Adressenanzahl des Tunnellimits für die Datenebene im Rechenzentrum

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Problem
  - Netzwerkdiagramm beenden
- Lösung
  - Netzwerktopologie
  - Konfigurieren
    - Zentrale Richtlinienkonfiguration
    - Lokalisierte Richtlinienkonfiguration
  - Datenverkehrsfluss
    - Normales Szenario
    - Failover-Szenario
- Zusätzliche Informationen

Einleitung

In diesem Dokument wird eine Lösung zur Behebung von Skalierungsproblemen bei SD-WAN-Edges im Rechenzentrum in der Nähe der Tunnelgrenzwerte für die Datenebene beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie Kenntnisse über SD-WAN haben.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- SD-WAN-Controller Version 20.6.3.0.54 (ES)
- Cisco IOS® XE (im Controllermodus) 17.06.03a.0.2 (ES)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

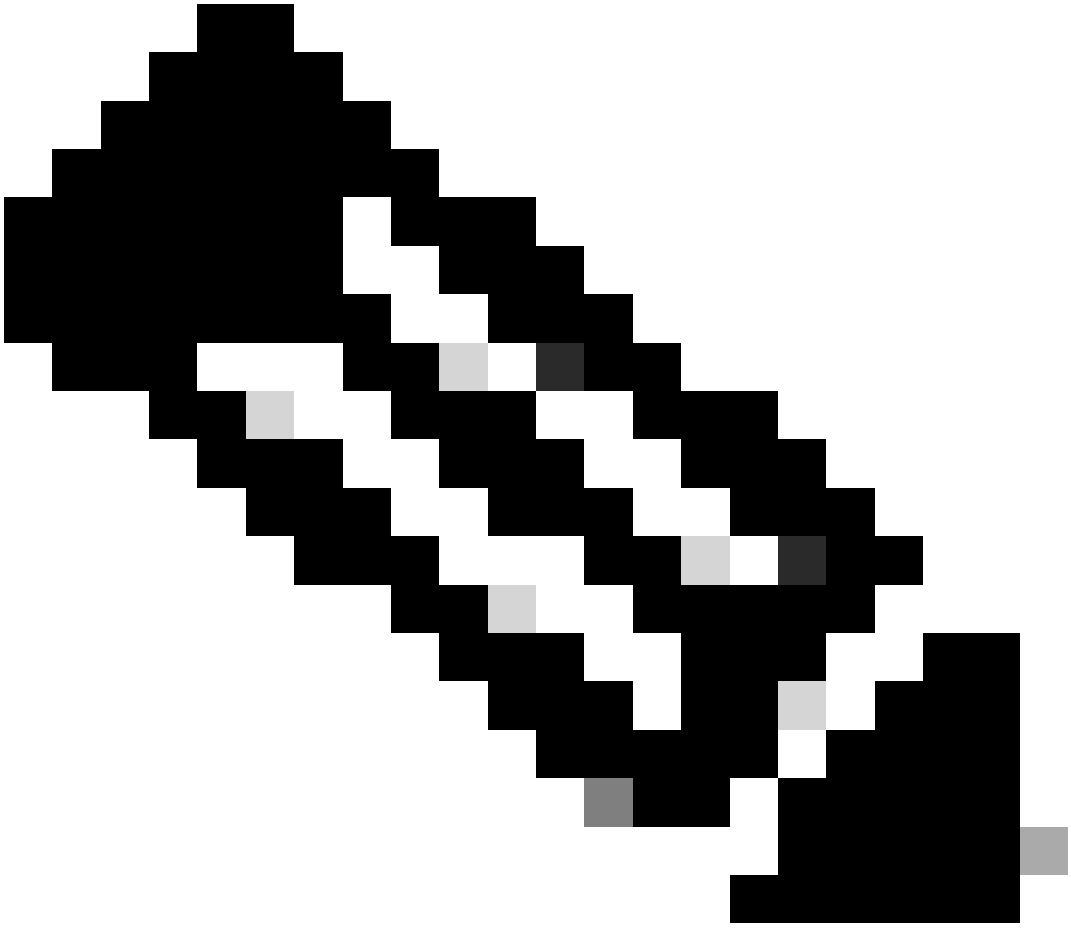
Hintergrundinformationen

Überblick über das Netzwerkdesign:

- VPN: VPN 10, VPN 20
- Transportverbindungen: Multiprotocol Label Switching (MPLS), LTE, Internet
- Router-Details:
  - Primärer Router: 2 in jedem Rechenzentrum
    - Modell: ASR1002-HX
    - Cisco IOS XE Softwareversion: 17.06.03a.0.2
  - Sekundärer Router: 1 in jedem Rechenzentrum
    - Modell: ISR4451-X
    - Cisco IOS XE Softwareversion: 17.06.03a.0.22
- Routing-Protokoll: Auf der LAN-Seite des Rechenzentrums wird Border Gateway Protocol (BGP) verwendet.

Problem

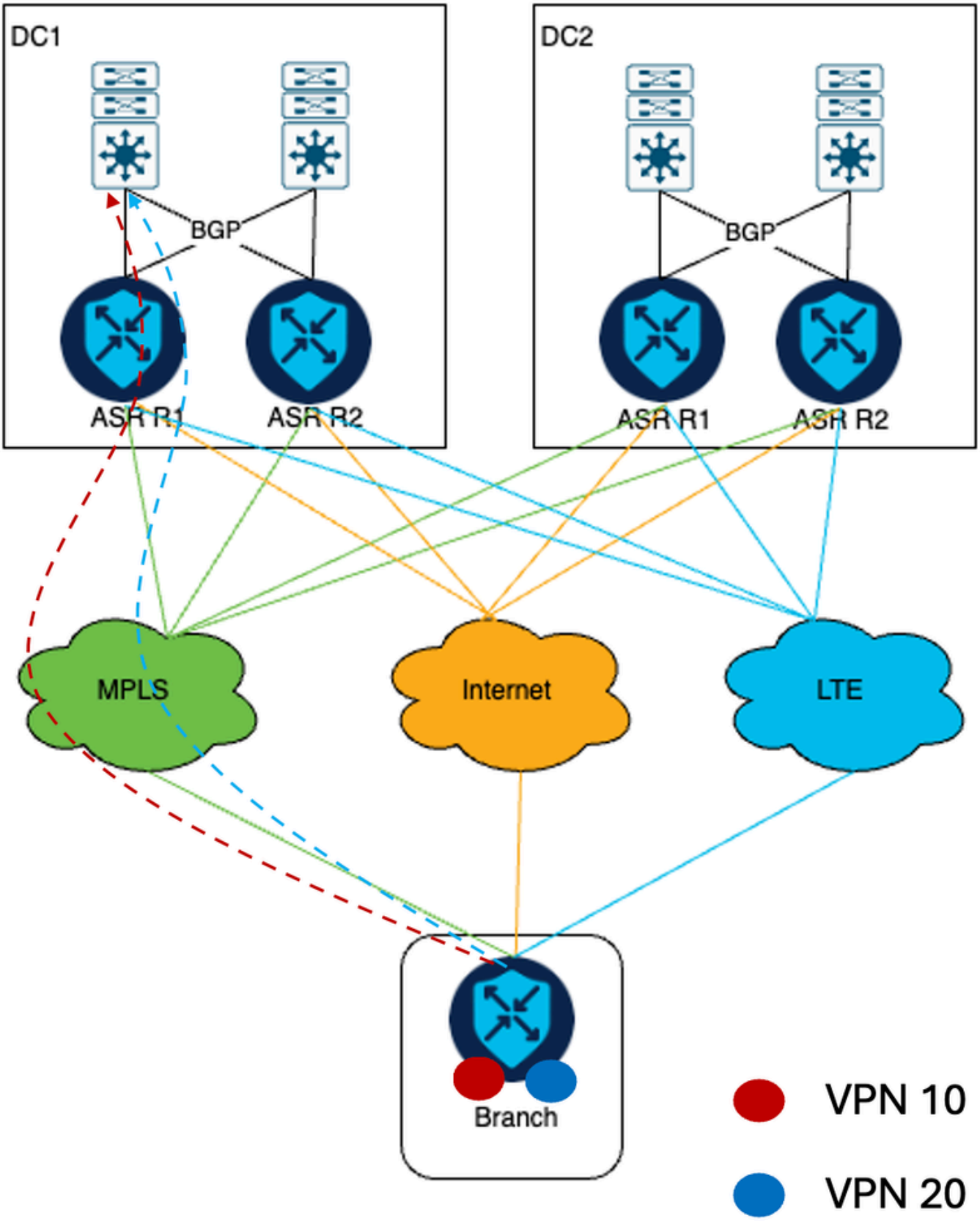
In diesem Dokument wird der Kundenfallbericht mit der gezeigten Topologie erörtert. Die Netzwerkinfrastruktur des Kunden besteht aus zwei Rechenzentren mit jeweils zwei bereitgestellten ASR1002-HX SD-WAN cEdge. Ziel dieser Netzwerkarchitektur ist es, ca. 3.000 Filialstandorte in das SD-WAN-Overlay zu integrieren und die Verfügbarkeit von drei verschiedenen Transportverbindungen zu nutzen.



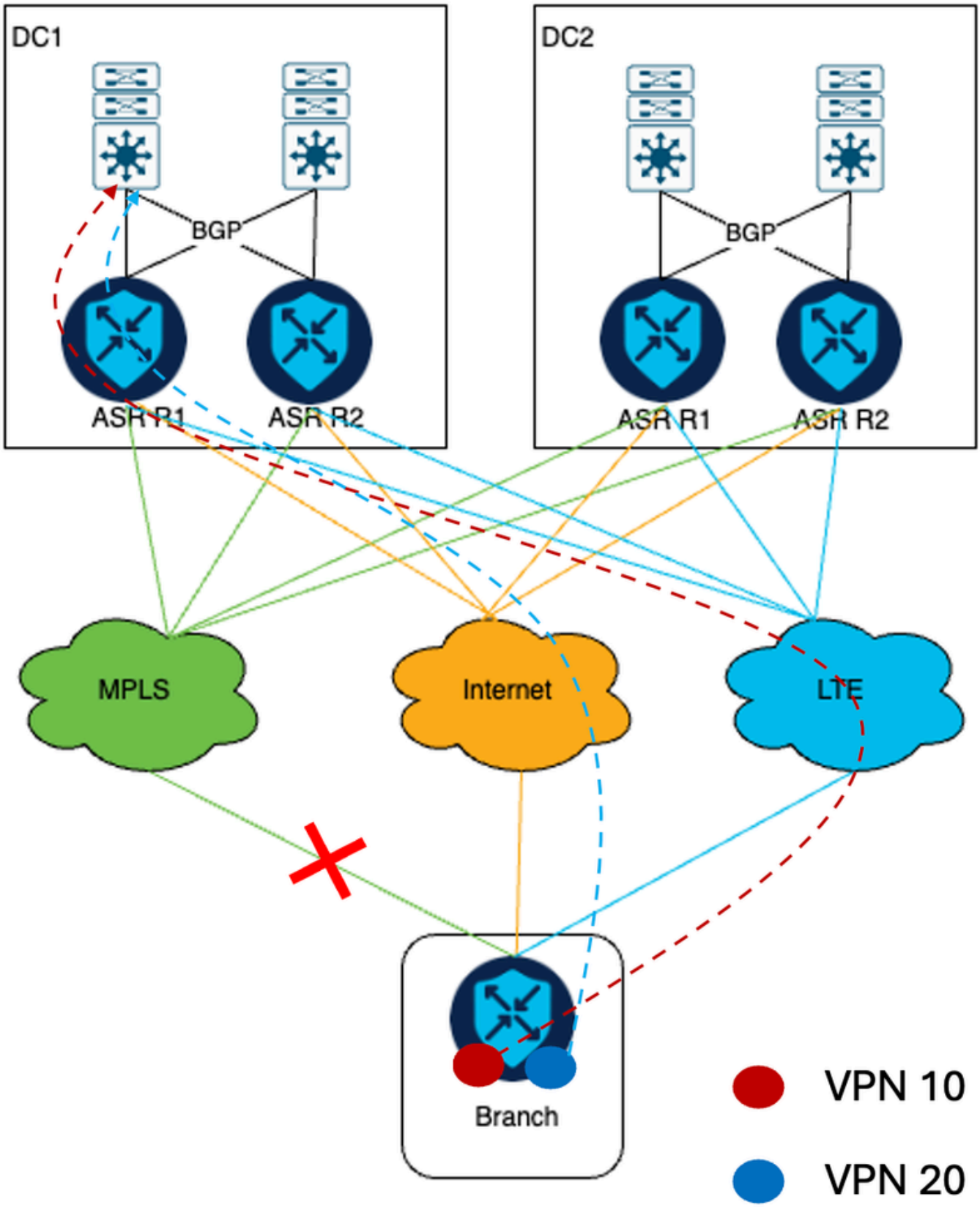
Hinweis: Hub-and-Spoke-Topologie wird bereitgestellt. DC1- und DC2-Edges sind Hubs. Alle Remote-Zweigstellen bilden IPsec-Tunnel über drei verfügbare Transportstrecken mit DC-Edges.

Netzwerkdiagramm beenden

Der gesamte Datenverkehr von VPN 10 und VPN 20 durchläuft den MPLS-Transport.



Wenn die MPLS-Verbindung ausfällt, wird der VPN 10-Datenverkehr zum LTE-Datenverkehr und der VPN 20-Datenverkehr zum Internetdatenverkehr.

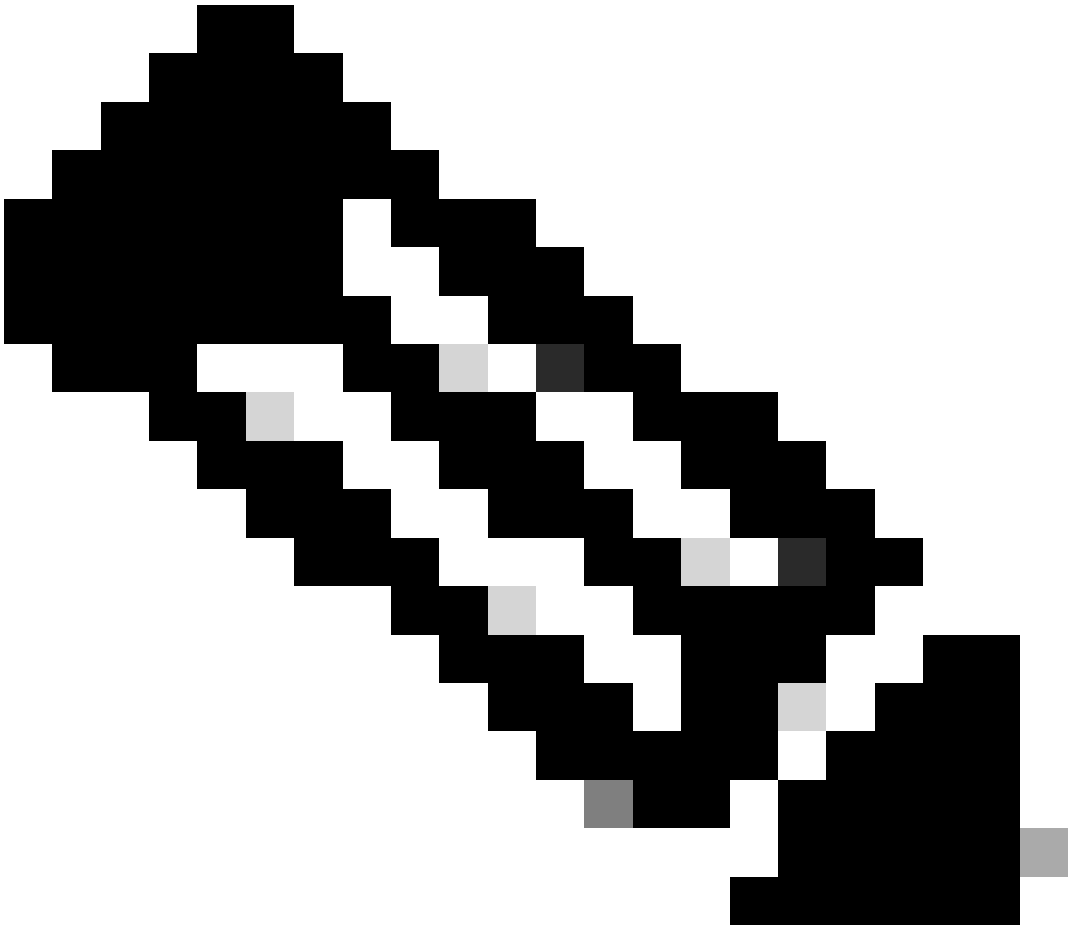


Die technische Herausforderung in diesem Szenario ergibt sich aus dem Umfang und den spezifischen Anforderungen einer Netzwerkbereitstellung der Kunden. Bei einer Bereitstellung von 3.000 SD-WAN-Routern, die IPSec-Tunnel über drei Transportarten zum Rechenzentrums-Router herstellen, beträgt die Gesamtzahl der IPSec-Tunnel, die auf den primären Headend-Routern ASR1002-HX gebildet werden, 9.000. Der ASR1002-HX ist jedoch auf 8000 IPSec-Tunnel

beschränkt (Quelle: ASR1K-Datenblatt).

Lösung

Um dieses Problem zu lösen, entschied sich der Kunde, in jedem Rechenzentrum ein ISR4451-X cEdge-Gerät gemäß den zukünftigen Skalierbarkeitsanforderungen des Kunden hinzuzufügen.



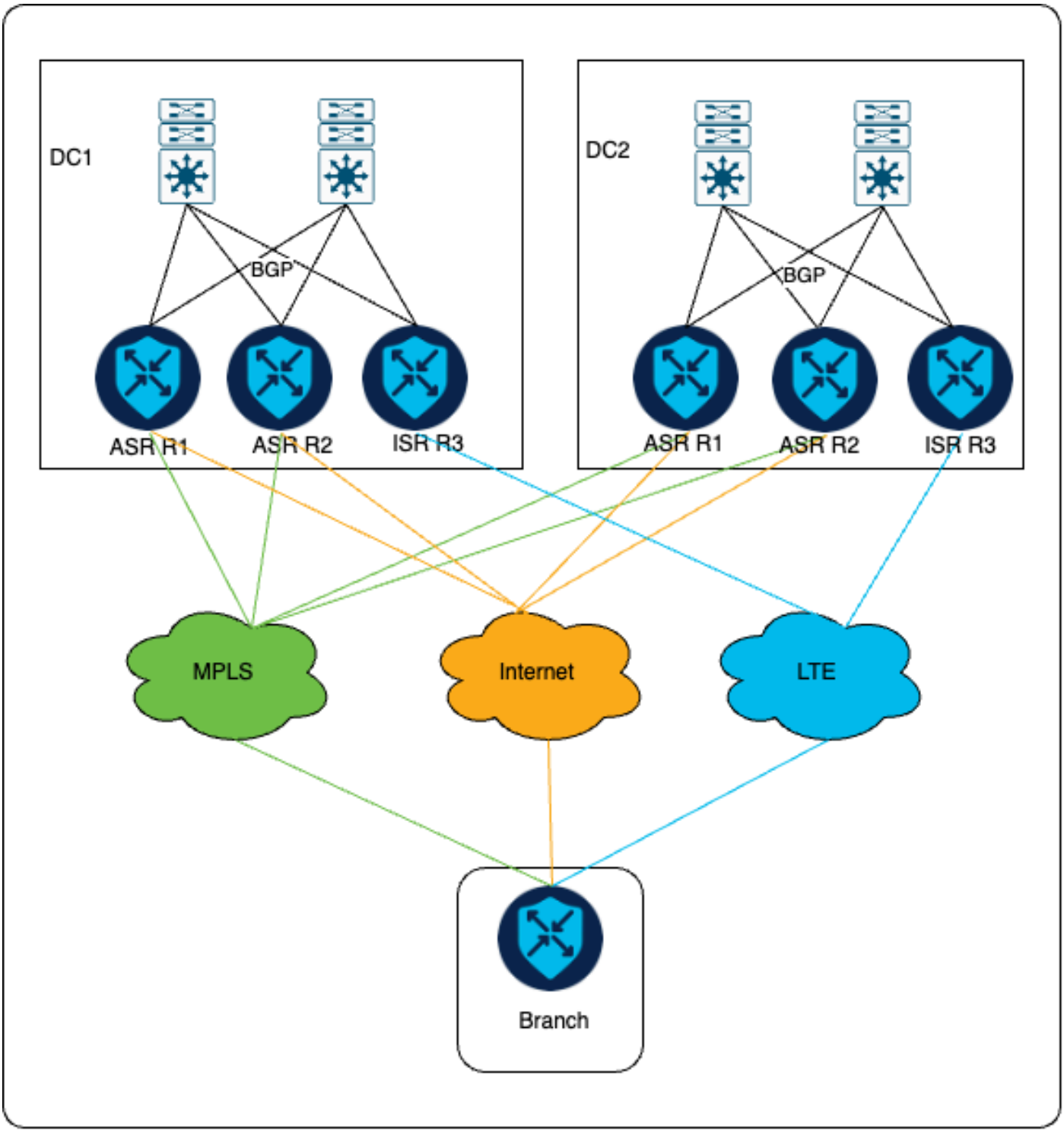
> Hinweis: Wählen Sie ein zusätzliches Gerätemodell basierend auf den Skalierbarkeitsanforderungen des Kunden aus.

Netzwerktopologie

Im Rahmen der Lösung bilden primäre Aggregation Services Router (ASR) cEdges weiterhin einen IPSec-Tunnel über MPLS und Internet-Transport, und neu installierte Integrated Service Router (ISR) cEdges bilden einen IPsec-Tunnel nur über LTE-Transport.

Wie im Diagramm dargestellt, werden IPSec-Tunnel zwischen dem ASR-Headend und der

Außenstelle über MPLS und das Internet eingerichtet, während zwischen dem ISR und der Außenstelle IPSec-Tunnel ausschließlich über LTE eingerichtet werden.



Die Kundenanforderung besteht darin, dass der gesamte VPN 10- und VPN 20-Datenverkehr unter normalen Umständen MPLS-Transport für die Kommunikation nutzt. Beim Ausfall einer MPLS-Verbindung wird der VPN 20-Datenverkehr jedoch über das Internet umgeleitet, während der VPN 10-Datenverkehr über den LTE-Transport umgeleitet wird. Dies geschieht wie vor dem Hinzufügen von zusätzlichem cEdge.

Konfigurieren

Es werden zentrale und lokalisierte Richtlinien verwendet, um sicherzustellen, dass der Datenverkehr entsprechend der Kundenpräferenz über den richtigen Transportweg gesendet wird. Datenverkehr, der über die Internetverbindung und die LTE-Verbindung von der Außenstelle eingeht, wird markiert. Diese Tags stellen sicher, dass LAN-Switches am Headend Antwortnachrichten für VPN 10 korrekt an den ISR-Router senden und dass VPN 20-Datenverkehr an ASR-Headend-Geräte gesendet wird.

Zentrale Richtlinienkonfiguration

Hier ist die Richtlinie, die ausgearbeitet wurde, um die Kundenanforderungen zu erfüllen. Für den über die Internetverbindung eingehenden Datenverkehr wird ein OMP-Tag von 200 zugewiesen. Dem über die LTE-Verbindung eingehenden Datenverkehr wird dagegen ein OMP-Tag von 100 zugewiesen.

<#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>
```

Beim Weiterleiten des Datenverkehrs von SD-WAN-Routern an Core-Switches im Rechenzentrum wird das AS-PATH-Feld manipuliert, wenn die Route LAN-seitig in das BGP übermittelt wird. Zum Zeitpunkt der Neuverteilung von OMP-Routen im BGP wird eine Routing-Map in der BGP-Konfiguration angewendet.

Wenn die MPLS-Verbindung betriebsbereit ist, verteilen nur die primären cEdges die Routen im BGP neu, da kein Datenverkehr über LTE empfangen wird. Bei Ausfall einer MPLS-Verbindung gilt jedoch Folgendes:

- Für VPN 10 verteilen die ASR-Edges Routen neu, indem sie das AS-PATH-Feld viermal anhängen, während der ISR-cEdge Routen dreimal neu verteilt, indem er das AS-PATH-Feld anhängt. Durch diese Konfiguration wird sichergestellt, dass der ISR cEdge für das Senden von Antworten bevorzugt wird.
- Ähnlich verteilen die ASR cEdges Präfixe für VPN 20, ohne einen AS-PATH anzuhängen, und der ISR cEdge verteilt Präfixe neu, indem er das AS-PATH-Feld dreimal anfügt. Dadurch wird sichergestellt, dass die ASR-Kanten bevorzugt werden.

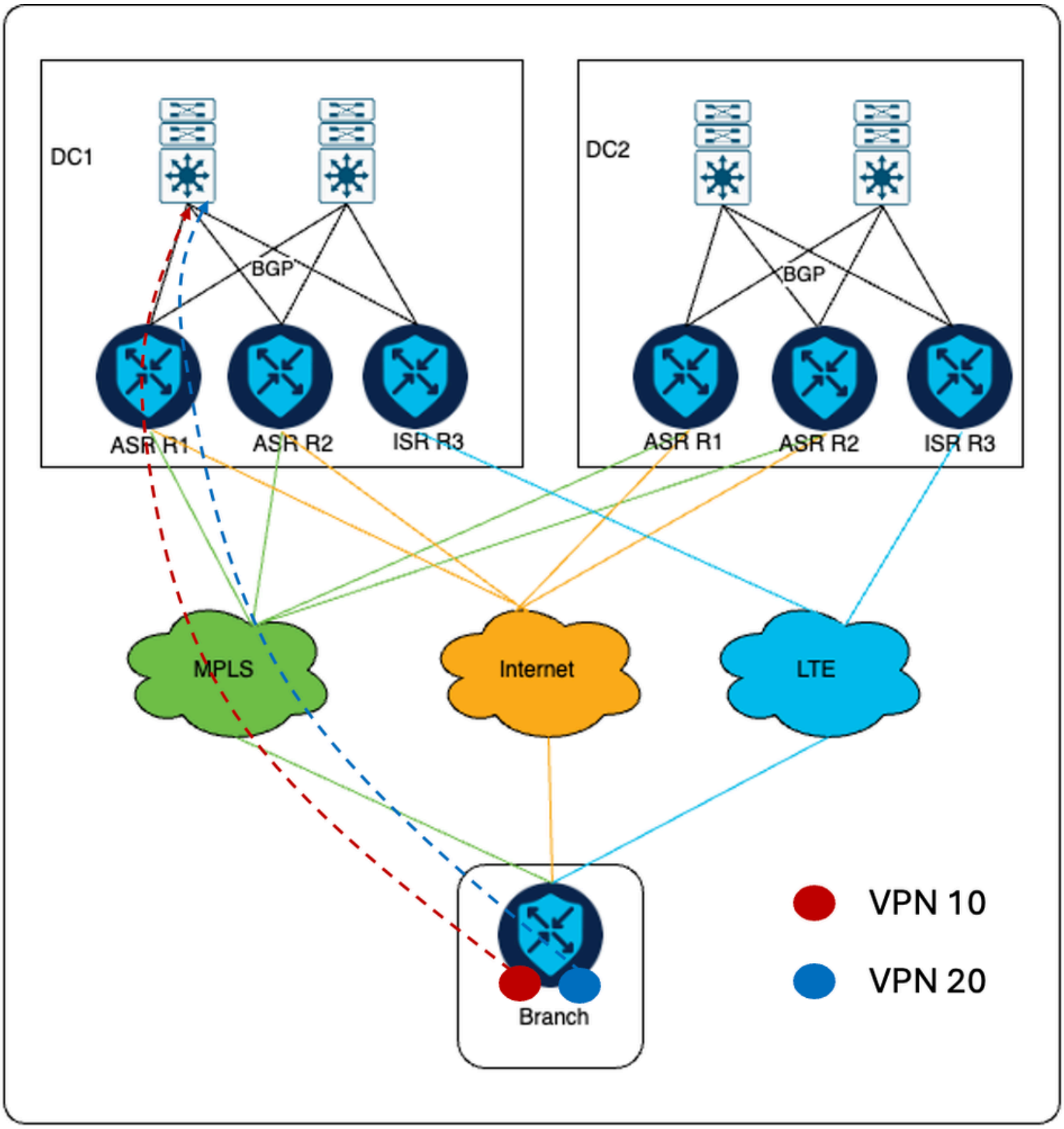
Lokalisierte Richtlinienkonfiguration

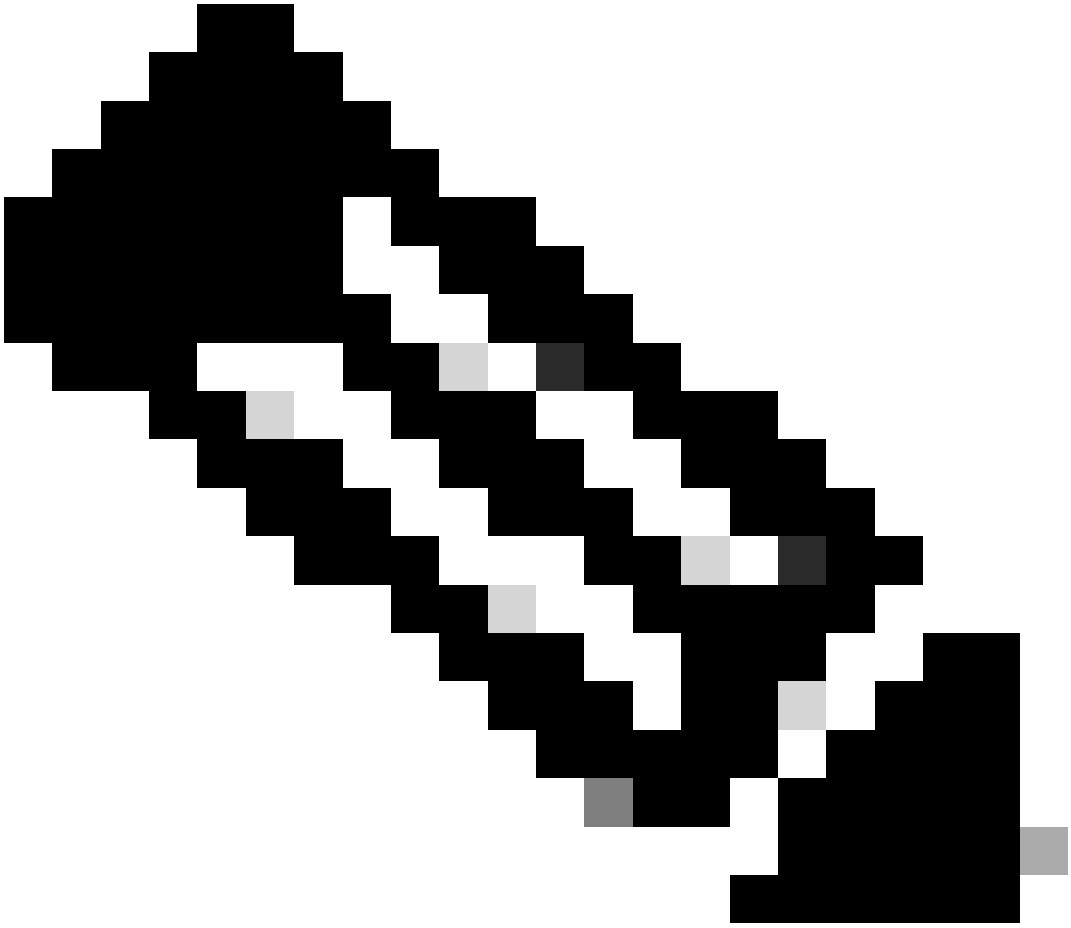
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_VPN-10_out_v001 permit 65535

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
```

Datenverkehrsfluss

Normales Szenario

Wenn die MPLS-Verbindung aktiv ist, durchläuft der gesamte Datenverkehr von VPN 10 und VPN 20 den MPLS-Transport.

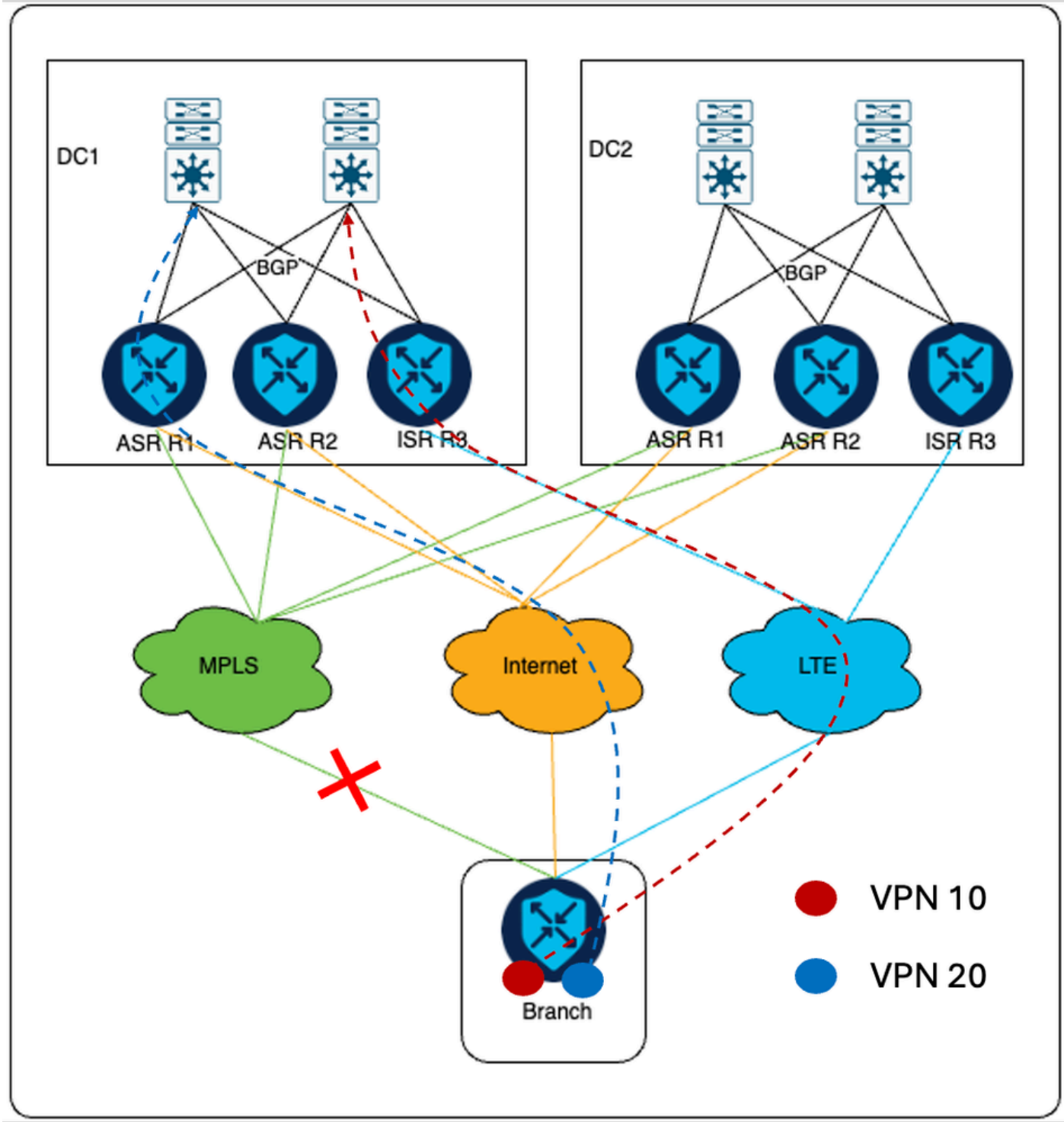

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



Hinweis: DC1 ist das primäre DC.

Failover-Szenario

Bei einem Ausfall der MPLS-Verbindung wird der VPN 10-Datenverkehr über LTE zum ISR cEdge übertragen. Hierbei wird VPN 20-Datenverkehr über das Internet an das ASR cEdge-Gerät gesendet.



Bei Datenrückverkehr von Core-Switches wird für VPN 10-Datenverkehr an den ISR cEdge gesendet, da die AS-PATH-Länge über den ISR im Vergleich zum ASR kleiner ist, wie im Abschnitt über lokalisierte Richtlinien angegeben. Auf ähnliche Weise wird VPN 20-Datenverkehr an ASR-Edges gesendet, da AS-PATH über ASR im Vergleich zu ISR kleiner ist.

Zusätzliche Informationen

In der früheren Konfiguration sind alle cEdges in jedem Rechenzentrum nur über den Internettransport mit den SD-WAN-Controllern verbunden. Auf diese Weise verfügen ISR-Router über einen konfigurierten Internet-Tunnel. Die Anforderung besteht darin, sicherzustellen, dass

ISR cEdge einen IPsec-Tunnel zu entfernten Zweigstellen nur über LTE-Transport bildet, und um die vorgegebene Anforderung zu erfüllen, muss die Tunnelfarbe für den Internet-Transport von ISR mit einer öffentlichen Farbe konfiguriert werden, die in der Kundeneinrichtung nicht verwendet wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.