使用集中数据策略插入服务：一种独特的交通机动用例

目录

简介

本文档介绍使用服务链控制从Internet到托管于SDWAN分支站点的服务器的入站流量的示例场景。

背景信息

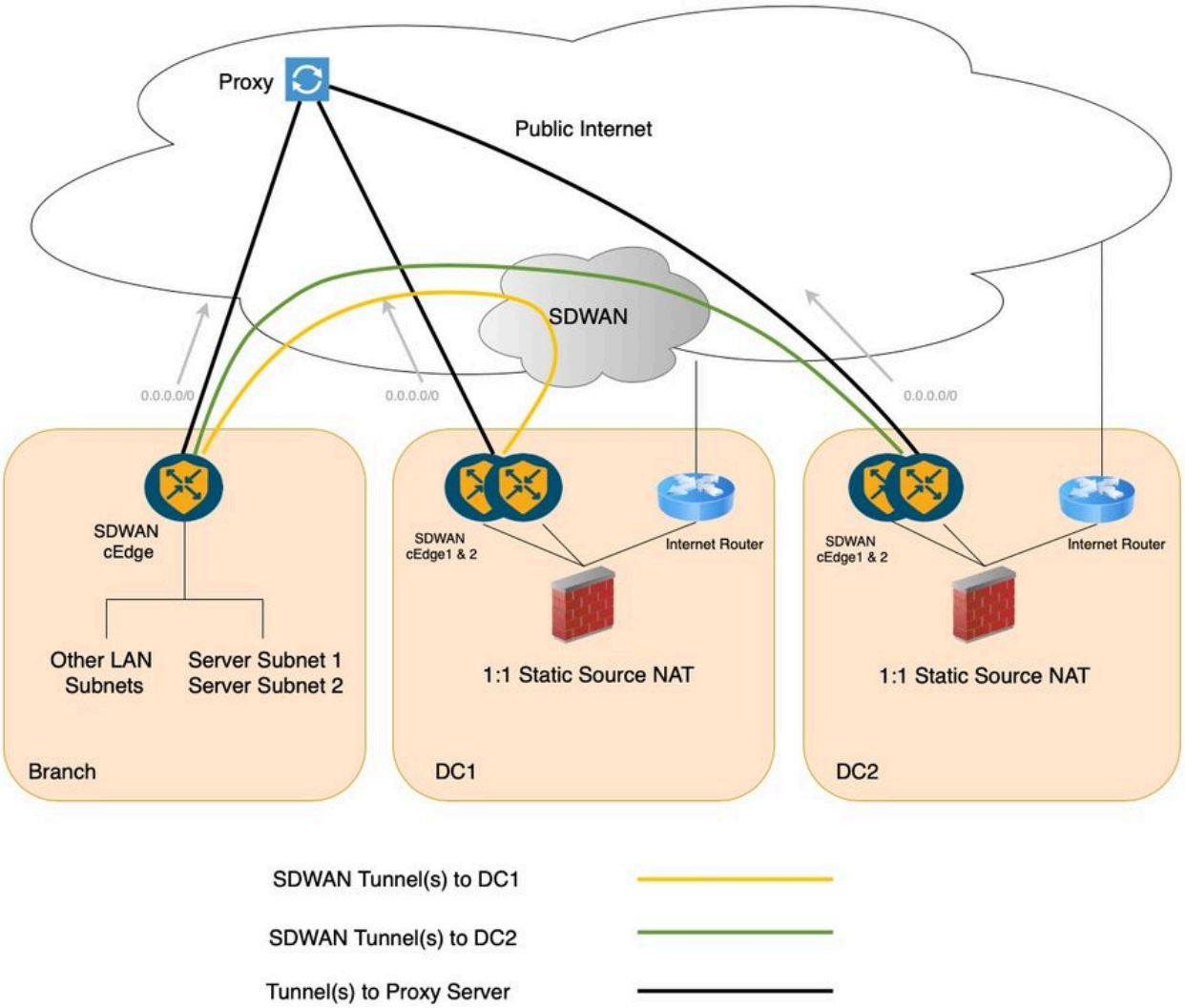
文档还显示，通过使用服务链，可以轻松跟踪数据中心(DC)LAN链路故障，以通知Branch SDWAN路由器使用数据策略更改流量路径，否则这是不可能的，如果没有数据链接，流量很容易在DC中进入黑洞。

此处的入站流量通过DC防火墙进行路由，以实现管理和安全。

示例拓扑

为了描绘此场景（如下图所示），已考虑采用双DC设置和分支站点的标准SDWAN部署。但是，为了简单起见，可以有多个分支。DC和分支站点通过安全SDWAN重叠进行通信，即通过SDWAN安全IPSec隧道进行通信。在此现有设置中，DC和分支站点都具有通向服务虚拟路由和转发(VRF)中的代理服务器的隧道，并且服务VRF/虚拟专用网络(VPN)中的默认路由指向此代理。

此拓扑设置包含托管两个服务器子网（服务器子网1和服务器子网2）的分支机构站点。有两个数据中心，每个数据中心防火墙执行1:1静态网络地址转换(NAT)以允许从互联网访问相应的分支服务器子网。为了精确起见，数据中心1防火墙对服务器子网1执行1:1静态NAT，数据中心2防火墙对服务器子网2执行相同的操作。

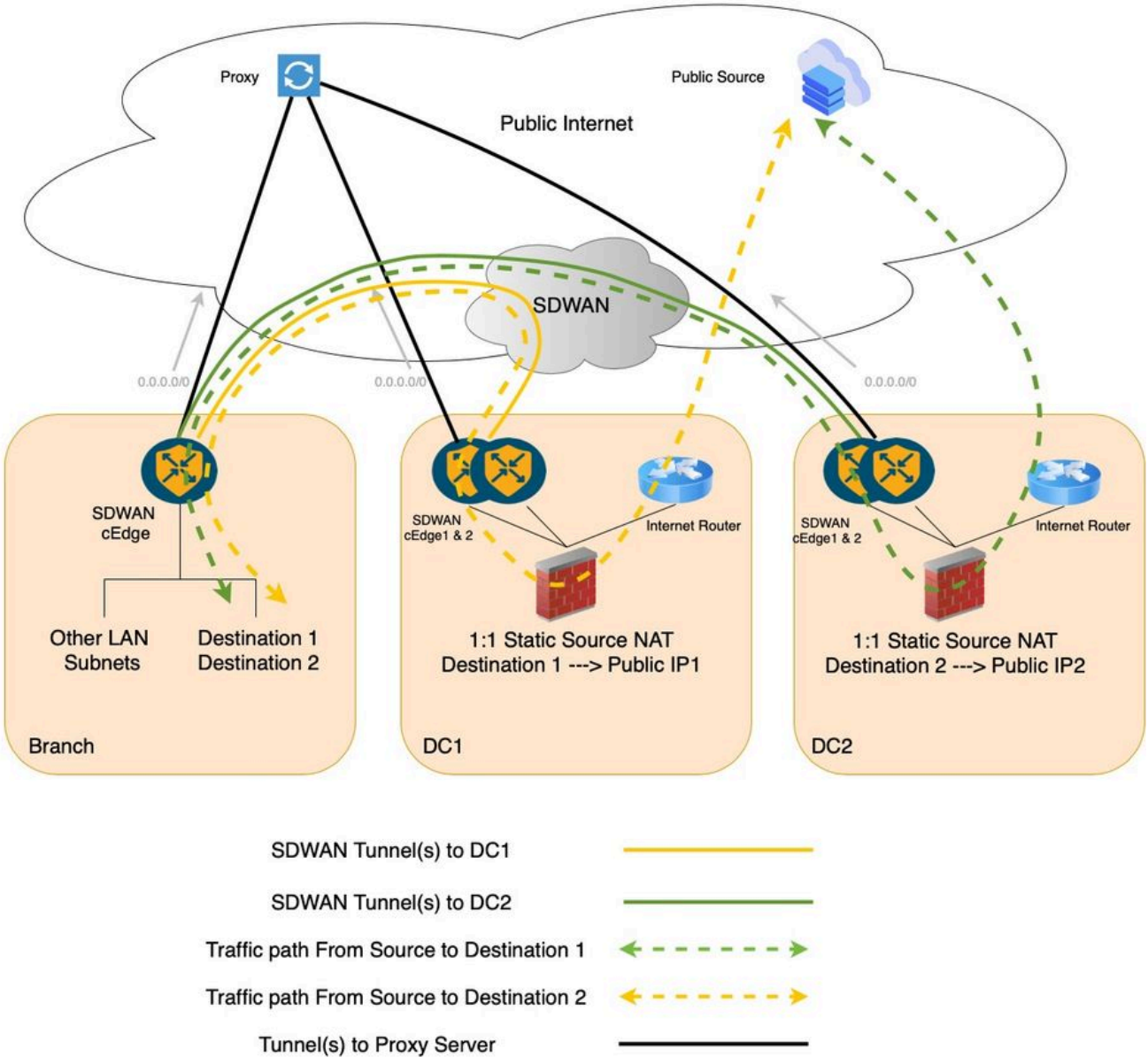


客户需求

在了解了早期设置后，可以提及来自客户的要求：

- 公共应用程序（如MS Teams）必须访问托管在分支机构的这些服务器。如前所述，DC中状态防火墙的可用性使客户请求使用它们，而不是直接入站连接到分支机构站点。
- 分支机构中的服务器子网1必须可通过DC1到达，分支机构中的服务器子网2必须通过DC2从Internet到达。
- 客户网络内不得路由任何公有IP。
- Branch托管服务器子网1和2配置了专用IP，并且专用IP到公共IP转换必须在各自的DC FW中进行。
- 不得有任何底层路由更改。

注意：如果DC或分支站点中的流量流未发生变化，来自互联网的转发流量将通过DC防火墙到达分支站点的服务器。另一方面，返回流量将直接通过Branch SDWAN路由器上的代理（使用默认路由）以到达互联网源。这是不对称的流量。



可能的解决方案

对于早期的要求，有两种可能的解决方案：

1. 采用集中数据策略的自定义流量工程，在DC LAN链路发生故障时流量会进入黑洞。
2. 使用集中数据策略插入服务，在DC LAN链路发生故障时，流量不会进入黑洞。

1.采用集中式数据策略的自定义流量工程

如果考虑集中数据策略下的自定义流量工程数据策略（一个用于分支，另一个用于DC），则分支数据策略使用远程tlocs将流量从分支发送到DC，第二个数据策略进一步将DC内的流量从cEdge路由到防火墙(FW)。但是，在分支中配置remote-tloc选项后，分支SDWAN路由器不知道DC SDWAN路由器1的LAN链路故障。也就是说，如果DC SDWAN路由器1上的LAN链路发生故障，则Branch路由器不会察觉该流量并将该流量转发到DC SDWAN路由器01。因此，该流量很容易在DC SDWAN路由器1上成为黑洞。

配置（使用自定义数据策略）

应用于DC SDWAN路由器从隧道方向：

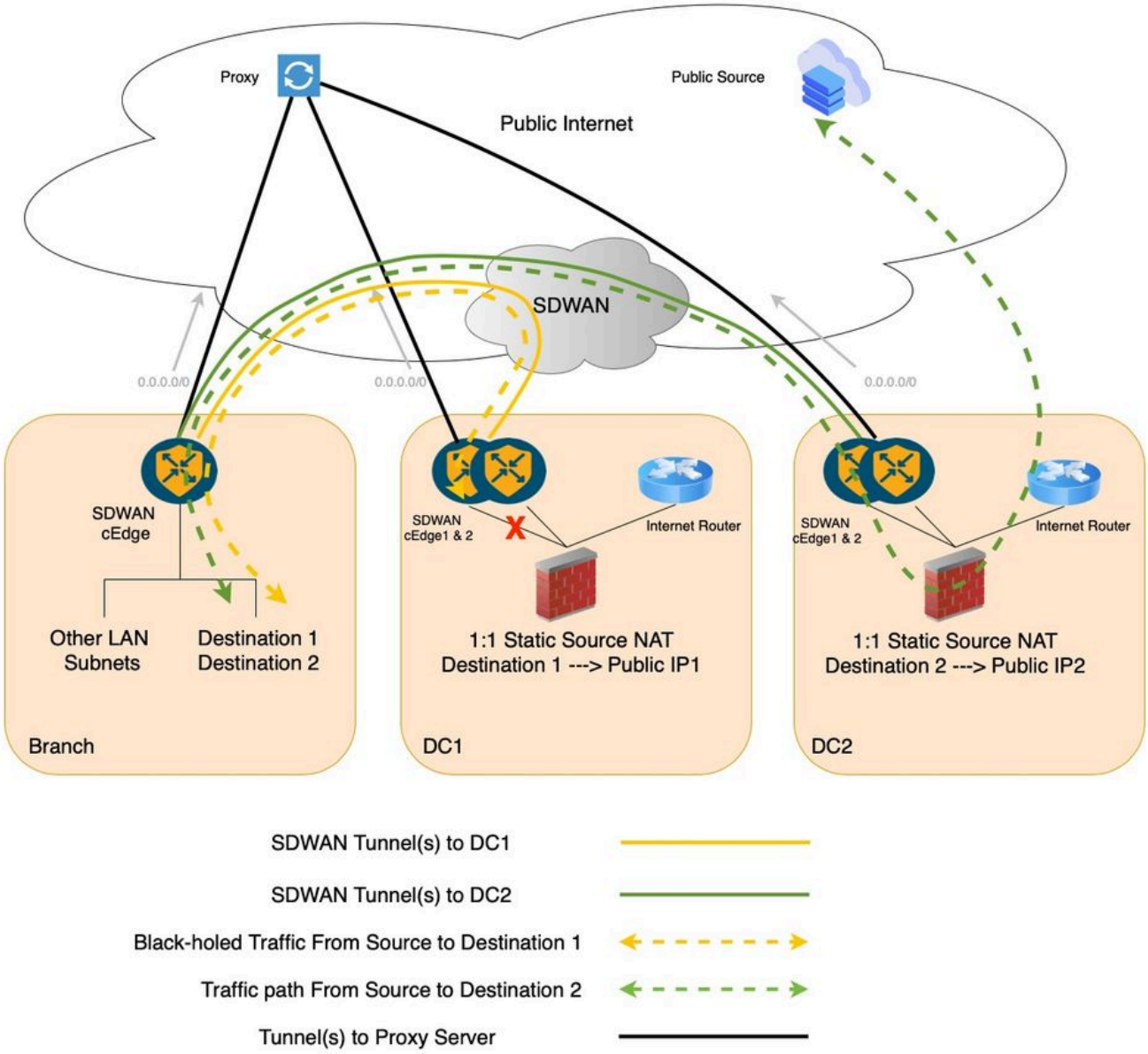
```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
       next-hop <Firewall_IP>
      !
     !
```

应用于Branch SDWAN路由器的服务方向：

```
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
  !
```

使用自定义数据策略的流量(DC SDWAN路由器1LAN链路故障案例)

如果DC SDWAN路由器1 LAN链路发生故障，DC SDWAN路由器1上的流量会进入黑洞。



2.使用集中数据策略插入服务

思科SDWAN服务链本身非常灵活且完全自动化。在传统WAN设置中。如果您必须在特定流量的路径中插入防火墙，则通常与每一跳的大量手动配置相关联。相反，思科SD-WAN服务插入过程非常简单，只需将相关流量与集中控制或数据策略相匹配，将防火墙服务设置为下一跳，然后通过从思科SDWAN管理器到思科SDWAN控制器的单个网络配置协议(NETCONF)事务将策略应用于目标站点列表。

以下是在我们的配置示例中插入防火墙即服务的步骤：

1.将防火墙定义为DC cEdge设备上的服务。这可以使用VPN功能模板以及直接登录设备来实现。服务跟踪默认启用，这意味着如果DC防火墙无法从DC SDWAN主路由器cEdge1访问，则整个服务将关闭，流量将回退到DC的辅助路由器cEdge2。

2.构建和应用集中数据策略，以双向将FW服务插入流量路径。

配置（带有服务插入）

在DC SDWAN路由器上配置：

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

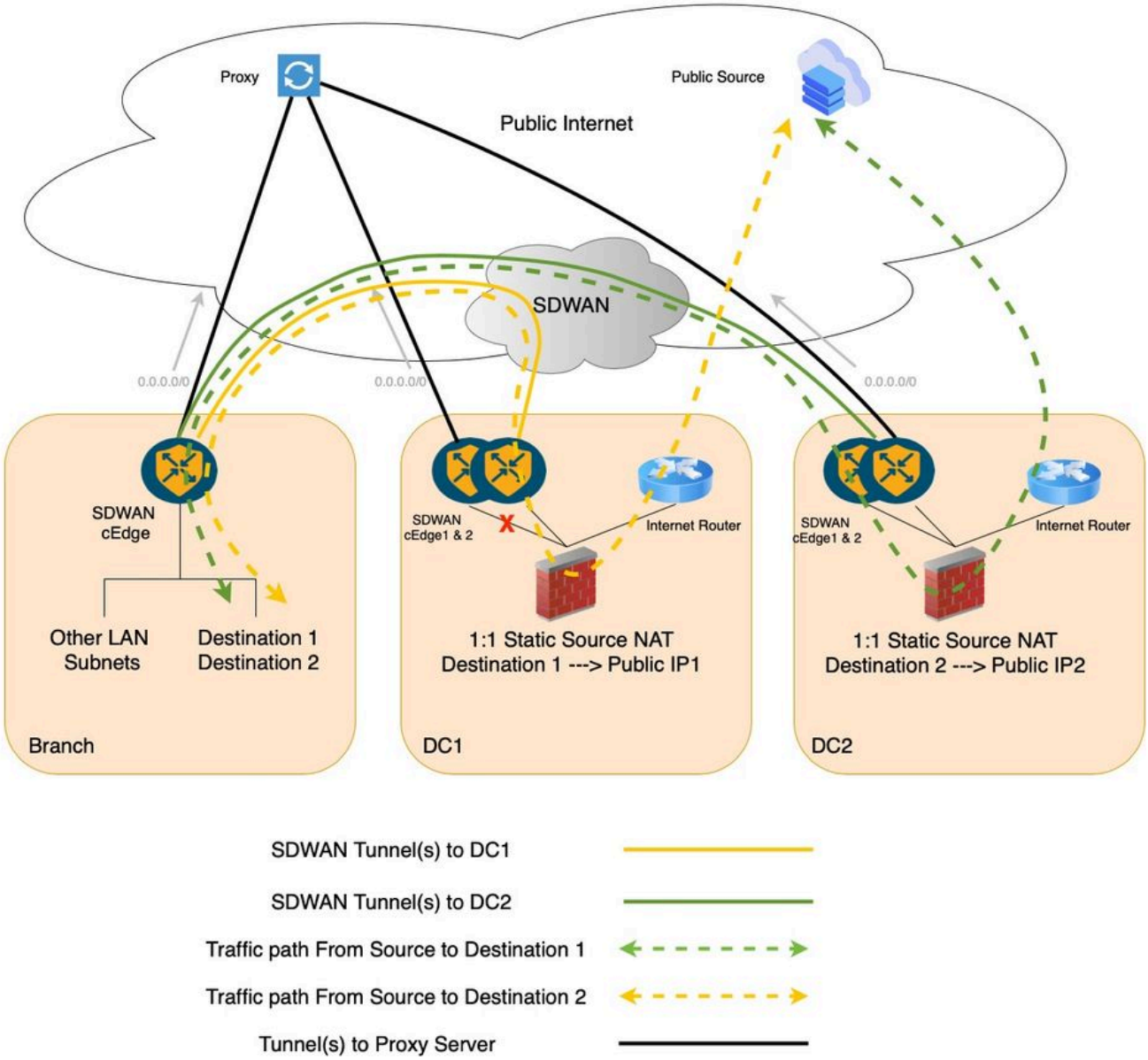
DC SDWAN路由器上的早期配置定义了“防火墙”类型的服务，该服务会通告给Cisco SDWAN控制器。当防火墙服务的可达性断开或防火墙自身关闭时，DC SDWAN路由器会停止通告相同内容。

服务链接策略定义为在分支机构SDWAN路由器服务方向应用：

```
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
  !
```

带有服务插入的流量（DC SDWAN路由器1 LAN链路故障情况）

如果DC SDWAN Router 1 LAN链路发生故障，流量将故障转移到该DC SDWAN路由器2。



这些策略先决条件或预定义列表在Cisco Catalyst SDWAN Manager上定义，如图所示，以供参考：

```
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
!
!
```

流量详细信息，更好地了解流量

外部到内部流量

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。

对于此流量影响，按如下方式在各自的跳数中执行：

Internet Source(MS Teams)> DC1 FW。

Internet Source(MS Teams)> DC2 FW。

DC1和DC2通过DC上的Internet CPE将各自的公共IP池通告给Internet。

DC1 FW > DC1 cEdge01。

DC2 FW > DC2 cEdge01。

内部子网的防火墙路由。

DC1 cEdge01 > Branch cEdge01。

DC2 cEdge01 > Branch cEdge01。

通过重叠管理协议(OMP)重叠的思科SDWAN路由。

Branch cEdge01 > Server Subnet 1。

Branch cEdge01 > Server Subnet 2。

内部子网的分支路由器路由。

内部到外部流量

服务器子网1 > Branch cEdge 01 > DC1 cEdge01 > DC1 FW(NAT)> Internet Source(MS Teams)。

服务器子网2 > Branch cEdge 01 > DC2 cEdge01 > DC2 FW(NAT)> Internet Source(MS Teams)。

对于此流量影响，按如下方式在各自的跳数中执行：

Server Subnet 1 > Branch cEdge 01。

Server Subnet 2 > Branch cEdge 01。

从服务器端进行内部路由。

分支cEdge 01 > DC1 cEdge01。

分支cEdge 01 > DC2 cEdge01。

使用集中数据策略（服务链）来影响流量路径。

DC1 cEdge01 > DC1 FW。

DC2 cEdge01 > DC2 FW。

使用服务标签以影响从SDWAN cEdge到DC上各个FW的流量路径。

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

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

来自服务器的私有IP源流量通过NAT出口FW，以便通过CPE访问Internet。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。