使用集中資料策略插入服務：一種獨特的交通機動用例

目錄

簡介

本文檔描述了服務連結用於控制從Internet到SDWAN分支站點託管伺服器的入站流量的示例場景。

背景資訊

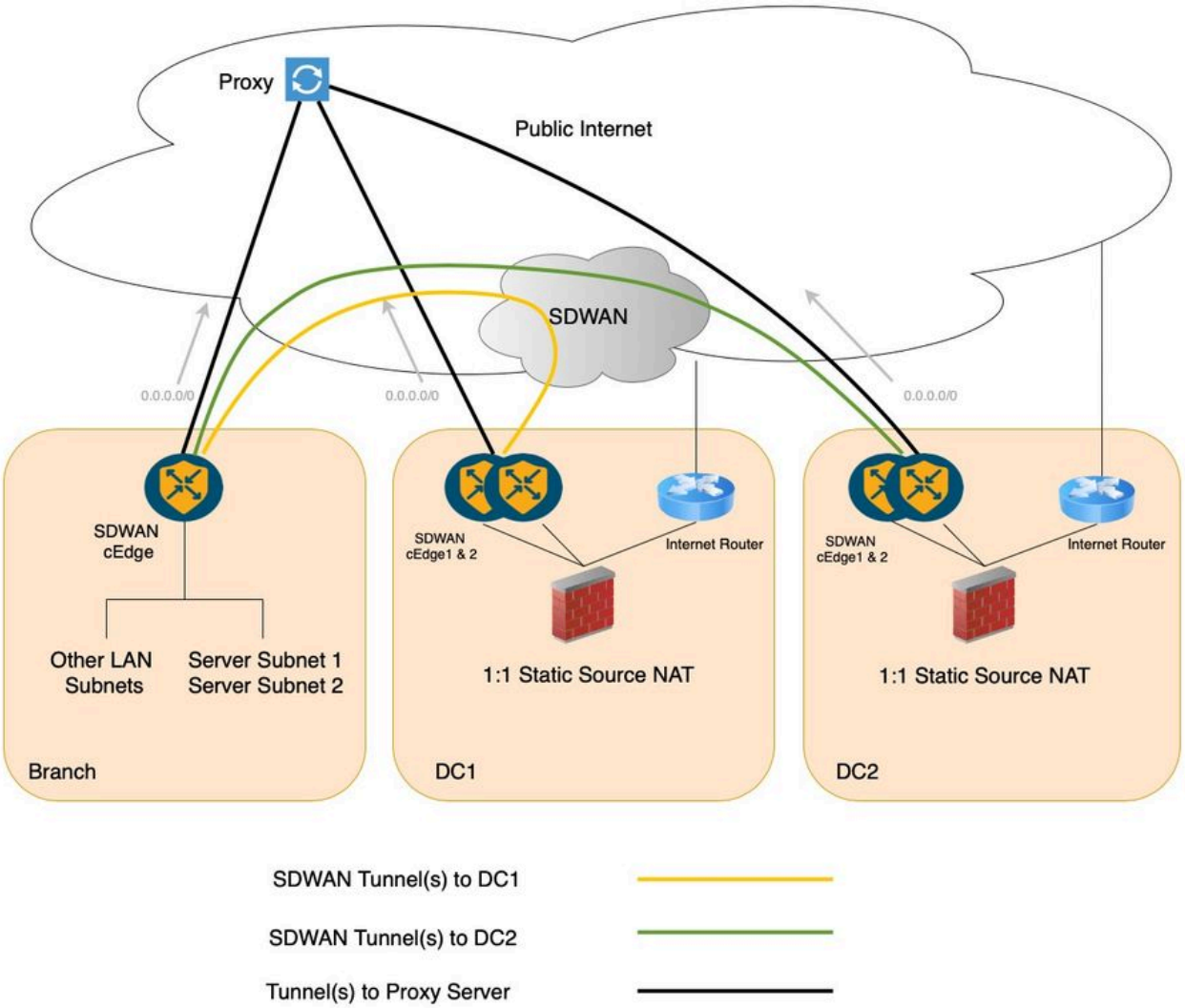
本文檔還顯示，通過使用服務鏈，可以輕鬆跟蹤資料中心(DC)LAN鏈路故障，以通知Branch SDWAN路由器使用資料策略更改流量路徑，否則不可能更改資料路徑，否則流量很容易在DC中陷入黑洞。

此處的入站流量通過DC防火牆進行路由，以實現管理和安全。

拓撲示例

已考慮採用雙DC設定和分支站點的標準SDWAN部署，以描繪此場景，如下圖所示。然而，為了簡單起見，可以有多個分支。DC和分支站點通過安全SDWAN重疊進行通訊，即通過SDWAN安全IPSec隧道。在此現有設定中，DC和分支站點都擁有到服務虛擬路由和轉發(VRF)中的代理伺服器的隧道，並且服務VRF/虛擬專用網路(VPN)中的預設路由指向此代理。

此拓撲設定包含一個分支站點，其中託管兩個伺服器子網：伺服器子網1和伺服器子網2。有兩個資料中心，每個資料中心防火牆執行1:1靜態網路地址轉換(NAT)，以允許從網際網路訪問各自的分支伺服器子網。確切地說，資料中心1防火牆對伺服器子網1執行1:1靜態NAT，資料中心2防火牆對伺服器子網2執行相同的操作。

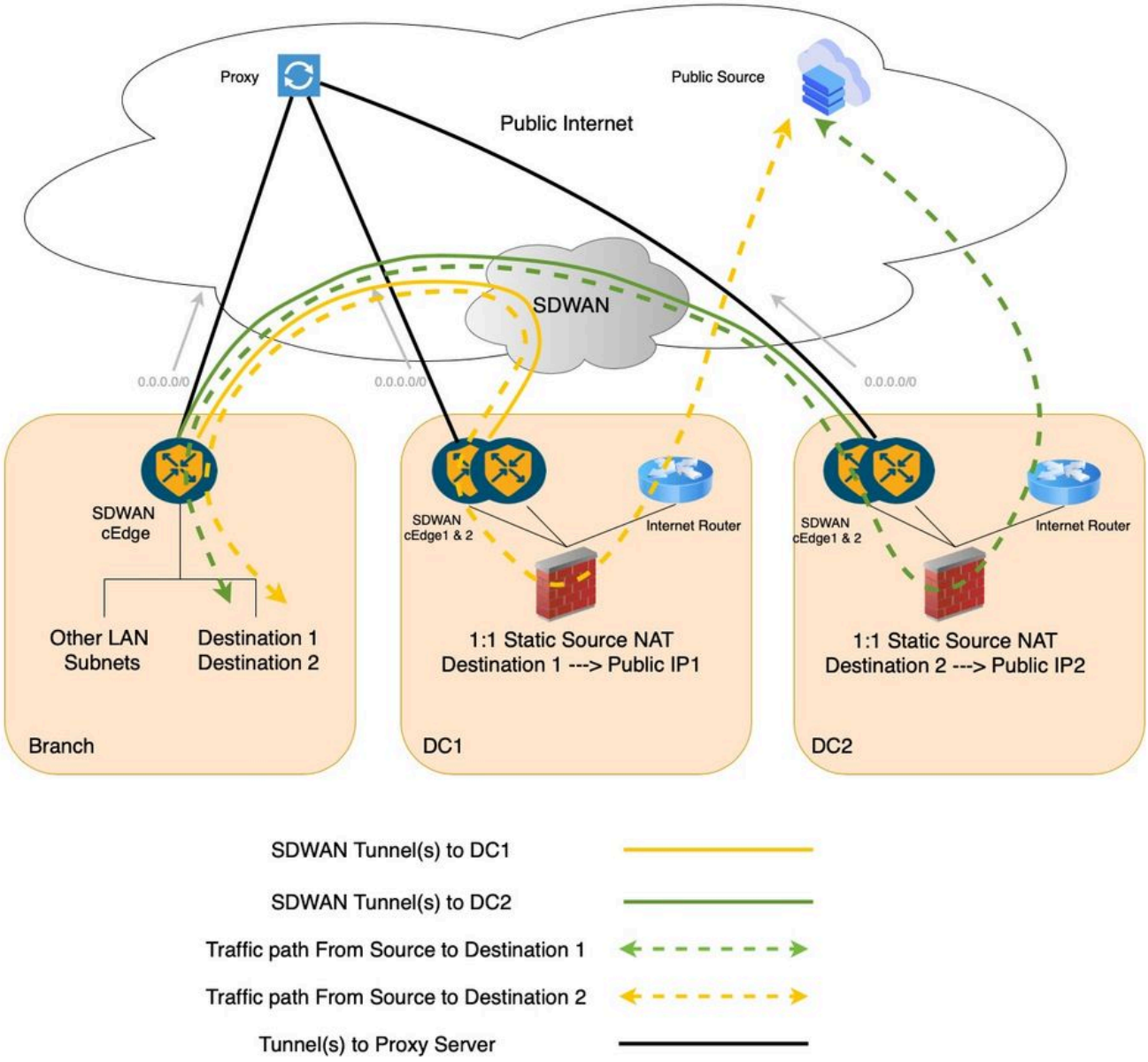


客戶需求

在瞭解了早期設定後，客戶提出的要求可如下所述：

- 公共應用程式（如MS Teams）必須訪問這些在分支機構中託管的伺服器。如前所述，DC中有狀態防火牆的可用性使客戶請求使用它們，而不是直接到分支機構站點的入站連線。
- 分支機構中的伺服器子網1必須可通過DC1訪問，而分支機構中的伺服器子網2必須通過DC2從Internet訪問。
- 客戶網路內不得路由任何公共IP。
- 分支機構託管伺服器子網1和2配置了專用IP，並且專用IP到公共IP轉換必須在各自的DC防火牆中進行。
- 不得有任何底層路由更改。

附註：如果DC或分支機構站點的流量流未發生更改，則來自網際網路的轉發流量將通過DC防火牆以到達分支機構站點的伺服器。另一方面，返回流量將直接通過Branch SDWAN路由器上的Proxy（使用預設路由），以便到達網際網路源。這是非對稱的流量流。



可能的解決方案

有兩種可能的解決方案來滿足早期的要求：

1. 使用集中式資料策略的自定義流量工程，在DC LAN鏈路出現故障時流量會進入黑洞。
2. 使用集中式資料策略插入服務，在DC LAN鏈路發生故障時，流量不會進入黑洞。

1.採用集中式資料策略的自定義流量工程

如果考慮集中資料策略下的自定義流量工程資料策略（一個用於分支，另一個用於DC），則分支資料策略使用遠端定位將流量從分支傳送到DC，而第二個資料策略進一步將DC內的流量從cEdge路由到防火牆(FW)。但是，由於分支中配置了remote-tloc選項，因此分支SDWAN路由器不知道DC SDWAN路由器1 LAN鏈路故障。也就是說，如果DC SDWAN路由器1上的LAN鏈路發生故障，則Branch路由器並不知道該流量，仍將該流量轉發到DC SDWAN路由器01。因此，該流量很容易在DC SDWAN路由器1上成為黑洞。

配置（使用自定義資料策略）

應用於DC SDWAN路由器從隧道方向：

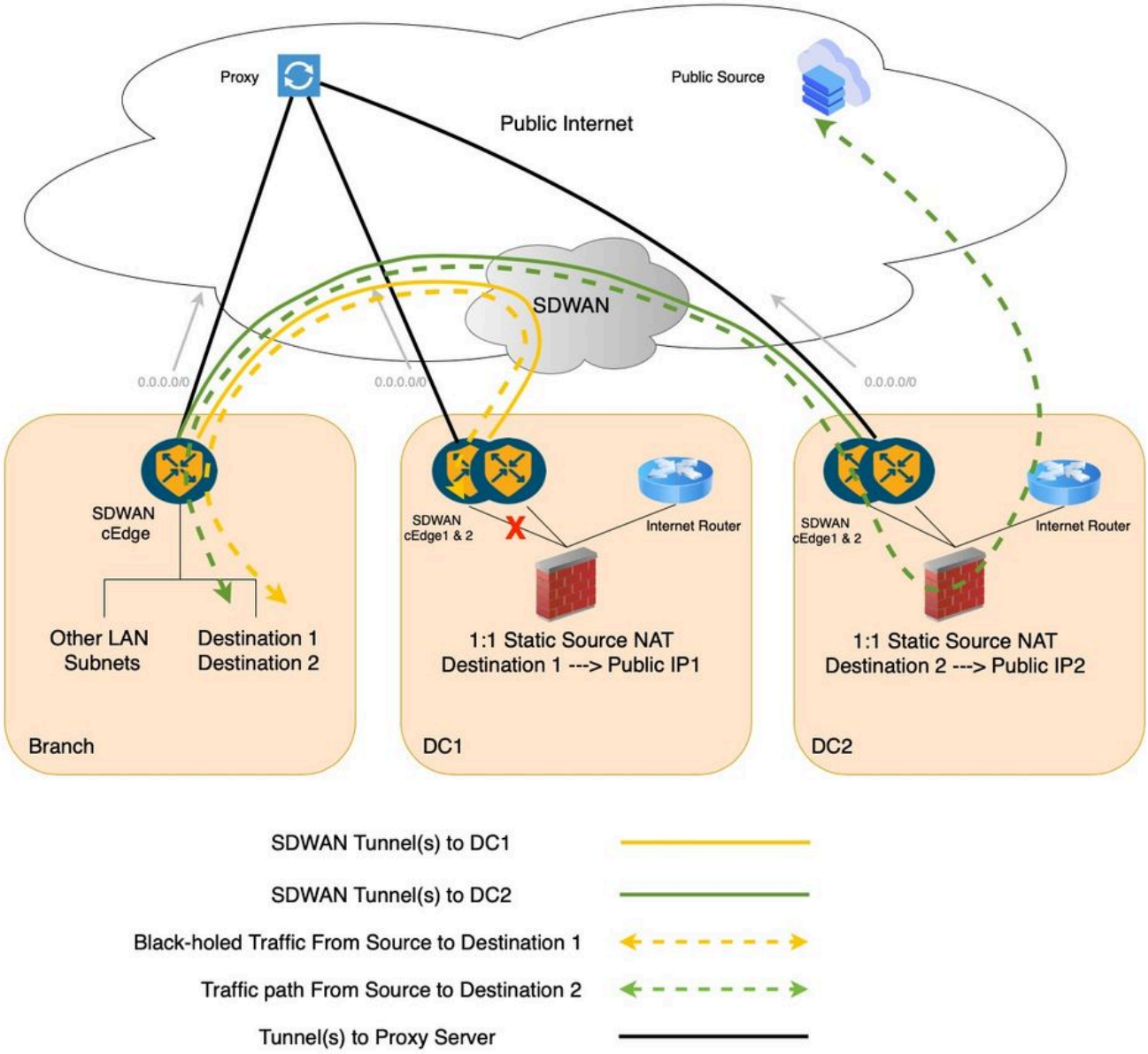
```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
       next-hop <Firewall_IP>
      !
     !
```

應用於Branch SDWAN路由器的服務方向：

```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
         tloc-list <DC_TLOC_LIST>
      !
     !
  !
  tloc-list <DC_TLOC_LIST>
   tloc <DC cEdge01 System IP> color <primary colour> encap ipsec preference 100
   tloc <DC cEdge02 System IP> color <secondary colour> encap ipsec preference 50
  !
```

使用自定義資料策略的流量(DC SDWAN路由器1 LAN鏈路故障案例)

在DC SDWAN路由器1 LAN鏈路出現故障的情況下，DC SDWAN路由器1上的流量會進入黑洞。



2.使用集中資料策略插入服務

Cisco SDWAN服務鏈本身非常靈活且完全自動化。在傳統WAN設定中。如果您必須在特定流量的路徑中插入防火牆，則它通常與每個躍點的大量手動配置相關聯。相反，Cisco SD-WAN服務插入過程非常簡單，只需將相關流量與集中控制或資料策略相匹配，將防火牆服務設定為下一個躍點，然後通過單個網路配置協定(NETCONF)事務將該策略應用於目標站點清單（從Cisco SDWAN Manager到Cisco SDWAN控制器）。

以下是我們的組態範例中插入防火牆即服務的步驟：

1.將防火牆定義為DC cEdge裝置上的服務。可以使用VPN功能模板以及直接登入裝置來實現這一點。服務跟蹤預設啟用，這意味著如果DC防火牆無法從DC SDWAN主路由器cEdge1訪問，則整個服務將關閉，流量將回退到DC的輔助路由器cEdge2。

2.構建並應用集中式資料策略，以雙向將防火牆服務插入到流量路徑中。

配置（帶有服務插入）

在DC SDWAN路由器上配置：

```
!
sdwan
  service firewall vrf X
  ipv4 address <fw next-hop ip>
!
commit
```

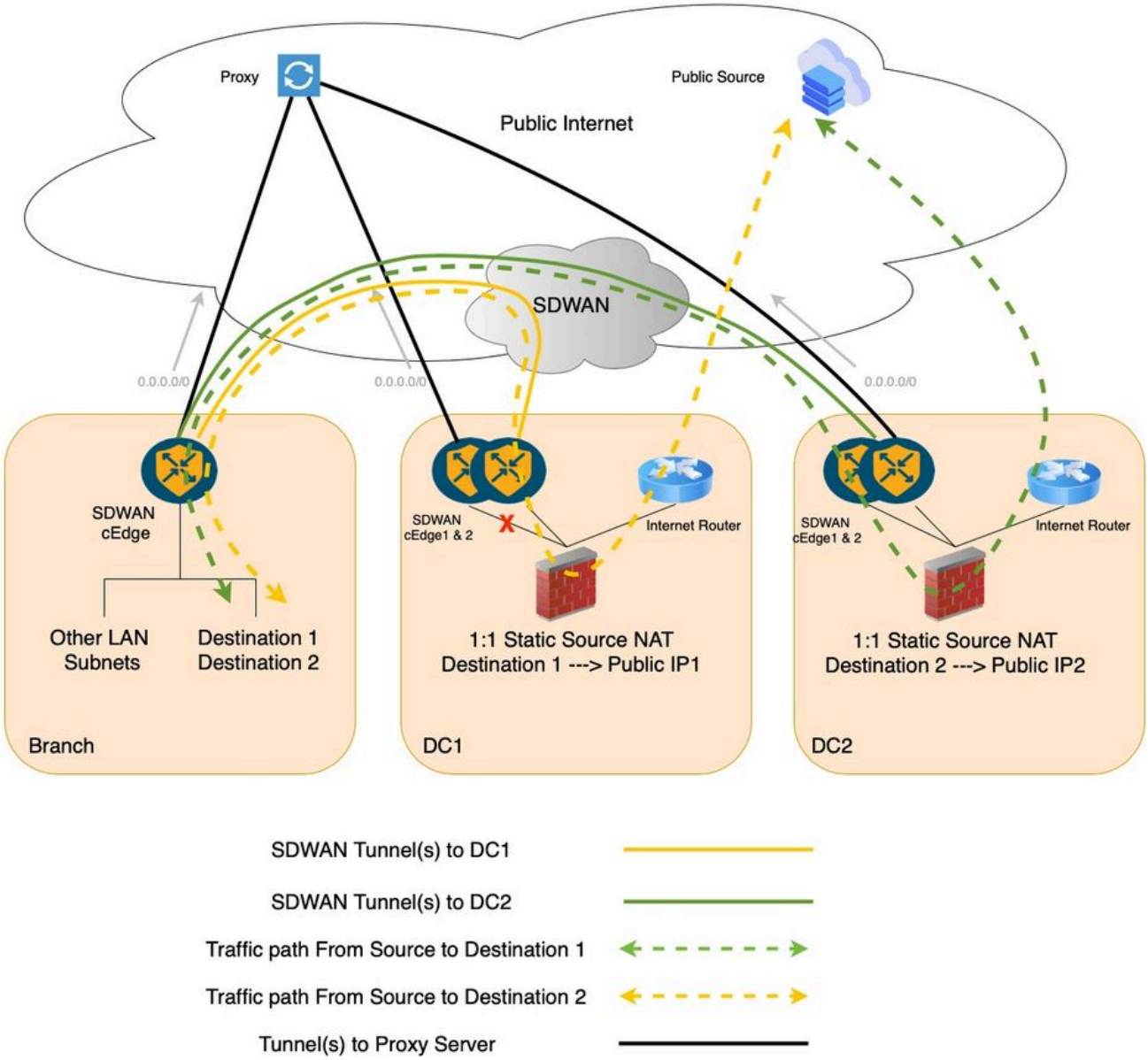
DC SDWAN路由器的早期配置定義了「防火牆」型別的服務，該服務會通告給Cisco SDWAN控制器。當防火牆服務的可達性關閉或防火牆本身關閉時，DC SDWAN路由器會停止通告相同內容。

服務鏈策略定義為：應用於分支SDWAN路由器的服務方向：

```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
       service  FW vpn X tloc-list <DC_TLOC_LIST>
      !
     !
  !
  tloc-list <DC_TLOC_LIST>
   tloc <DC cEdge01 System IP> color <primary colour> encap ipsec preference 100
   tloc <DC cEdge02 System IP> color <secondary colour> encap ipsec preference 50
  !
```

帶有服務插入的流量（DC SDWAN路由器1 LAN鏈路故障案例）

如果DC SDWAN Router 1 LAN鏈路出現故障，流量將故障轉移到DC SDWAN Router 2。



這些策略先決條件或預定義清單在Cisco Catalyst SDWAN Manager上定義，如以下所示以供參考：

```
lists
  data-prefix-list <BranchSiteServerSubnet>
   ip-prefix <ip/mask>
  !
  data-prefix-list <PublicIPSubnet>
   ip-prefix <ip/mask>
  !
  site-list <BranchSiteList>
   site-id <BranchSiteID>
  !
  !
  tloc-list <DC_TLOC_LIST>
   tloc <DC cEdge01 System IP> color <primary colour> encap ipsec preference 100
   tloc <DC cEdge02 System IP> color <secondary colour> encap ipsec preference 50
  !
  !
  vpn-list <VPN_Name>
```

```
 vpn X
!
!
```

流量詳細資訊有助於更好地瞭解流量

從外部到內部的流量

Internet Source(MS Teams)> DC1 FW(NAT)> DC1 cEdge01 > Branch cEdge01 > Server Subnet 1。

Internet Source(MS Teams)> DC2 FW(NAT)> DC2 cEdge01 > Branch cEdge01 > Server Subnet 2。

因此，流量影響在各自的躍點中完成，如下所示：

Internet Source(MS Teams)> DC1 FW。

Internet Source(MS Teams)> DC2 FW。

DC1和DC2通過DC處的網際網路CPE向網際網路通告各自的公共IP池。

DC1 FW > DC1 cEdge01。

DC2 FW > DC2 cEdge01。

內部子網的防火牆路由。

DC1 cEdge01 > Branch cEdge01。

DC2 cEdge01 > Branch cEdge01。

透過重疊管理通訊協定(OMP)重疊的Cisco SDWAN路由。

Branch cEdge01 > Server Subnet 1。

Branch cEdge01 > Server Subnet 2。

內部子網的分支路由器路由。

內部到外部流量

Server Subnet 1 > Branch cEdge 01 > DC1 cEdge 01 > DC1 FW(NAT)> Internet Source(MS Teams)。

伺服器子網2 > Branch cEdge 01 > DC2 cEdge 01 > DC2 FW(NAT)> Internet Source(MS Teams)。

因此，流量影響在各自的躍點中完成，如下所示：

伺服器子網1 > Branch cEdge 01。

伺服器子網2 > Branch cEdge 01。

從伺服器端進行內部路由。

分支cEdge 01 > DC1 cEdge 01。

分支cEdge 01 > DC2 cEdge 01。

使用集中式資料策略（服務連結）來影響流量路徑。

DC1 cEdge01 > DC1 FW。

DC2 cEdge01 > DC2 FW。

使用服務標籤，以影響從SDWAN cEdge到DC上各個FW的流量路徑。

DC1 FW(NAT)> Internet Source(MS Teams)。

DC2 FW(NAT)> Internet Source(MS Teams)。

來自伺服器的私有IP源流量通過NAT輸出FW，以便通過CPE訪問Internet。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。