 10, as Bordas ASR redistribuem rotas anexando o campo AS-PATH quatro vezes, enquanto o ISR cEdge redistribui anexando o campo AS-PATH três vezes. Essa configuração garante que o ISR cEdge seja preferido para o envio de respostas.

- Da mesma forma, para VPN 20, as Bordas ASR redistribuem prefixos sem anexar nenhum AS-PATH, e o ISR cEdge redistribui prefixos anexando o campo AS-PATH três vezes. Isso garante que as bordas ASR sejam preferidas.

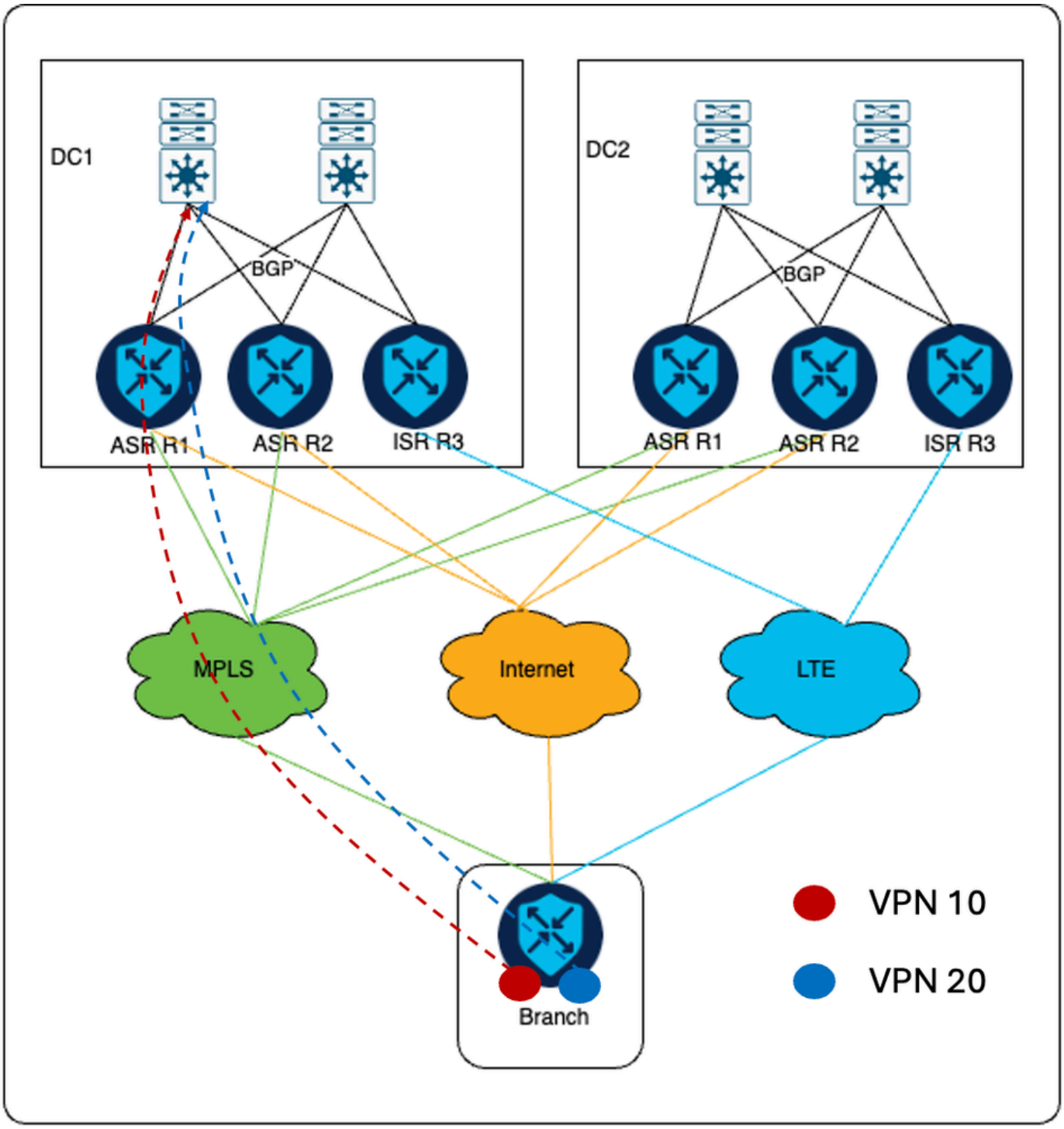
Configuração de Política Localizada

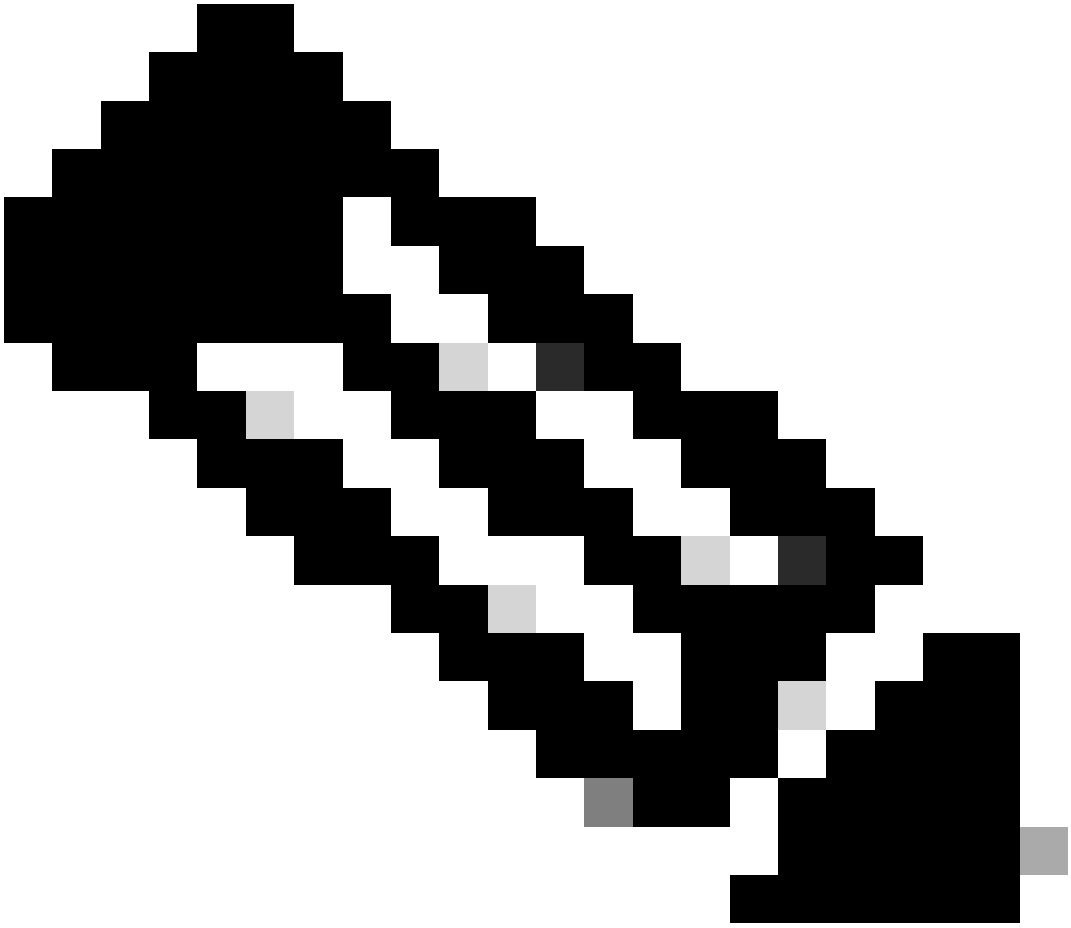
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

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
```

Fluxo de tráfico

Cenário Normal

Quando o link MPLS está ativo, todo o tráfego da VPN 10 e da VPN 20 atravessa o transporte MPLS.

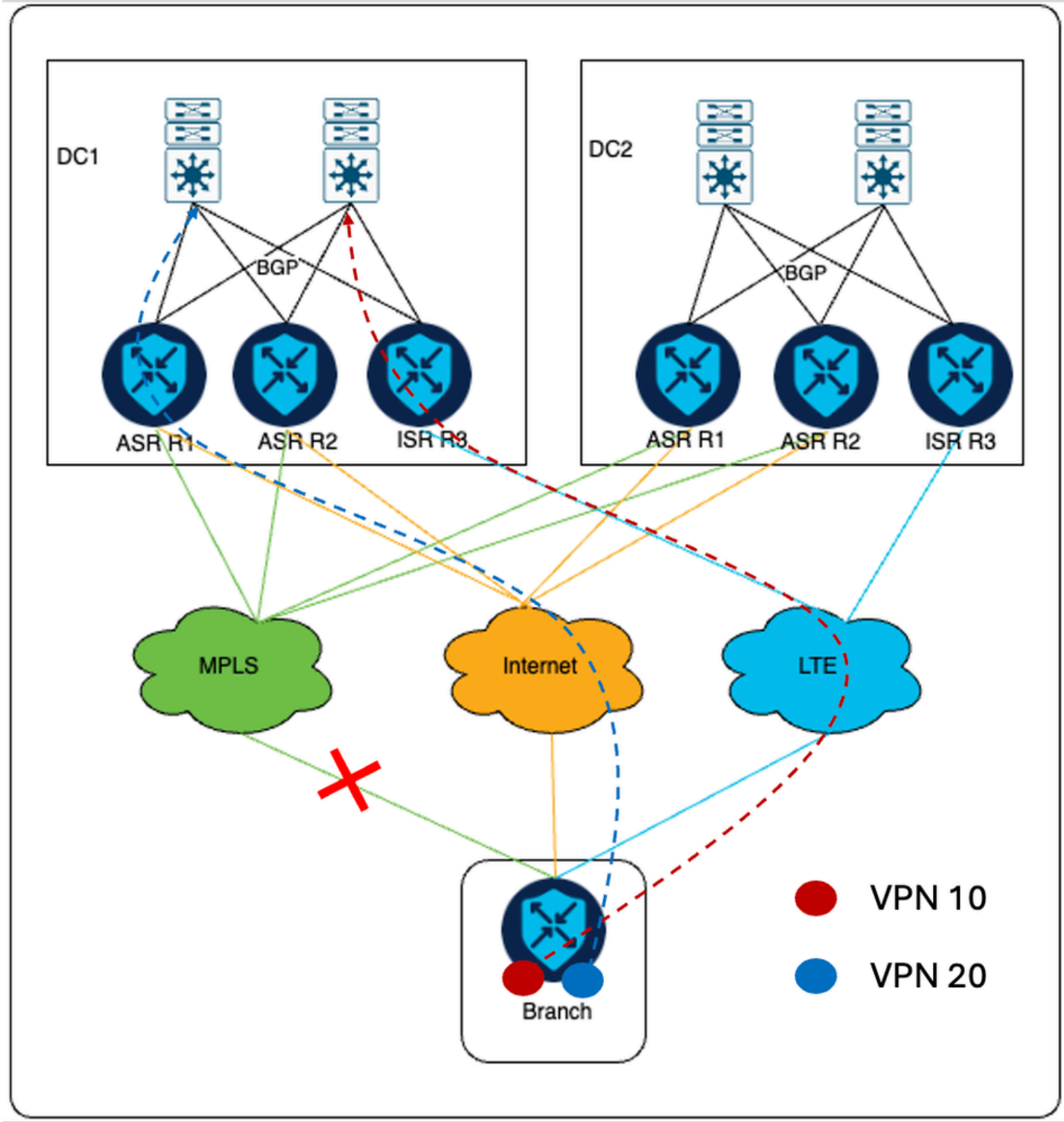

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



Observação: DC1 é o DC principal.

Cenário de failover

No caso de falha do link MPLS, o tráfego VPN 10 passa pelo transporte LTE em direção ao ISR cEdge. Onde o tráfego VPN 20 é enviado através do transporte da Internet para o dispositivo ASR cEdge.



Para o tráfego de retorno de switches centrais, para o tráfego VPN 10 é enviado para o ISR cEdge, pois o comprimento do AS-PATH é menor via ISR em comparação ao ASR, conforme especificado na seção de política localizada. Da mesma forma, o tráfego VPN 20 é enviado para as Bordas ASR, pois o AS-PATH é menor via ASR em comparação ao ISR.

Informações adicionais

Na configuração anterior, todas as bordas em cada DC são conectadas aos controladores SD-WAN somente através do transporte da Internet. Assim, os roteadores ISR têm o túnel de Internet configurado. O requisito é garantir que o ISR cEdge forme um túnel IPsec para filiais remotas

apenas através do transporte LTE e, para atingir o requisito especificado, a cor do túnel no transporte de Internet do ISR deve ser configurada com uma cor pública que não esteja em uso na configuração do cliente.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.