데이터 센터의 데이터 플레인 터널 제한 주소 번호

목차

소개

이 문서에서는 데이터 센터 SD-WAN cEdge가 데이터 플레인 터널 제한에 근접함에 따라 데이터 센터 SD-WAN cEdge의 확장 문제를 해결하기 위한 솔루션을 설명합니다.

사전 요구 사항

요구 사항

SD-WAN에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SD-WAN Controller 버전 20.6.3.0.54(ES)
- Cisco IOS® XE(컨트롤러 모드에서 실행) 17.06.03a.0.2(ES)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

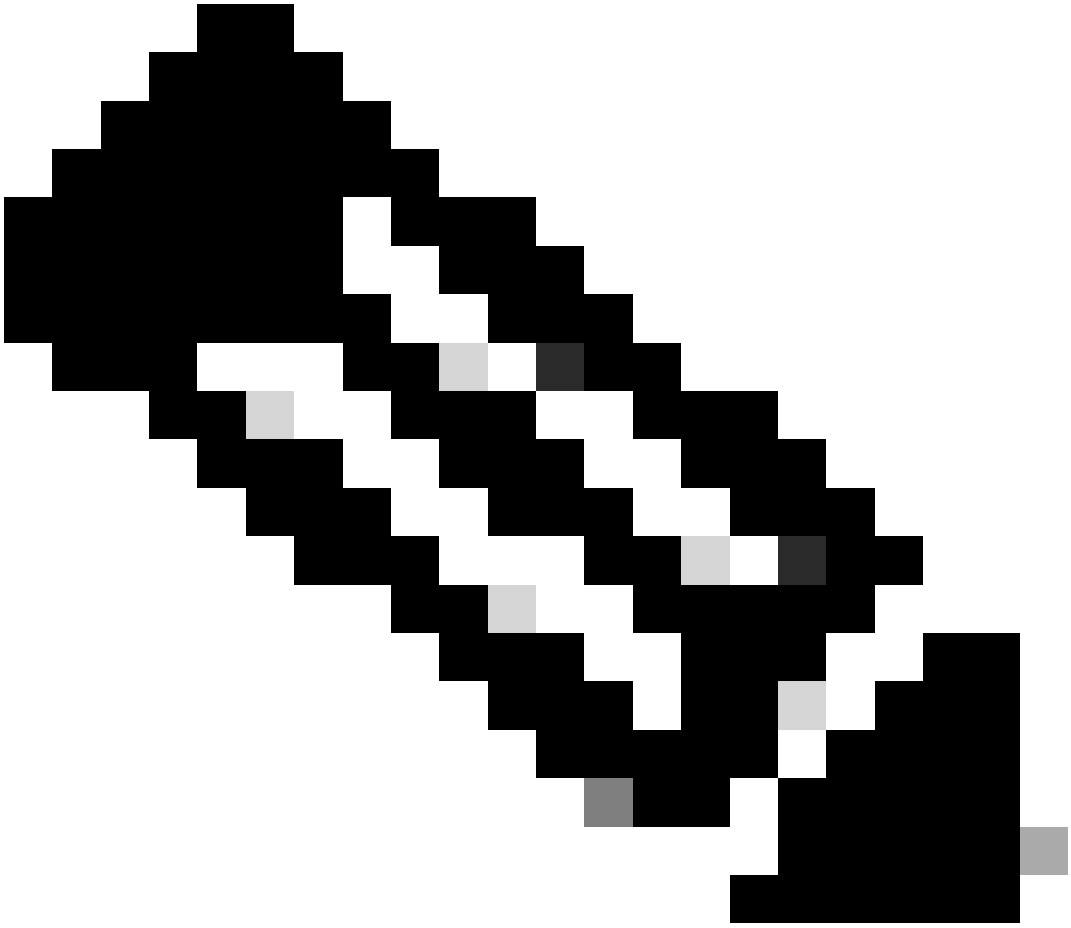
배경 정보

네트워크 설계 개요:

- VPN: VPN 10, VPN 20
- 전송 링크: MPLS(Multiprotocol Label Switching), LTE, 인터넷
- 라우터 세부 정보:
    - 기본 라우터: 각 데이터 센터에서 2개
      - 모델: ASR1002-HX
      - Cisco IOS XE 소프트웨어 버전: 17.06.03a.0.2
    - 보조 라우터: 각 데이터 센터에 1개
      - 모델: ISR4451-X
      - Cisco IOS XE 소프트웨어 버전: 17.06.03a.0.22
- 라우팅 프로토콜: BGP(Border Gateway Protocol)가 데이터 센터 LAN 측에서 사용됨

문제

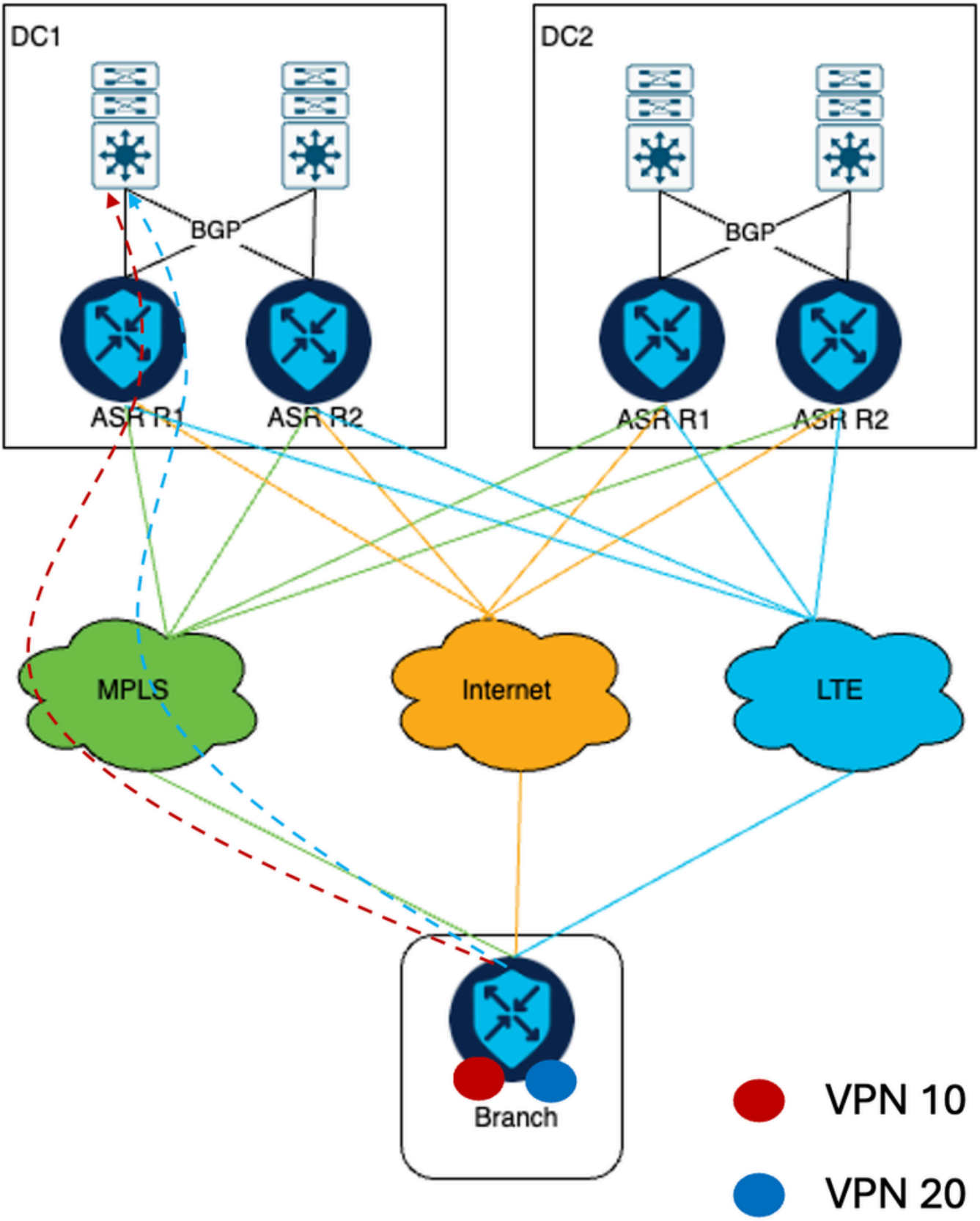
이 문서에서는 토폴로지가 표시된 고객 사례 연구에 대해 설명합니다. 고객의 네트워크 인프라는 두 개의 데이터 센터로 구성되며 각각 두 개의 ASR1002-HX SD-WAN cEdge가 구축되어 있습니다. 이 네트워크 아키텍처는 SD-WAN 오버레이에 약 3,000개의 매장 위치를 통합하는 것을 목표로 하며, 3개의 서로 다른 전송 링크의 가용성을 활용합니다.



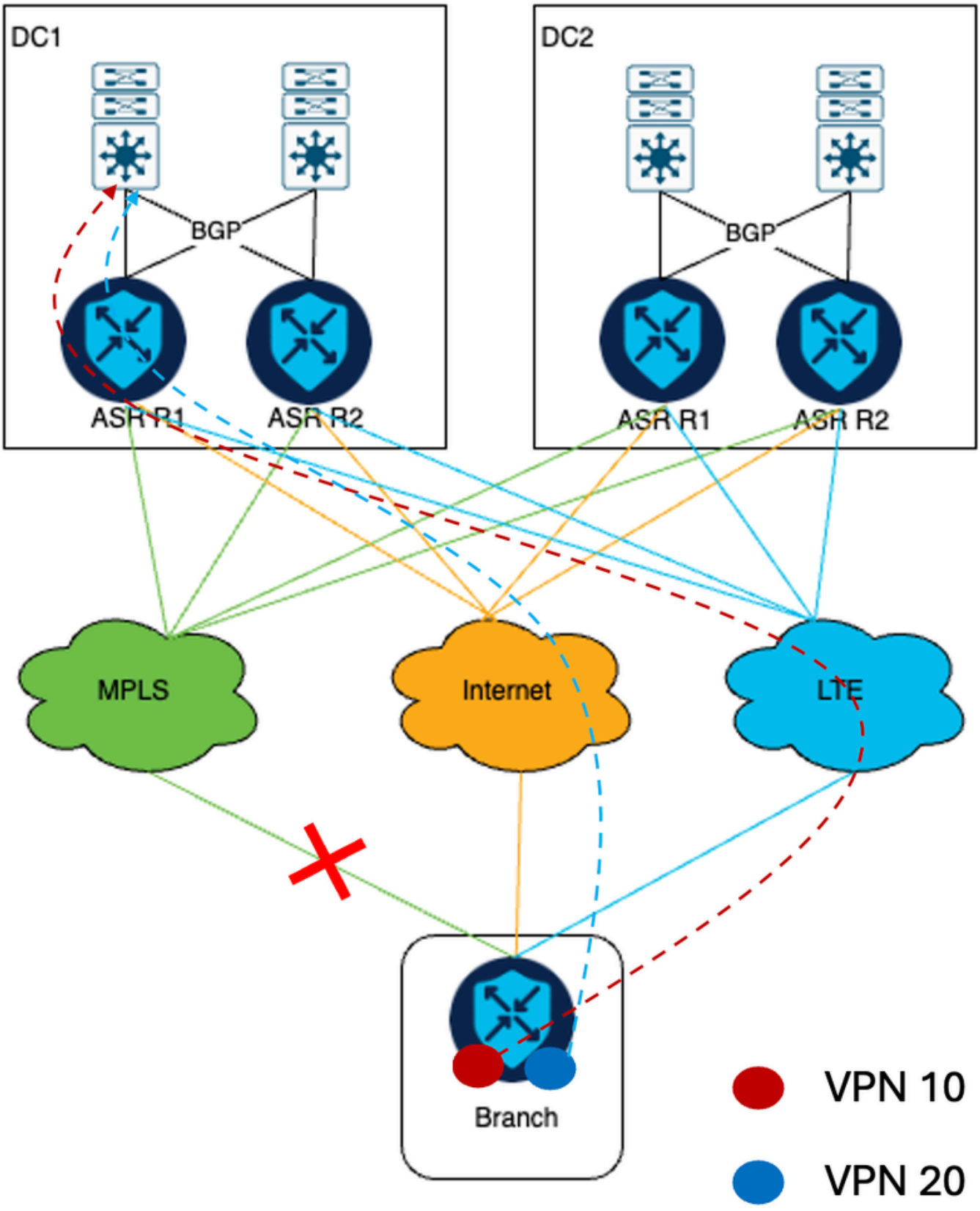
참고: 허브 및 스포크 토폴로지가 구축되었습니다. DC1 및 DC2 Edge는 허브입니다. 모든 원격 브랜치는 DC cEdge를 통해 사용 가능한 세 가지 전송을 통해 IPsec 터널을 형성합니다.

네트워크 다이어그램 종료

VPN 10 및 VPN 20의 모든 트래픽은 MPLS 전송을 통해 이동합니다.



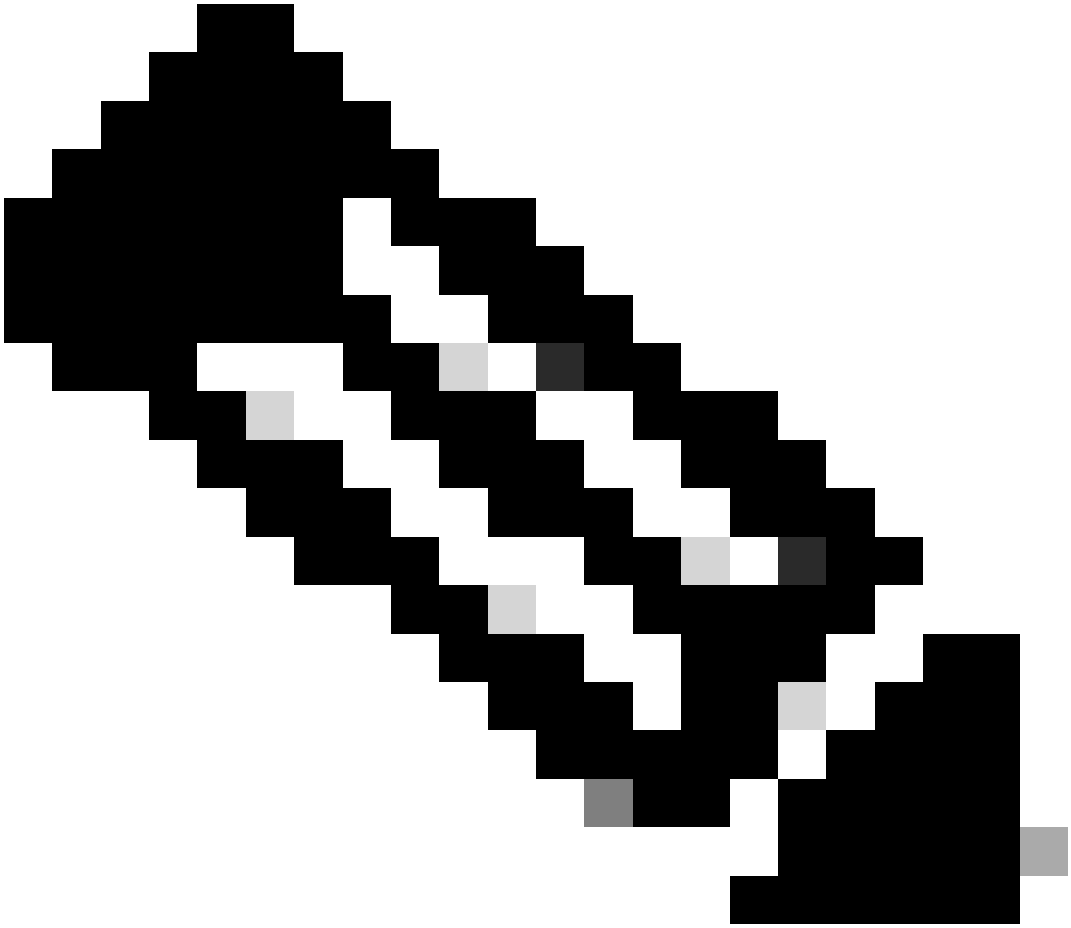
MPLS 링크가 중단되면 VPN 10 트래픽은 LTE 전송으로, VPN 20 트래픽은 인터넷 전송으로 이동합니다.



이 시나리오의 기술적 과제는 고객의 네트워크 구축의 규모 및 특정 요구 사항에 따라 발생합니다. 데이터 센터 라우터로의 세 가지 전송 유형을 통해 IPSec 터널을 설정하는 SD-WAN 라우터 3000개를 구축한 것을 고려하면 ASR1002-HX 기본 헤드엔드 라우터에 형성된 IPSec 터널의 총 수는 9000개에 이릅니다. 그러나 ASR1002-HX는 8000 IPSec 터널로 제한됩니다(출처: [ASR1K 데이터시트](#)).

솔루션

이를 해결하기 위해 고객은 향후 고객의 확장성 요구 사항에 따라 각 DC에 ISR4451-X cEdge 디바이스를 추가하기로 결정했습니다.

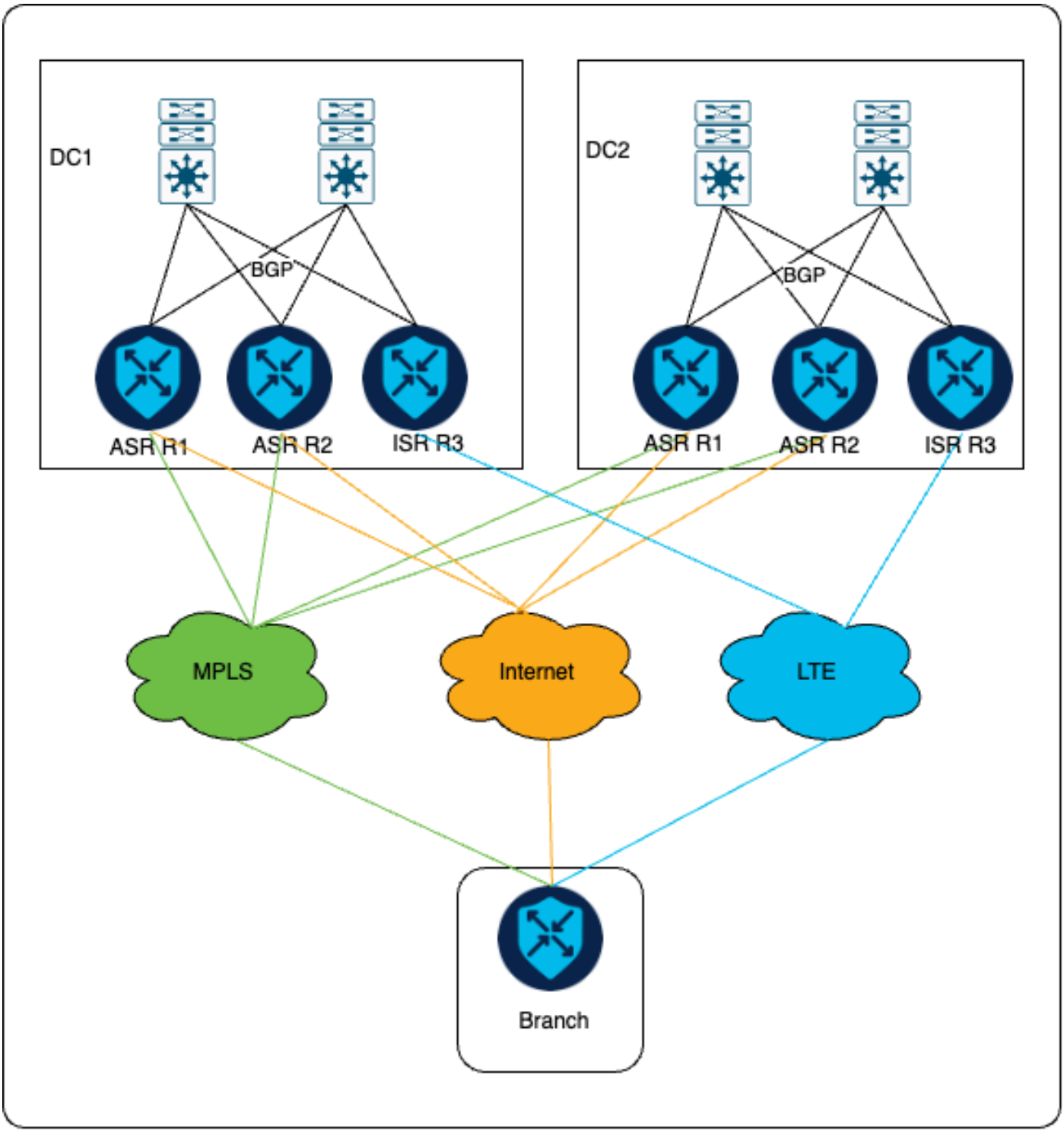


참고: 고객의 확장성 요구 사항에 따라 추가 디바이스 모델을 결정하십시오.

네트워크 토폴로지

솔루션의 일부로서, 기본 ASR(Aggregation Services Router) cEdge는 MPLS 및 인터넷 전송을 통해 IPSec 터널을 계속 형성하고 새로 설치된 ISR(Integrated Service Router) cEdge는 LTE 전송만 통해 IPsec 터널을 형성합니다.

다이어그램에 나와 있는 것처럼, IPSec 터널은 MPLS 및 인터넷을 통해 ASR 헤드엔드와 브랜치 간에 설정되고, ISR과 브랜치 간에는 LTE를 통해서만 설정됩니다.



일반적인 상황에서는 모든 VPN 10 및 VPN 20 트래픽이 통신에 MPLS 전송을 활용해야 합니다. 그러나 MPLS 링크 장애가 발생하면 VPN 20 트래픽은 인터넷 전송을 통해 다시 라우팅되는 반면, VPN 10 트래픽은 LTE 전송을 통해 다시 리디렉션되어 cEdge를 추가하기 전과 같은 동작이 수행됩니다.

구성

고객의 환경 설정에 따라 올바른 전송을 통해 트래픽이 전송되도록 보장하는 중앙 집중식 및 지역화된 정책이 사용됩니다. 지사 위치에서 인터넷 링크 및 LTE 링크를 통해 들어오는 트래픽은 태그가 지정됩니다. 이러한 태그는 헤드엔드의 LAN 스위치가 VPN 10에 대한 회신 메시지를 ISR 라우터로 올바르게 전송하고 VPN 20 트래픽이 ASR 헤드엔드 장치로 전송되도록 하는 데 사용됩니다.

중앙 집중식 정책 컨피그레이션

다음은 고객의 요구 사항을 충족하기 위해 마련된 정책입니다. 인터넷 링크를 통해 도착하는 트래픽에는 OMP 태그 200이 할당됩니다. 반면, LTE 링크를 통해 도착하는 트래픽에는 OMP 태그 100이 할당된다.

<#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>
```

DC에서는 SD-WAN 라우터에서 코어 스위치로 트래픽을 전달하는 동안 LAN 측의 BGP로 경로를 광고할 때 AS-PATH 필드가 조작됩니다. 경로 맵은 BGP에서 OMP 경로를 재배포할 때 BGP 컨피그레이션에 적용됩니다.

MPLS 링크가 작동하는 경우, LTE를 통해 트래픽이 수신되지 않으므로 기본 cEdge만 BGP에서 경로를 재배포합니다. 그러나 MPLS 링크 장애가 발생하는 경우:

- VPN 10의 경우 ASR cEdge는 AS-PATH 필드를 4번 추가하여 경로를 재배포하는 반면 ISR cEdge는 AS-PATH 필드를 3번 추가하여 경로를 재배포합니다. 이 컨피그레이션을 통해 ISR cEdge가 회신 전송에 선호됩니다.
- 마찬가지로 VPN 20의 경우 ASR cEdge는 AS-PATH를 추가하지 않고 접두사를 재배포하며 ISR cEdge는 AS-PATH 필드를 세 번 추가하여 접두사를 재배포합니다. 이렇게 하면 ASR Edge가 우선적으로 사용됩니다.

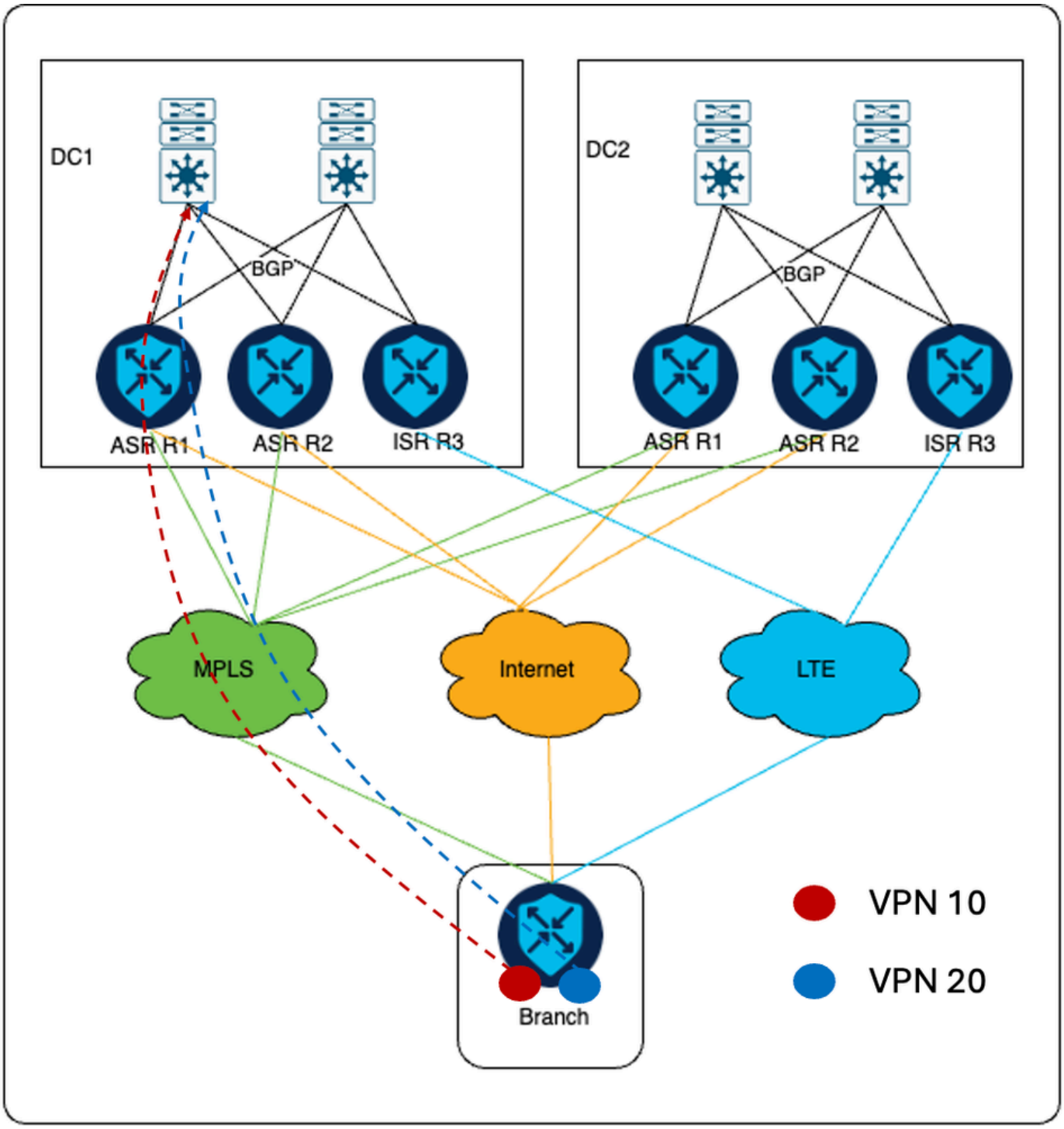
현지화된 정책 컨피그레이션

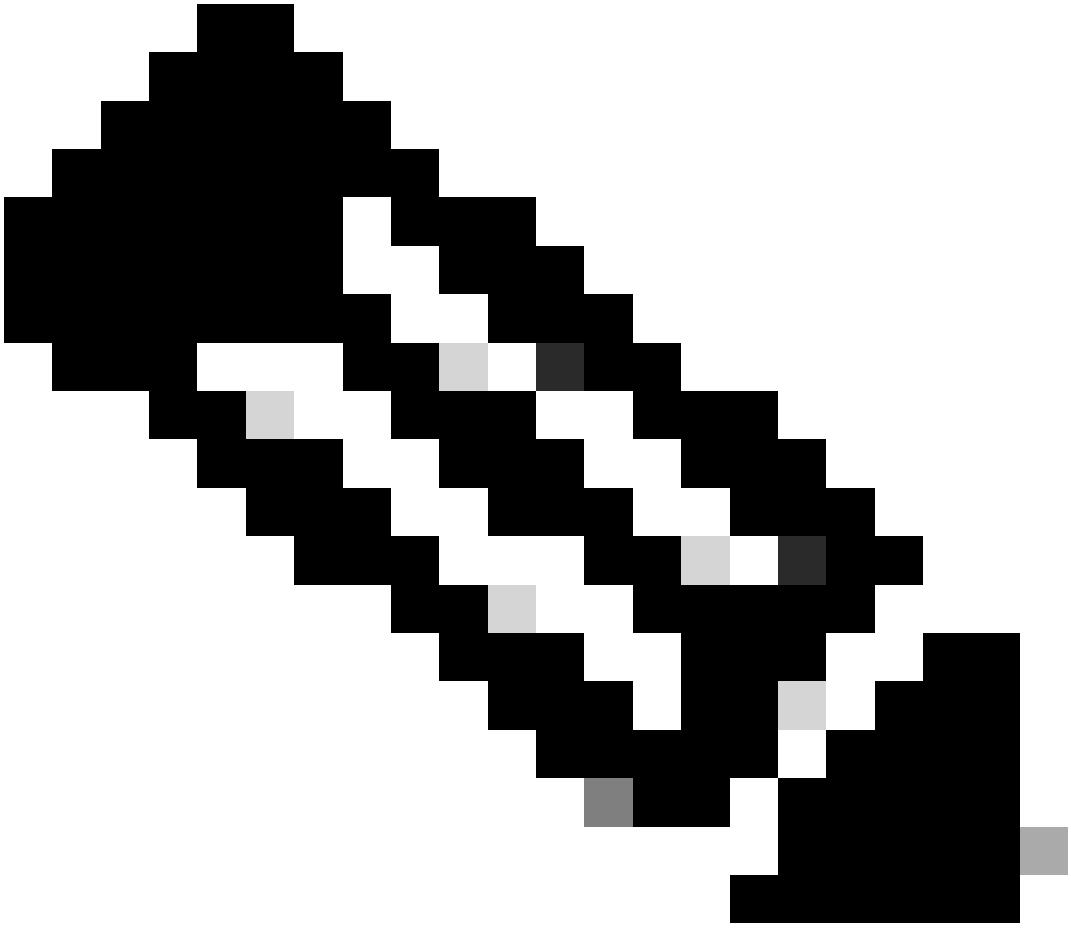
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

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
```

트래픽 흐름

일반 시나리오

MPLS 링크가 작동하면 VPN 10 및 VPN 20의 모든 트래픽이 MPLS 전송을 통해 이동합니다.

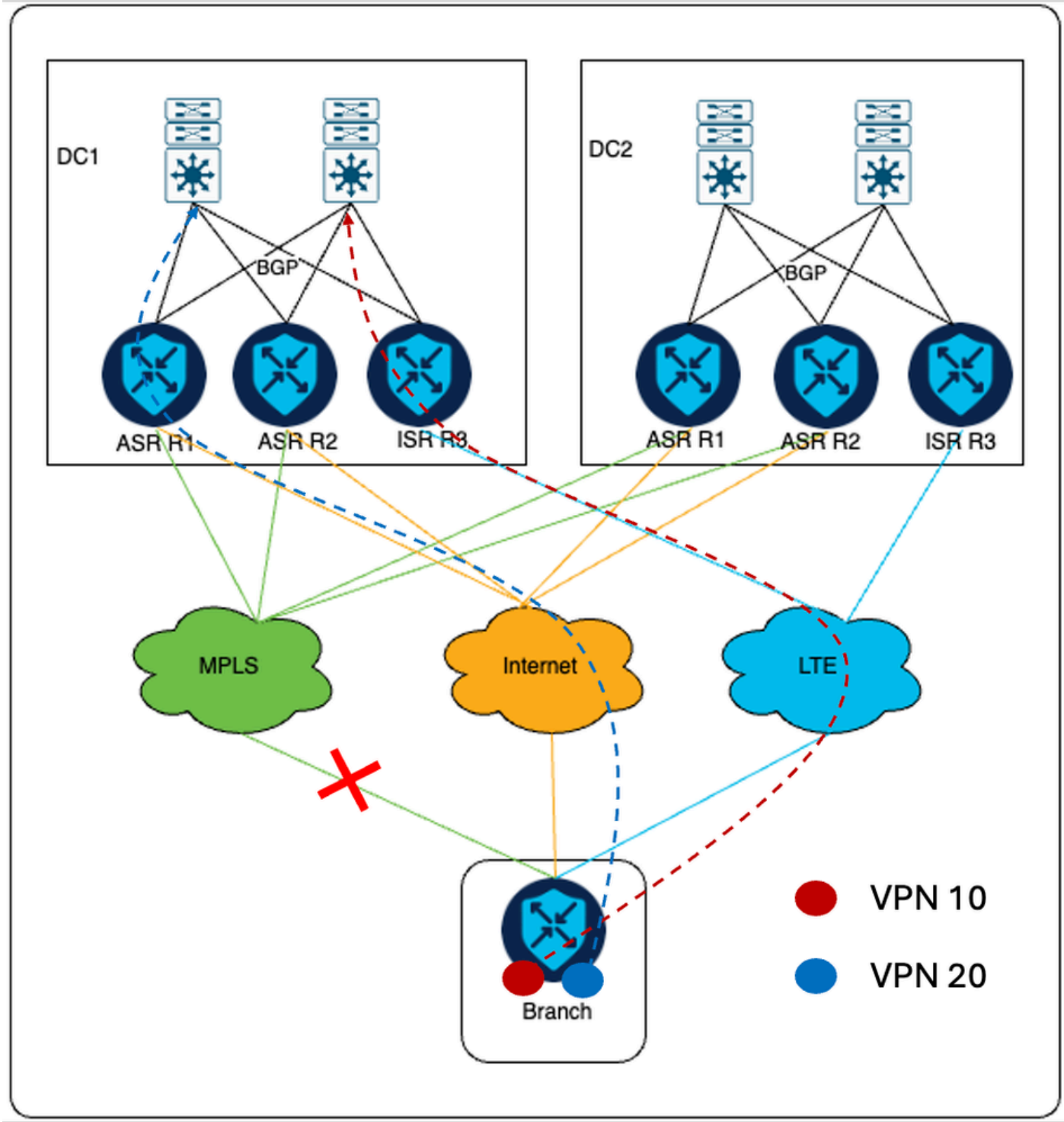

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



참고: DC1이 기본 DC입니다.

장애 조치 시나리오

MPLS 링크 장애 시 VPN 10 트래픽은 LTE 전송을 통해 ISR cEdge로 이동합니다. 여기서 VPN 20 트래픽은 인터넷 전송을 통해 ASR cEdge 디바이스로 전송됩니다.



코어 스위치에서 반환 트래픽의 경우, VPN 10 트래픽은 ISR을 통해 AS-PATH 길이가 현지화된 정책 섹션에 지정된 ASR에 비해 작으므로 ISR cEdge로 전송됩니다. 마찬가지로 VPN 20 트래픽은 AS-PATH가 ISR에 비해 ASR을 통해 작으므로 ASR cEdge로 전송됩니다.

추가 정보

이전 설정에서는 각 DC의 모든 cEdge가 인터넷 전송을 통해서만 SD-WAN 컨트롤러에 연결됩니다. 따라서 ISR 라우터에는 인터넷 터널이 구성되어 있습니다. 요구 사항은 ISR cEdge가 LTE 전송을 통해서만 원격 지사에 IPsec 터널을 형성하도록 하는 것이며, 주어진 요구 사항을 달성하기 위해 ISR의 인터넷 전송에 대한 터널 색상을 고객 설정에서 사용되지 않는 공용 색상으로 구성해야 합니

다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.