データセンターのデータプレーントンネル制限のアドレス番号

内容

はじめに

このドキュメントでは、データセンターのSD-WAN cEdgeがデータプレーンのトンネルの限界に近づくにつれて発生するスケーリングの問題に対処するためのソリューションについて説明します。

前提条件

要件

SD-WANに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- SD-WANコントローラバージョン20.6.3.0.54(ES)
- Cisco IOS® XE（コントローラモードで実行）17.06.03a.0.2(ES)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

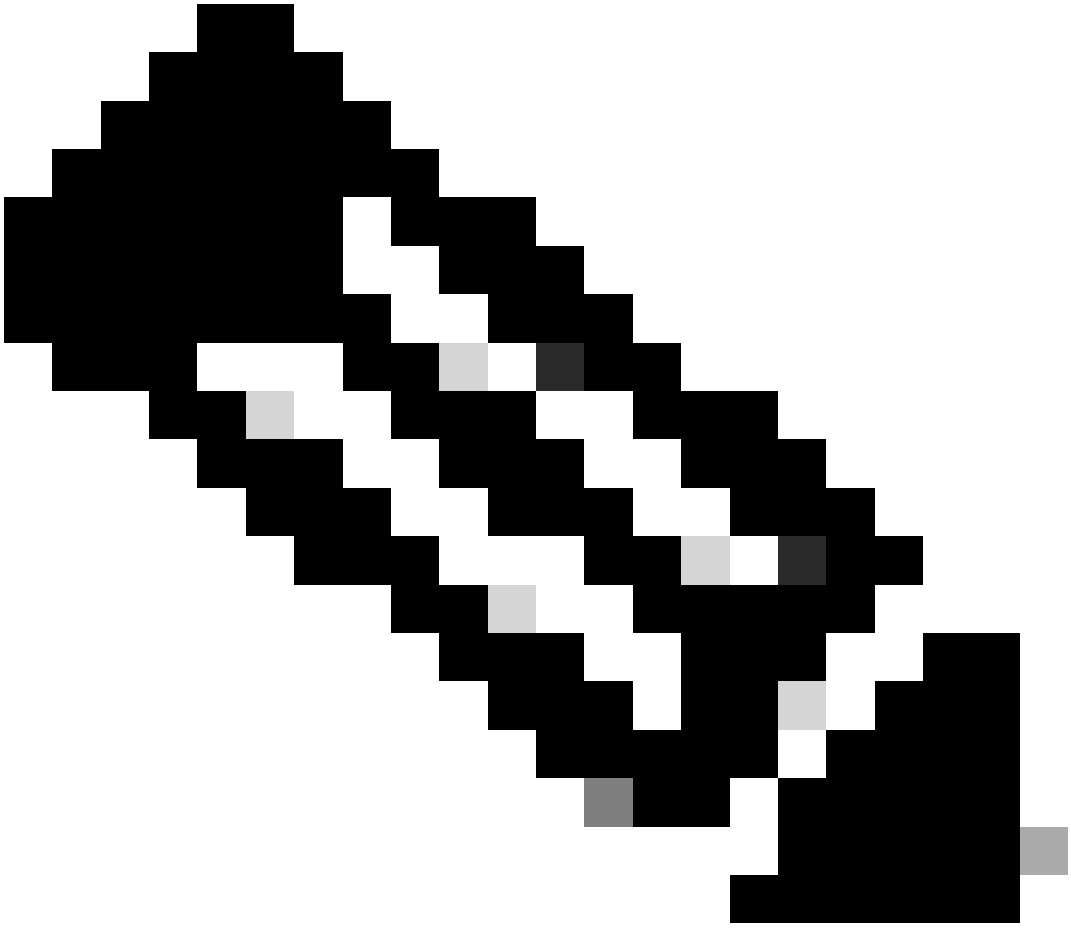
背景説明

ネットワーク設計の概要

- VPN:VPN 10、VPN 20
- トランスポートリンク：マルチプロトコルラベルスイッチング(MPLS)、LTE、インターネット
- ルータの詳細：
    - プライマリルータ：各データセンターに2台
      – モデル：ASR1002-HX
      - Cisco IOS XEソフトウェアバージョン：17.06.03a.0.2
    - セカンダリルータ：各データセンターに1台
      – モデル：ISR4451-X
      - Cisco IOS XEソフトウェアバージョン：17.06.03a.0.22
- ルーティングプロトコル：ボーダーゲートウェイプロトコル(BGP)がデータセンターLAN側で使用されます。

問題

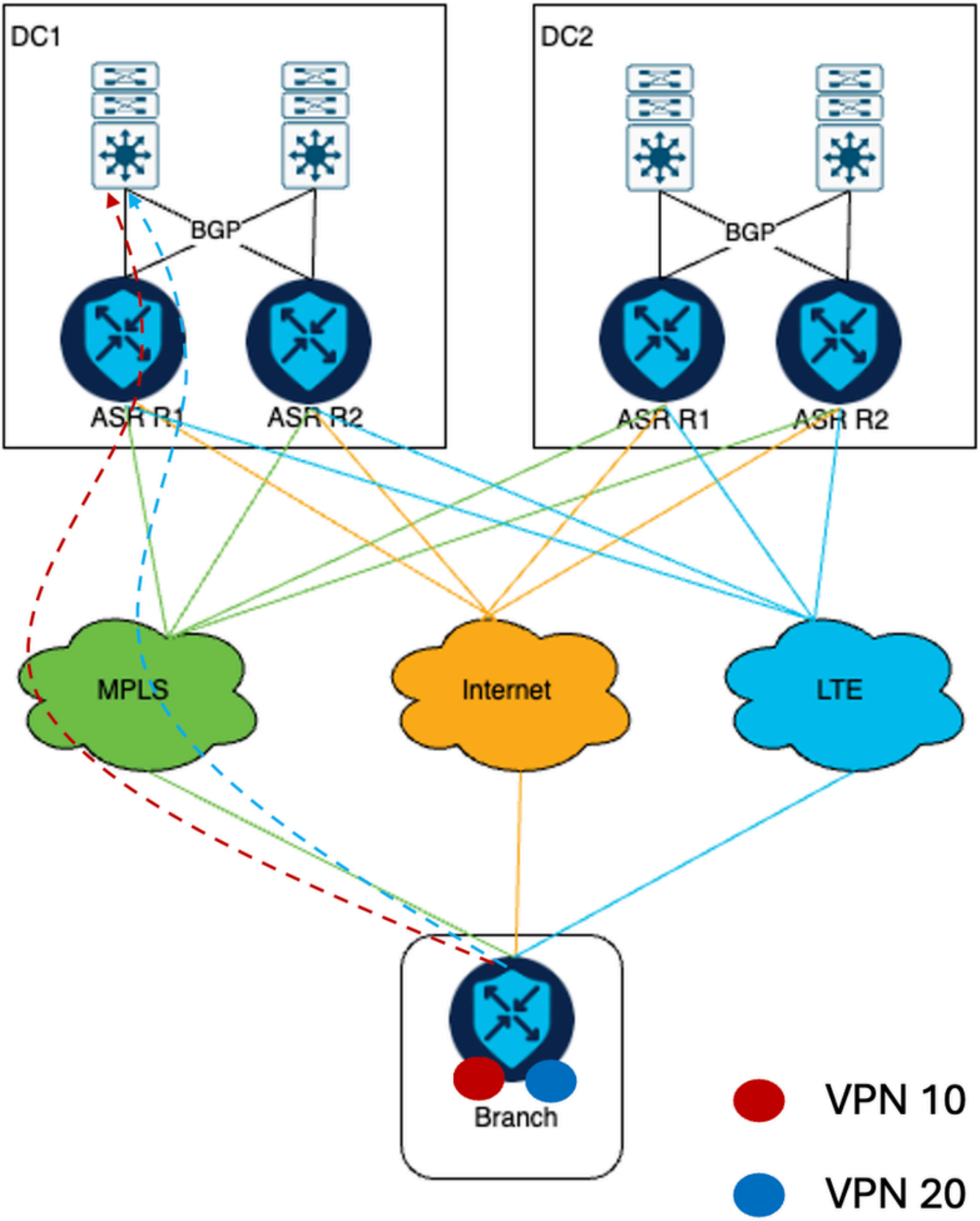
このドキュメントでは、トポロジを示した顧客事例について説明します。顧客のネットワークインフラストラクチャは2つのデータセンターで構成され、各データセンターには2つのASR1002-HX SD-WAN cEdgeが導入されています。このネットワークアーキテクチャは、3つの異なるトランスポートリンクの可用性を活用して、約3000の店舗ロケーションをSD-WANオーバーレイに組み込むことを目的としています。



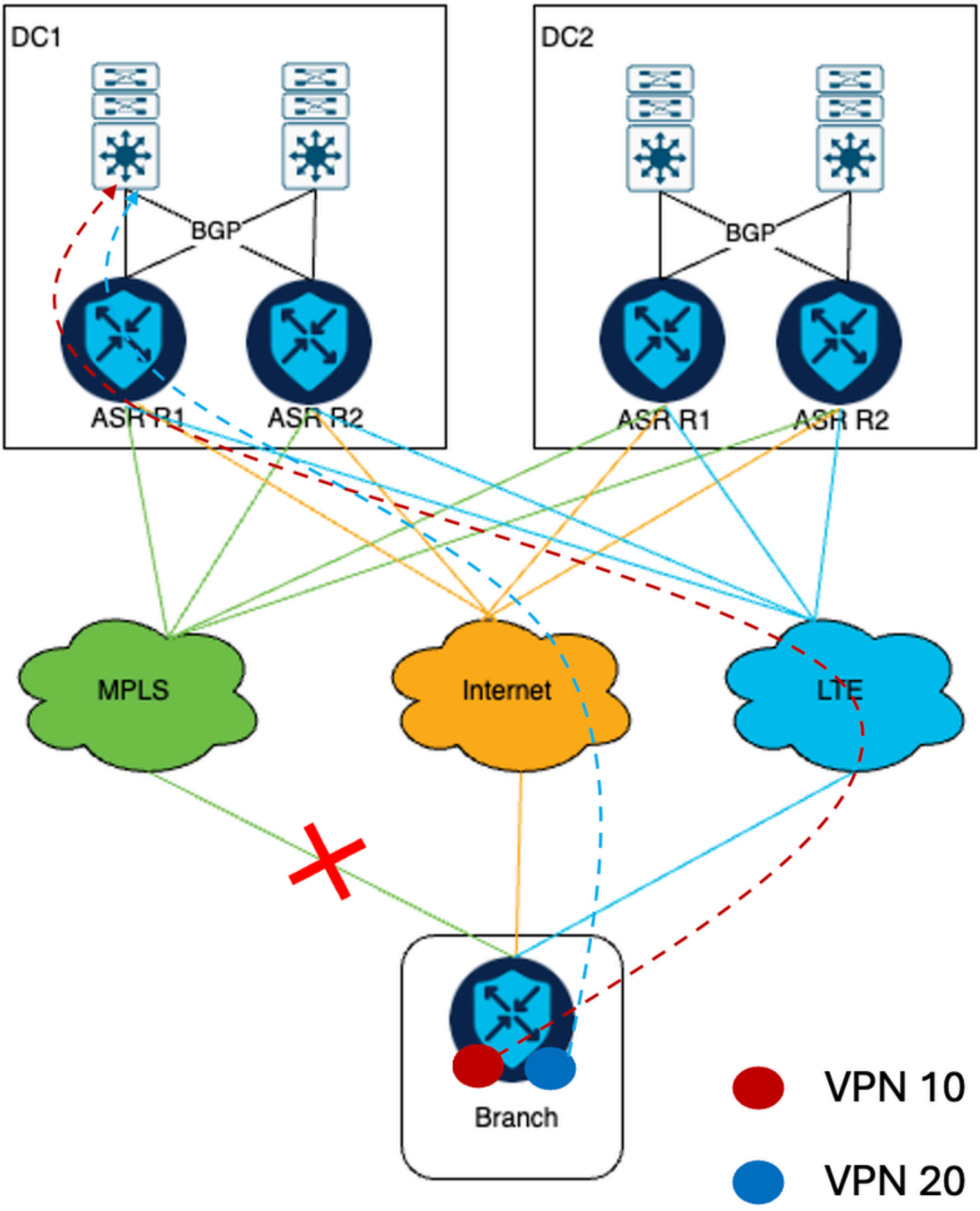
注：ハブアンドスポークトポロジが導入されています。DC1とDC2のcEdgeはハブです。すべてのリモートブランチは、DC cEdgeを使用して3つの利用可能なトランスポート上でIPsecトンネルを形成します。

ネットワークダイアグラムの終了

VPN 10およびVPN 20からのトラフィックはすべて、MPLSトランスポートを通ります。



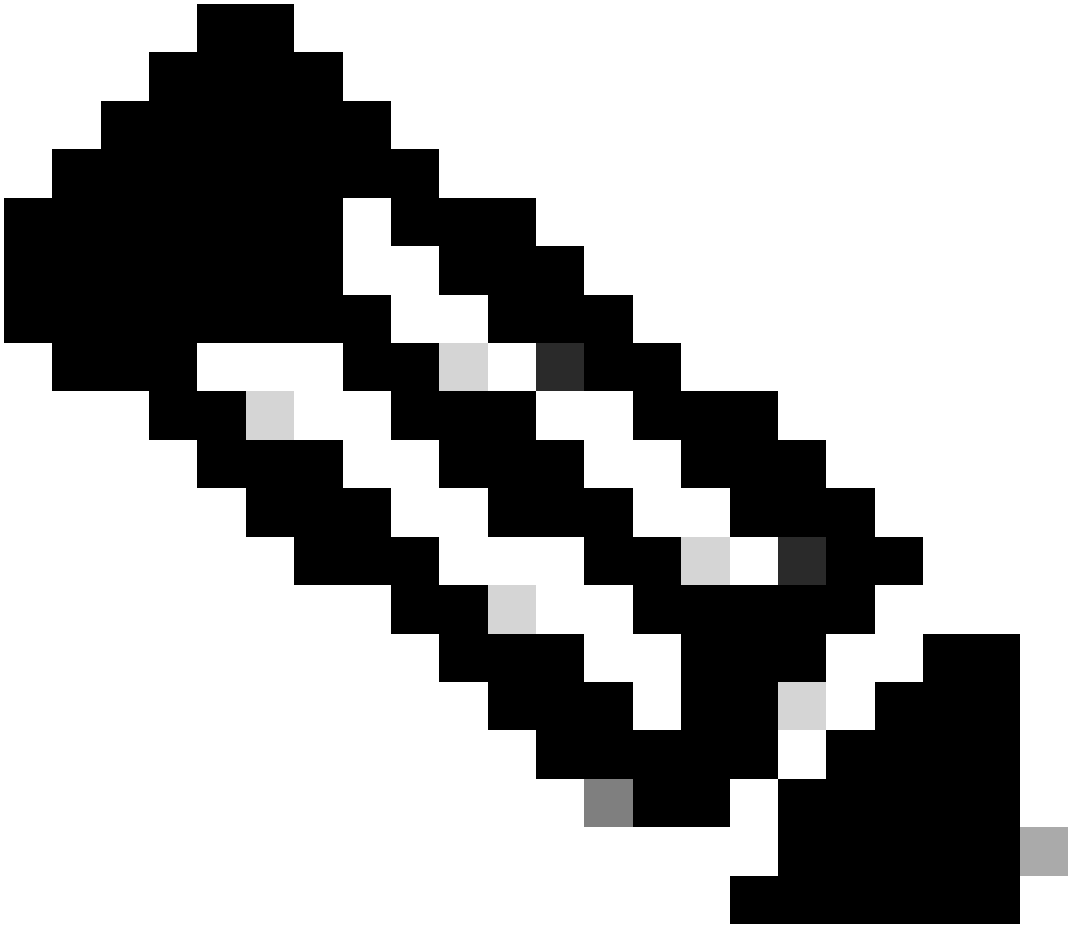
MPLSリンクがダウンすると、VPN 10トラフィックはLTEトランスポートに、VPN 20トラフィックはインターネットトランスポートに移行します。



このシナリオの技術的な課題は、お客様のネットワーク展開の規模と固有の要件から生じます。3種類の転送を通じてIPSecトンネルを確立する3000台のSD-WANルータをデータセンタールータに導入することを考慮すると、ASR1002-HXプライマリヘッドエンドルータで形成されるIPSecトンネルの総数は9000になります。ただし、ASR1002-HXのIPSecトンネル数は8,000に制限されています(出典：ASR1K Datasheet)。

解決方法

この問題を解決するため、お客様は将来の拡張性要件に応じて、各DCにISR4451-X cEdgeデバイスを追加することを決定しました。

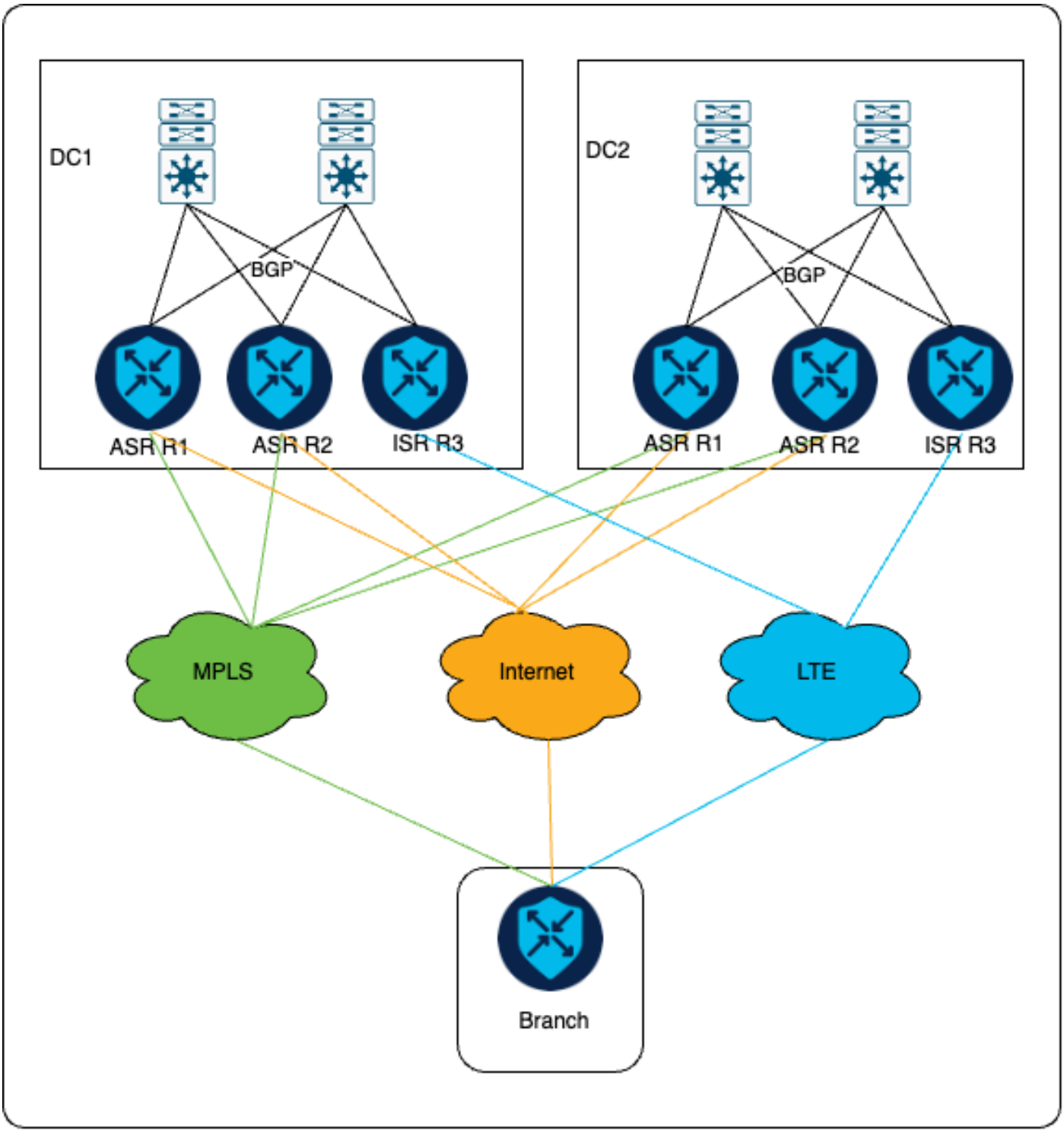


注：お客様の拡張性要件に基づいて、追加のデバイスモデルを決定します。

Network Topology

このソリューションの一部として、プライマリのアグリゲーションサービスルータ(ASR)cEdgeは引き続きMPLSおよびインターネット転送を介したIPSecトンネルを形成しますが、新しくインストールされたサービス統合型ルータ(ISR)cEdgeはLTE転送のみを介したIPsecトンネルを形成します。

図に示すように、IPSecトンネルはASRヘッドエンドとブランチの間でMPLSとインターネットを介して確立されるのに対し、ISRとブランチの間ではLTEを介してのみ確立されます。



顧客の要件は、通常の状況では、すべてのVPN 10およびVPN 20トラフィックが通信にMPLSトランスポートを使用することです。ただし、MPLSリンクに障害が発生した場合、VPN 20トラフィックはインターネットトランスポートを介して再ルーティングされますが、VPN 10トラフィックはLTEトランスポートを介してリダイレクトされ、cEdgeを追加する前と同じ動作になります。

設定

中央集中型およびローカライズされたポリシーは、お客様の好みに応じた正しいトランスポートを介してトラフィックが送信されるようにするために使用されます。インターネットリンクおよびLTEリンクを経由してブランチロケーションから着信するトラフィックには、タグが付けられ

ます。これらのタグは、ヘッドエンドのLANスイッチがVPN 10の応答メッセージをISRルータに正しく送信し、VPN 20トラフィックがASRヘッドエンドデバイスに送信されるようにするために使用されます。

一元化されたポリシー設定

これは、お客様の要件を満たすために作成されたポリシーです。インターネットリンク経由で着信するトラフィックには、200のOMPタグが割り当てられます。一方、LTEリンク経由で着信するトラフィックには、100のOMPタグが割り当てられます。

<#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>
```

DCでは、SD-WANルータからコアスイッチにトラフィックを転送する際に、LAN側でルートをBGPにアドバタイズするときにAS-PATHフィールドが操作されます。ルートマップは、BGPでのOMPルートの再配布時にBGP設定に適用されます。

MPLSリンクが動作している場合、LTE経由でトラフィックを受信しないため、プライマリcEdgeだけがBGPでルートを再配布します。ただし、MPLSリンクに障害が発生した場合は、次の手順を実行します。

- VPN 10の場合、ASR cEdgeはAS-PATHフィールドを4回追加してルートを再配布し、ISR cEdgeはAS-PATHフィールドを3回追加してルートを再配布します。この設定により、応答の送信にISR cEdgeが優先されるようになります。
- 同様に、VPN 20の場合、ASR cEdgeはAS-PATHを追加せずにプレフィックスを再配布し、

ISR cEdgeはAS-PATHフィールドを3回追加してプレフィックスを再配布します。これにより、ASR cEdgeが優先されます。

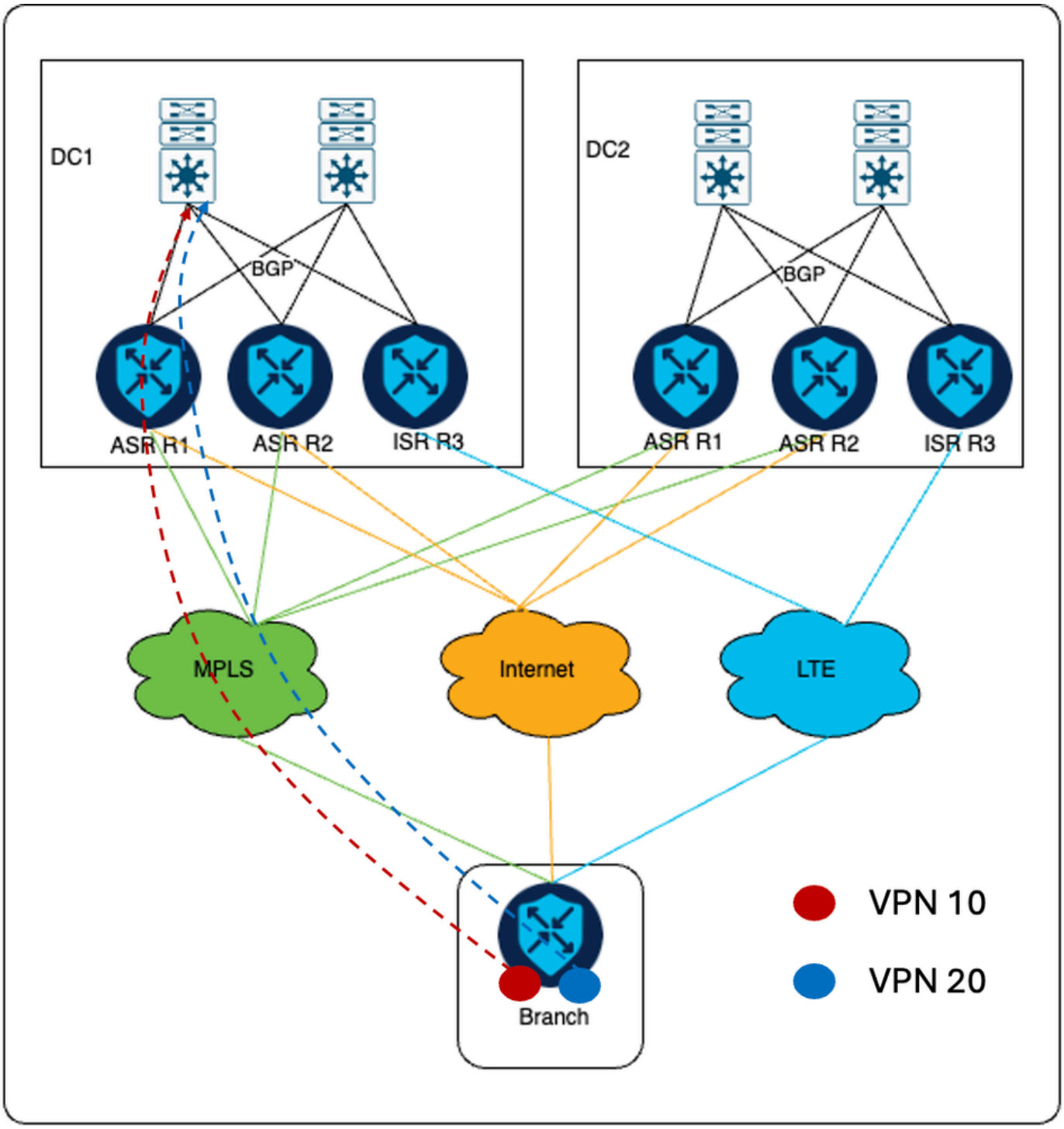
ローカライズされたポリシー設定

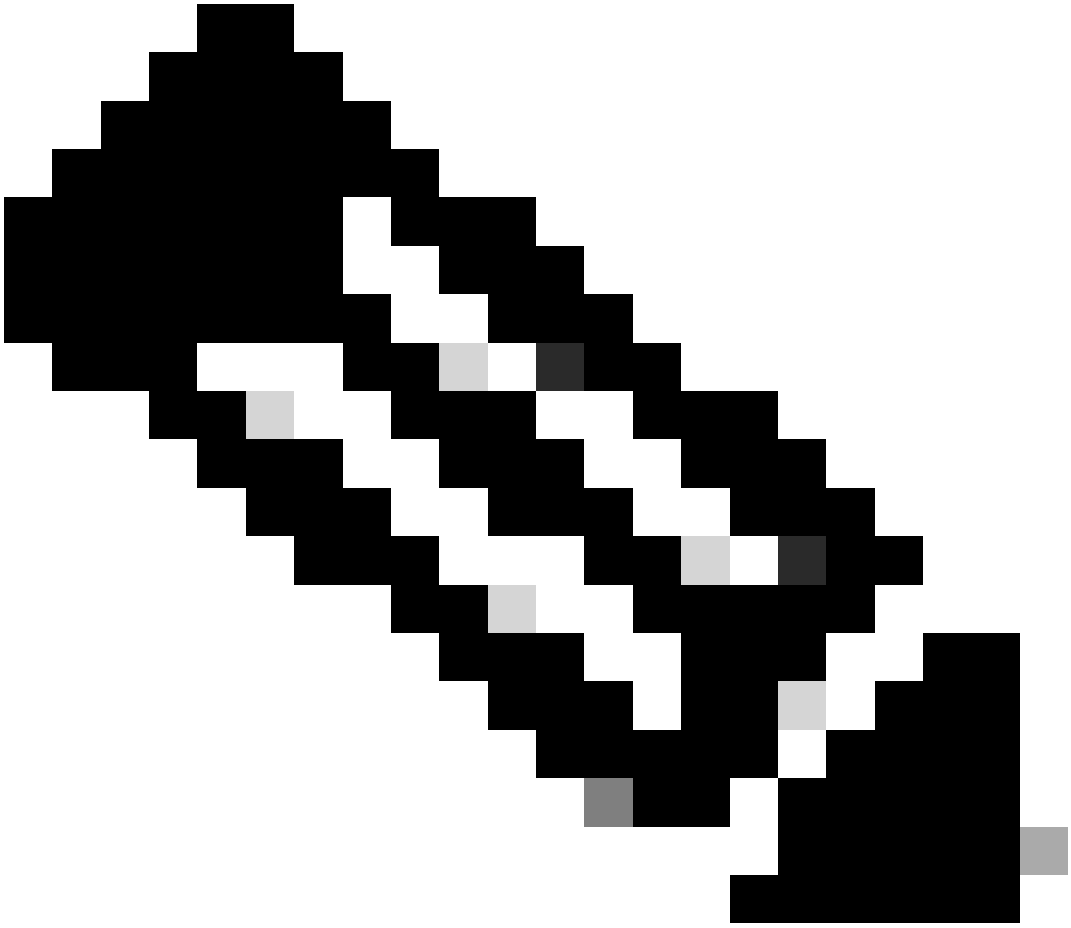
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

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

通常のシナリオ

MPLSリンクがアップ状態になると、VPN 10とVPN 20からのすべてのトラフィックはMPLSトランスポートを通過します。

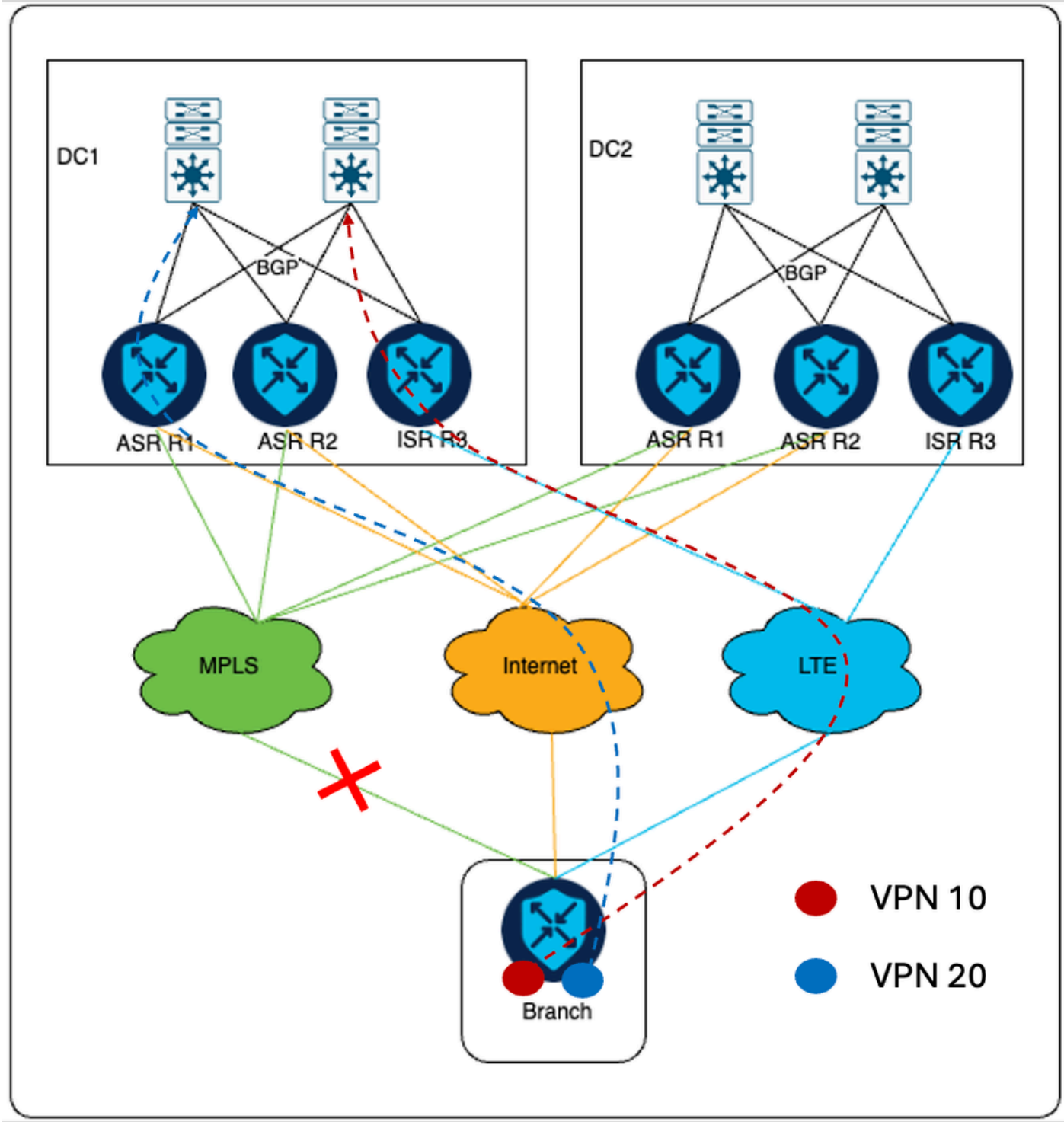

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



注:DC1はプライマリDCです。

フェールオーバーシナリオ

MPLSリンクに障害が発生した場合、VPN 10トラフィックはISR cEdgeに向かうLTE転送を介して通過します。ここで、VPN 20トラフィックはインターネットトランスポート経由でASR cEdgeデバイスに送信されます。



コアスイッチからのリターントラフィックの場合、VPN 10トラフィックはISR cEdgeに送信されます。これは、ローカライズされたポリシーセクションで指定されているように、AS-PATHの長さがASRよりもISR経由で短いためです。同様に、VPN 20トラフィックはASR cEdgeに向けて送信されます。これは、AS-PATHがISRと比較してASR経由で小さいためです。

追加情報

以前の設定では、各DCのすべてのcEdgeは、インターネット転送を介してのみSD-WANコントローラに接続されます。したがって、ISRルータにはインターネットトンネルが設定されています。要件は、ISR cEdgeがLTE転送を介してのみリモートブランチへのIPsecトンネルを形成するよ

うにすることです。この要件を満たすには、ISRのインターネットトランスポート上のトンネルカラーを、顧客の設定で使用されていないパブリックカラーで設定する必要があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。