Numero di indirizzi del limite del tunnel Data Plane nel data center

Sommario

Introduzione

Questo documento descrive una soluzione per risolvere i problemi di scalabilità nei bordi SD-WAN dei centri dati quando si avvicinano ai limiti del tunnel del piano dati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di SD-WAN.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SD-WAN Controller versione 20.6.3.0.54 (ES)
- Cisco IOS® XE (esecuzione in modalità controller) 17.06.03a.0.2 (ES)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

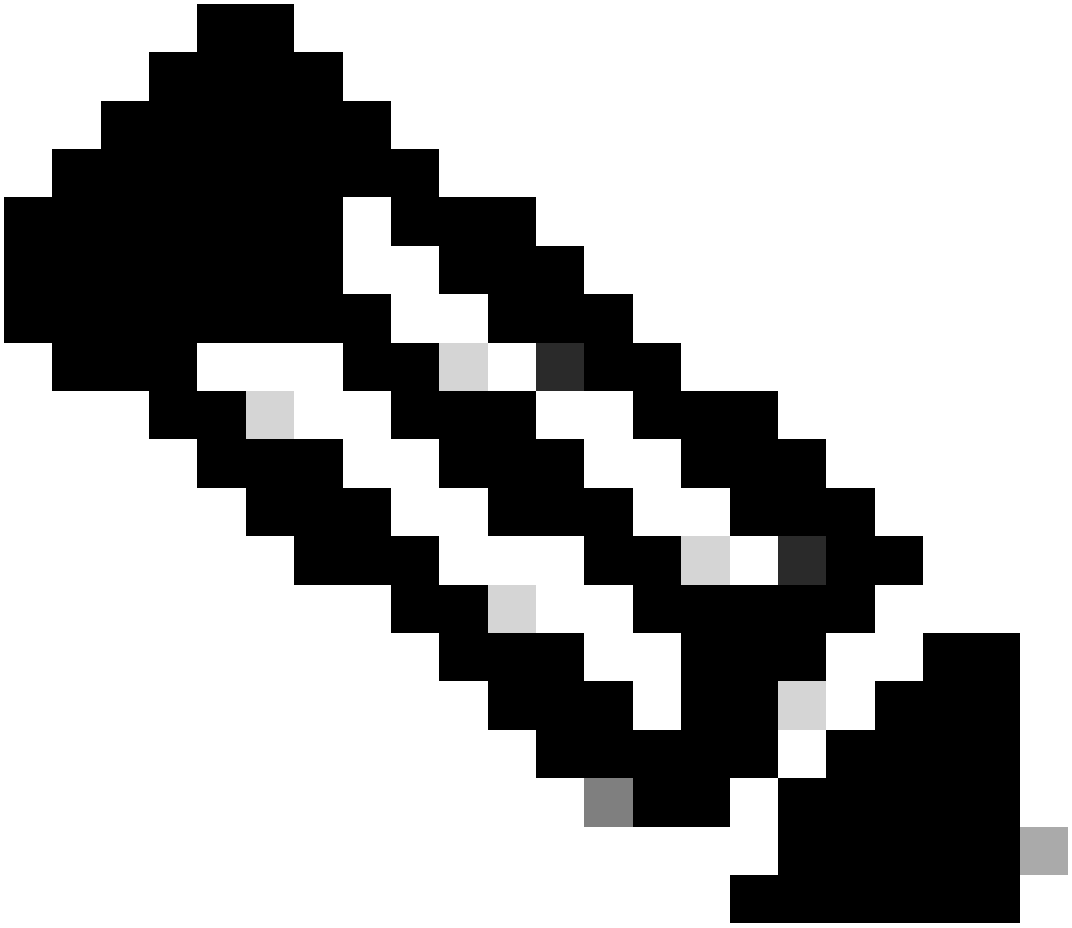
Premesse

Panoramica della progettazione della rete:

- VPN: VPN 10, VPN 20
- Collegamenti di trasporto: Multiprotocol Label Switching (MPLS), LTE, Internet
- Dettagli router:
    - Router principale: 2 in ogni centro dati
      - Modello: ASR1002-HX
      - Software Cisco IOS XE versione: 17.06.03a.0.2
    - Router secondario: 1 in ogni centro dati
      - Modello ISR4451-X
      - Software Cisco IOS XE versione: 17.06.03a.0.2
- Protocollo di routing: Border Gateway Protocol (BGP) viene utilizzato sul lato LAN del data center

Problema

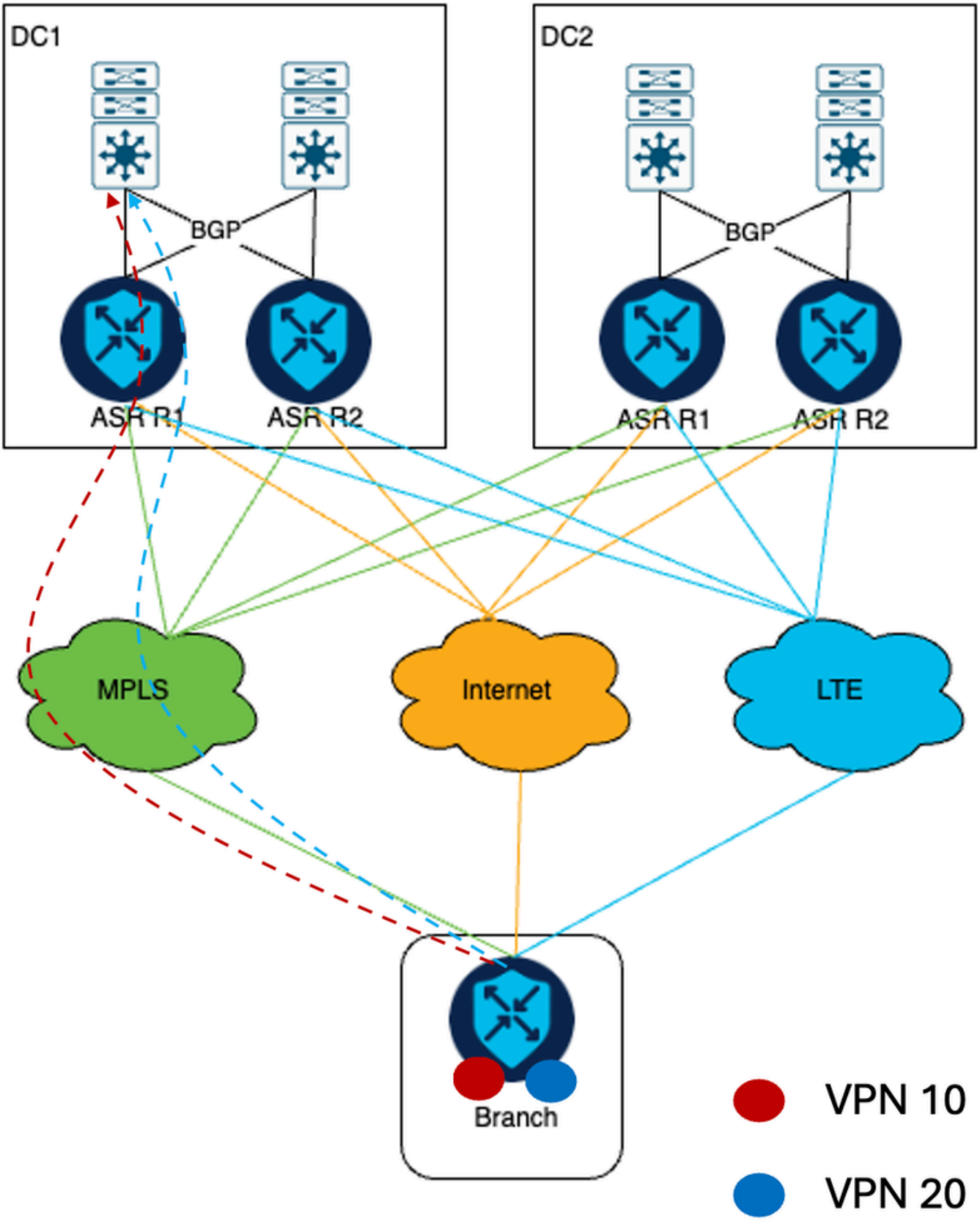
In questo documento viene illustrato il caso di studio del cliente, con la topologia mostrata, l'infrastruttura di rete del cliente comprende due centri dati, ciascuno con due ASR1002-HX SD-WAN cEdge installati. Questa architettura di rete intende incorporare circa 3000 punti vendita nella sovrapposizione SD-WAN, sfruttando la disponibilità di tre distinti collegamenti di trasporto.



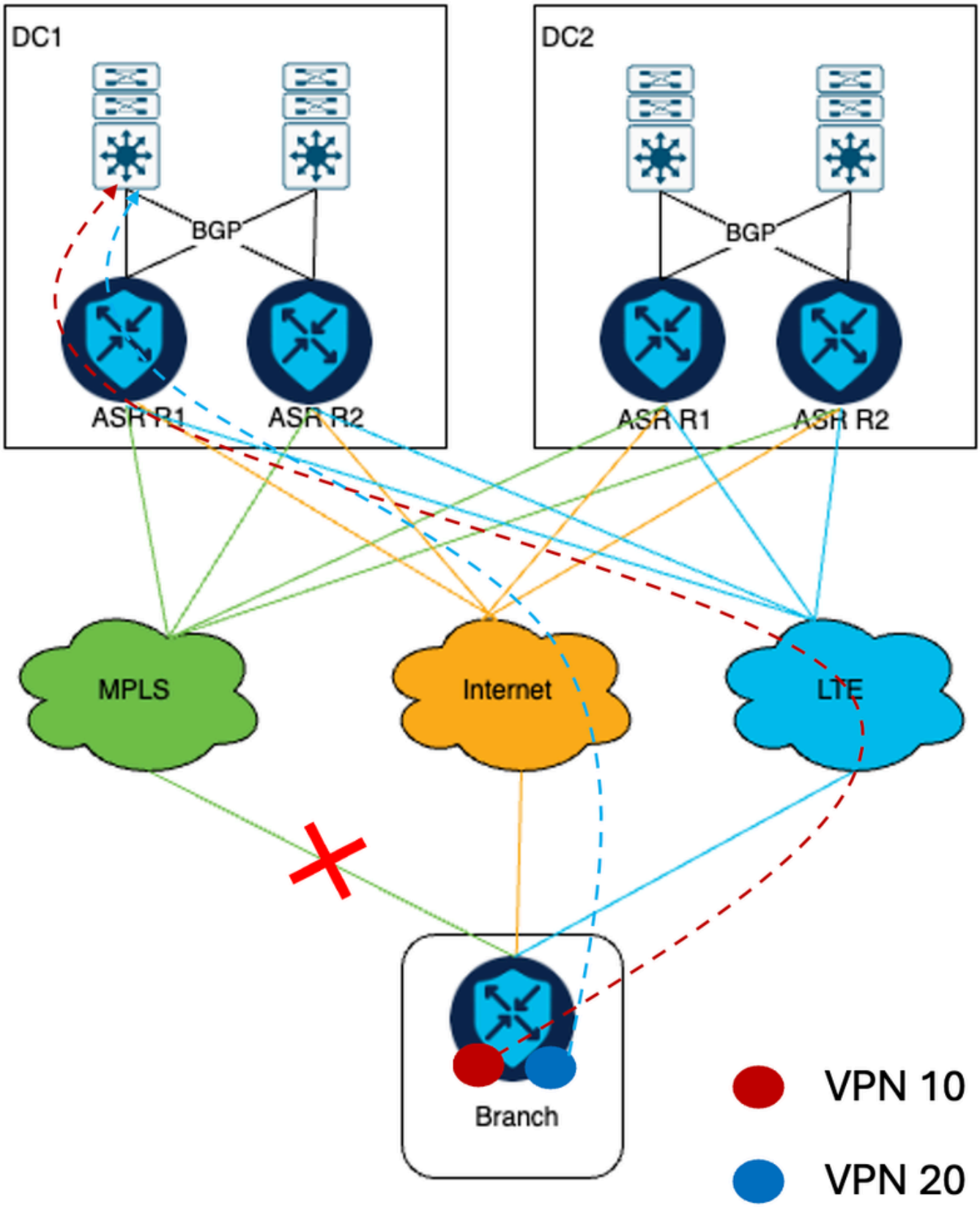
Nota: la topologia Hub e Spoke è distribuita. Gli spigoli DC1 e DC2 sono hub. Tutte le diramazioni remote formano tunnel IPsec su tre trasporti disponibili con bordi CC.

Uscita da diagramma reticolare

Tutto il traffico proveniente dalla VPN 10 e dalla VPN 20 attraversa il trasporto MPLS.



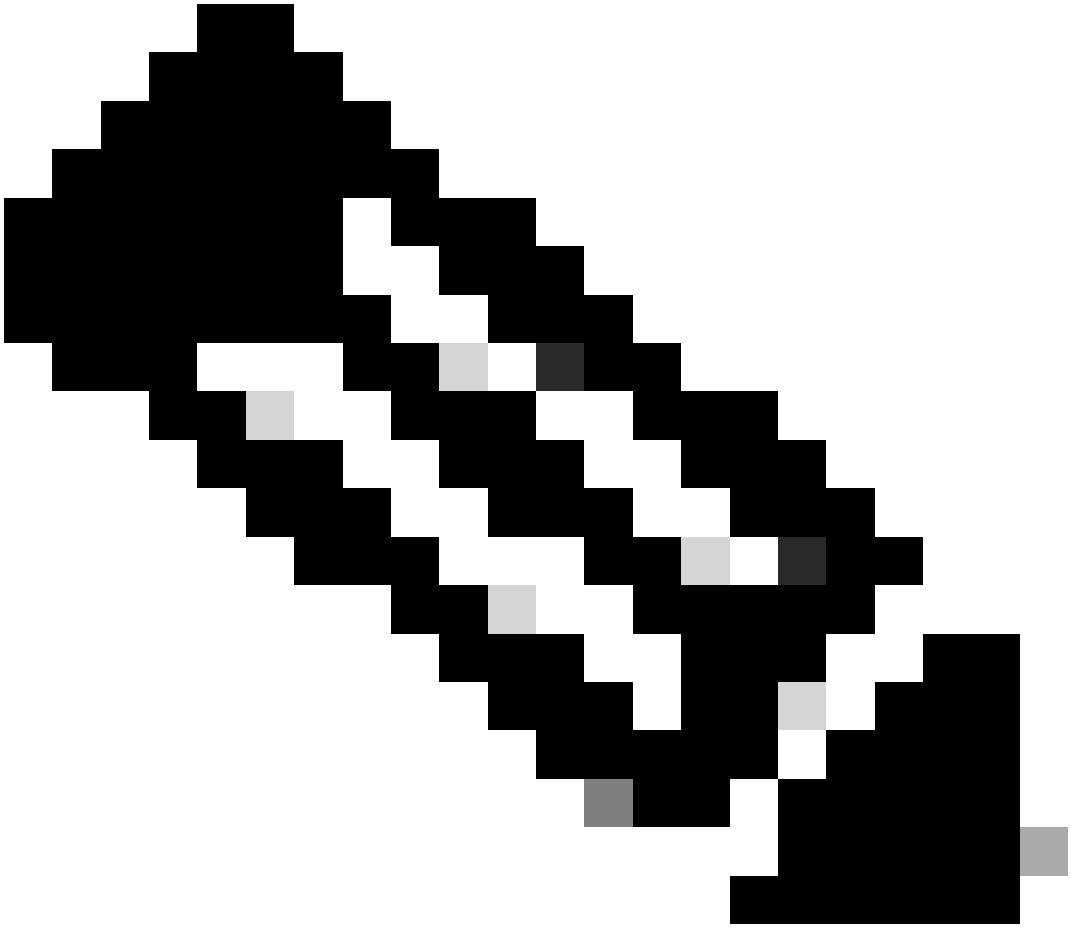
Se il collegamento MPLS si interrompe, il traffico VPN 10 si sposta sul trasporto LTE e il traffico VPN 20 si sposta sul trasporto Internet.



La sfida tecnica in questo scenario deriva dalla scala e dai requisiti specifici di un'installazione di rete dei clienti. Considerando l'implementazione di 3000 router SD-WAN che stabiliscono tunnel IPSec tramite tre tipi di trasporto al router del data center, il numero totale di tunnel IPSec formati sui router headend principali ASR1002-HX raggiunge 9000. Tuttavia, ASR1002-HX è limitato a 8000 tunnel IPSec (fonte: ASR1K Datasheet).

Soluzione

Per risolvere questo problema, il cliente ha deciso di aggiungere un dispositivo ISR4451-X cEdge in ogni controller di dominio in base ai futuri requisiti di scalabilità del cliente.



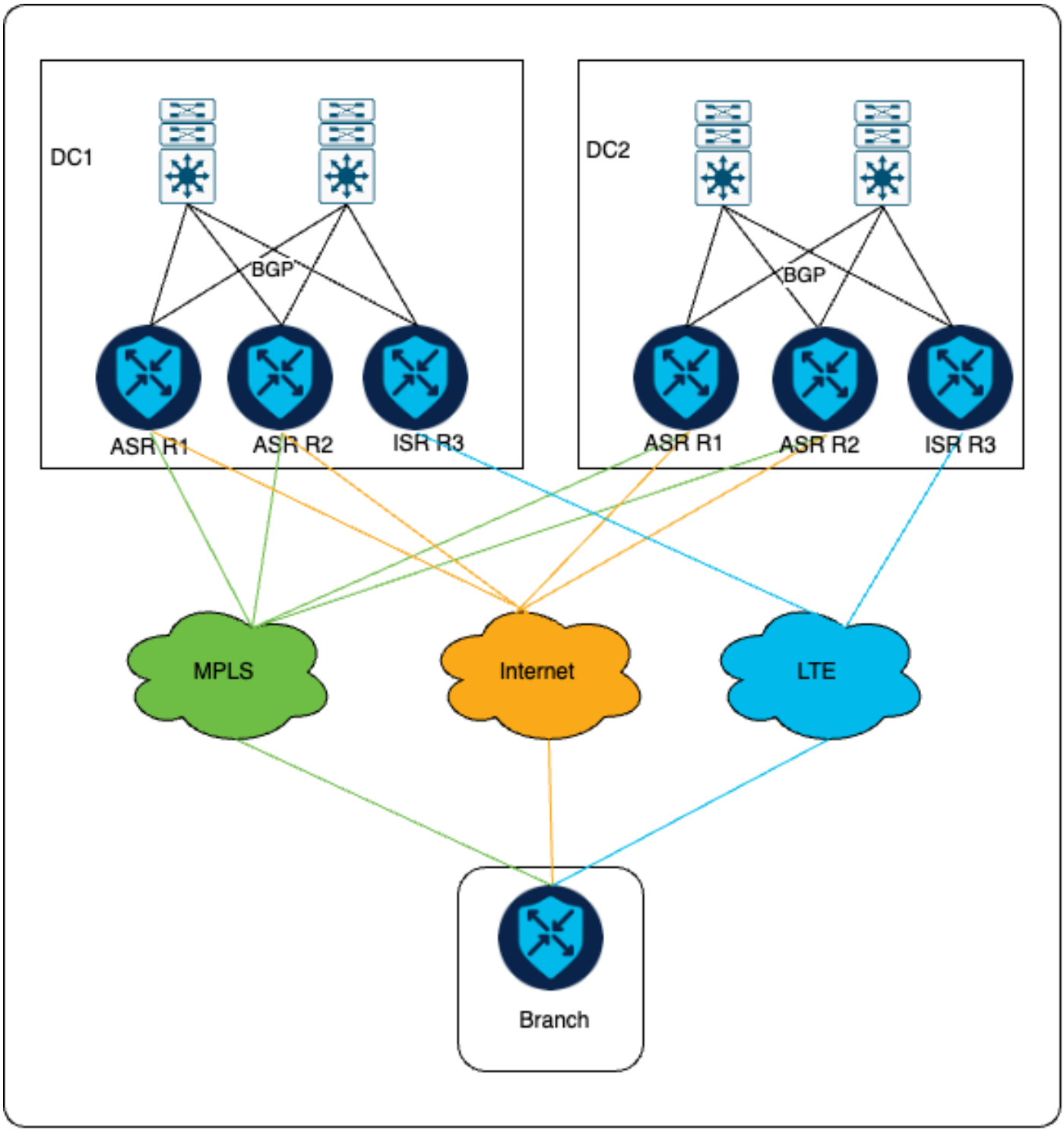
> Nota: scegliere un modello di dispositivo aggiuntivo in base ai requisiti di scalabilità del cliente.

Topologia della rete

Come parte della soluzione, gli spigoli ASR (Aggregation Services Router) primari continuano a formare un tunnel IPSec su MPLS e trasporto Internet, mentre i nuovi spigoli ISR (Integrated Service Router) installati formano un tunnel IPsec solo tramite trasporto LTE.

Come mostrato nel diagramma, i tunnel IPSec vengono stabiliti tra l'headend ASR e la succursale tramite MPLS e Internet, mentre tra l'ISR e la succursale, i tunnel IPSec vengono stabiliti solo

tramite LTE.



Il requisito del cliente è che, in circostanze normali, tutto il traffico VPN 10 e VPN 20 utilizzi il trasporto MPLS per la comunicazione. Tuttavia, in caso di errore di un collegamento MPLS, il traffico VPN 20 viene reindirizzato tramite il trasporto Internet, mentre il traffico VPN 10 viene reindirizzato tramite il trasporto LTE, come prima di aggiungere altri cEdge.

Configurazione

Per garantire l'invio del traffico attraverso il trasporto corretto in base alle preferenze del cliente, vengono utilizzate policy centralizzate e localizzate. Il traffico in entrata dalla succursale attraverso

il collegamento Internet e il collegamento LTE è contrassegnato. Questi tag vengono usati per garantire che gli switch LAN sull'headend inviino correttamente messaggi di risposta per VPN 10 al router ISR e che il traffico VPN 20 venga inviato ai dispositivi headend ASR.

Configurazione dei criteri centralizzata

Ecco la politica preparata per soddisfare le esigenze del cliente. Per il traffico in arrivo tramite collegamento Internet, viene assegnato un tag OMP di 200. Al traffico che arriva attraverso il collegamento LTE viene invece assegnato un tag OMP di 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>
```

Alla DC, durante l'inoltro del traffico dai router SD-WAN agli switch core, il campo AS-PATH viene manipolato quando si annuncia il percorso in BGP sul lato LAN. Una mappa delle route viene applicata nella configurazione BGP al momento della ridistribuzione delle route OMP in BGP.

Quando il collegamento MPLS è operativo, solo i bordi primari ridistribuiscono le route in BGP poiché non viene ricevuto alcun traffico tramite LTE. Tuttavia, in caso di errore del collegamento MPLS:

- Per la VPN 10, ASR Edge ridistribuisce le route aggiungendo il campo AS-PATH quattro volte, mentre ISR cEdge ridistribuisce aggiungendo il campo AS-PATH tre volte. Questa configurazione garantisce che l'ISR cEdge sia preferito per l'invio delle risposte.
- Analogamente, per VPN 20, ASR Edge ridistribuisce i prefissi senza aggiungere alcun AS-

PATH e ISR cEdge ridistribuisce i prefissi aggiungendo il campo AS-PATH tre volte. In questo modo si assicura che gli spigoli ASR siano preferiti.

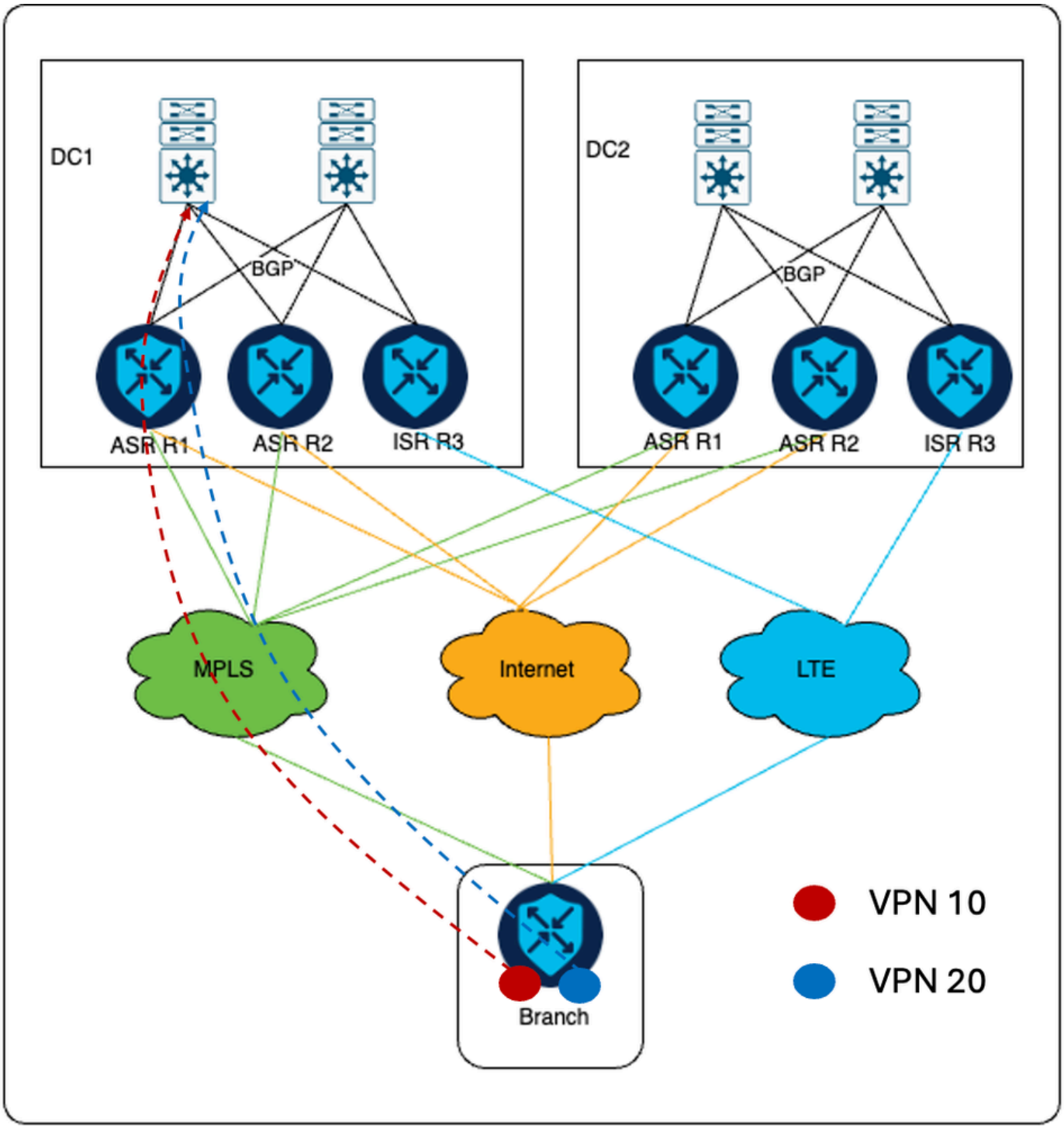
Configurazione criteri localizzati

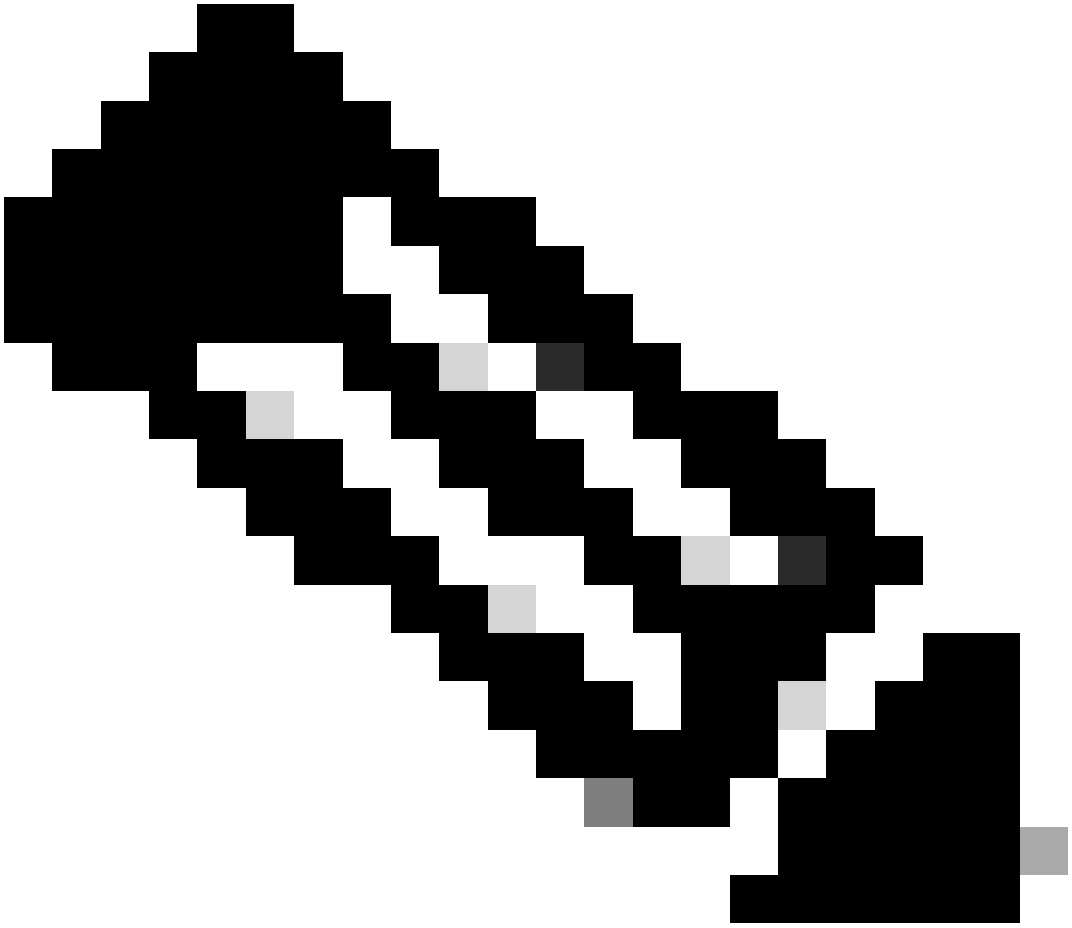
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

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
```

Flusso traffico

Scenario normale

Quando il collegamento MPLS è attivo, tutto il traffico proveniente dalla VPN 10 e dalla VPN 20 attraversa il trasporto MPLS.

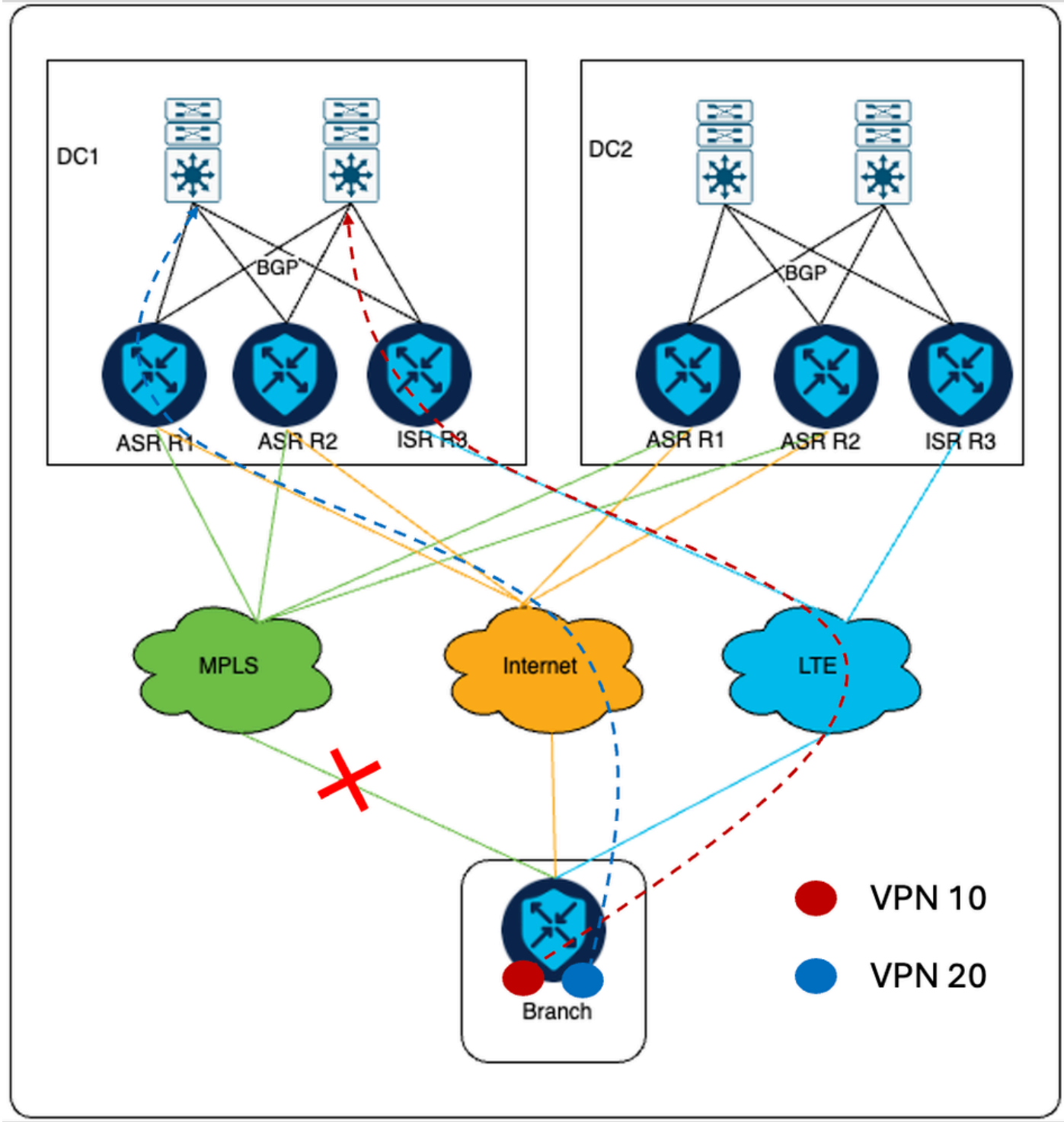

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



Nota: CD1 è il controller di dominio primario.

Scenario di failover

In caso di errore del collegamento MPLS, il traffico VPN 10 attraversa il trasporto LTE verso ISR cEdge. Dove il traffico VPN 20 viene inviato tramite trasporto Internet al dispositivo ASR cEdge.



Per il traffico di ritorno dagli switch principali, per il traffico VPN 10 viene inviato all'ISR cEdge perché la lunghezza di AS-PATH è inferiore tramite ISR rispetto all'ASR come specificato nella sezione dei criteri localizzati. Analogamente, il traffico VPN 20 viene inviato verso gli spigoli ASR in quanto AS-PATH è più piccolo tramite ASR rispetto a ISR.

Ulteriori informazioni

Nella configurazione precedente, tutti gli spigoli di ciascun DC sono collegati ai controller SD-WAN solo tramite trasporto via Internet. Di conseguenza, i router ISR dispongono di un tunnel Internet configurato. Il requisito è quello di garantire che ISR cEdge formi un tunnel IPsec per le filiali

remote solo tramite trasporto LTE e per raggiungere il requisito specificato, il colore del tunnel sul trasporto Internet di ISR deve essere configurato con un colore pubblico non utilizzato nella configurazione del cliente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).