# Inserción de servicios mediante una política de datos centralizada: Un caso práctico único de las maniobras de tráfico

## Contenido



## Introducción

Este documento describe un escenario de ejemplo en el que el encadenamiento de servicios se utiliza para controlar el flujo de tráfico entrante desde Internet a los servidores alojados en el sitio de sucursal de SDWAN.

## Antecedentes

El documento también muestra que mediante el encadenamiento de servicios se puede rastrear fácilmente la falla del link LAN del Data Center (DC) para notificar al router SDWAN de la sucursal que modifique la trayectoria de tráfico mediante la política de datos, lo que no es posible de otra manera y sin el cual el tráfico fácilmente se queda sin agujeros negros en el DC.

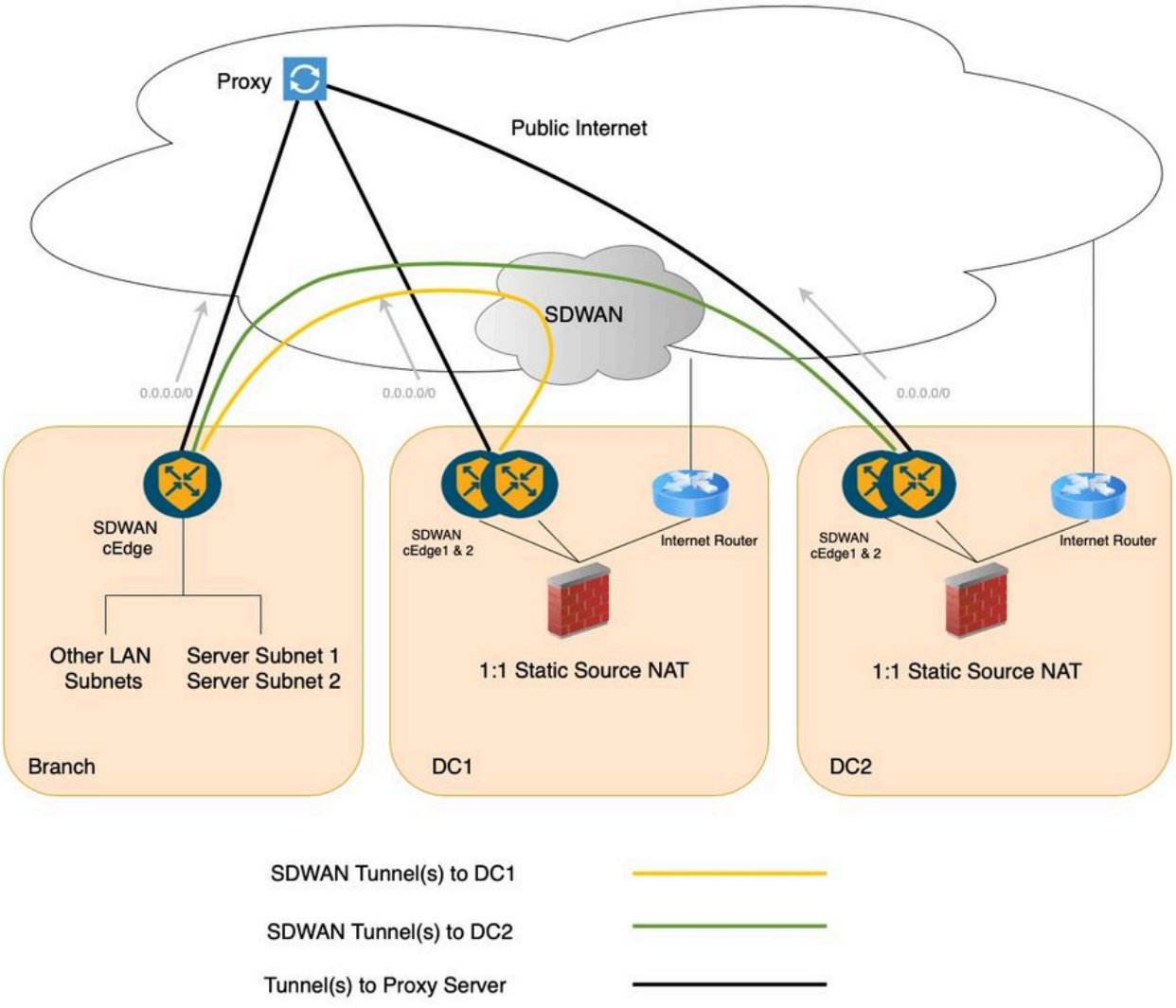
El tráfico entrante aquí se enruta a través de los firewalls del DC para la gestión y la seguridad.

## Topología de ejemplo

Se ha considerado una implementación SDWAN estándar con configuración de DC dual y una sucursal para representar este escenario como se muestra en el siguiente diagrama. Sin embargo, puede haber varias sucursales; por motivos de simplicidad, solo se ha descrito una. Los

Data Centers y las sucursales se comunican a través de la superposición SDWAN segura, es decir, a través de los túneles IPSec seguros de SDWAN. En esta configuración existente, tanto los DC como el sitio de la sucursal tienen túneles a los servidores proxy en el servicio Virtual Routing and Forwarding (VRF) y la ruta predeterminada en el servicio VRF/Virtual Private Network (VPN) apunta a este proxy.

Esta configuración de topología consta de una sucursal en la que se alojan dos subredes de servidores, Server Subnet 1 (Subred de servidor 1) y Server Subnet 2 (Subred de servidor 2). Hay dos Data Centers, en los que cada firewall del Data Center realiza la traducción de direcciones de red (NAT) estática 1:1 para permitir que la subred del servidor de la sucursal correspondiente sea accesible desde Internet. Para ser exactos, el firewall del Data Center 1 realiza la NAT estática 1:1 para la subred 1 del servidor y el firewall del Data Center 2 realiza la misma operación para la subred 2 del servidor.




## Requisitos del cliente

Con la configuración anterior en mente, el requisito del cliente puede ser como se mencionó:

- Las aplicaciones públicas como MS Teams tienen que acceder a estos servidores alojados en la sucursal. Como se ha indicado anteriormente, la disponibilidad de firmware stateful en

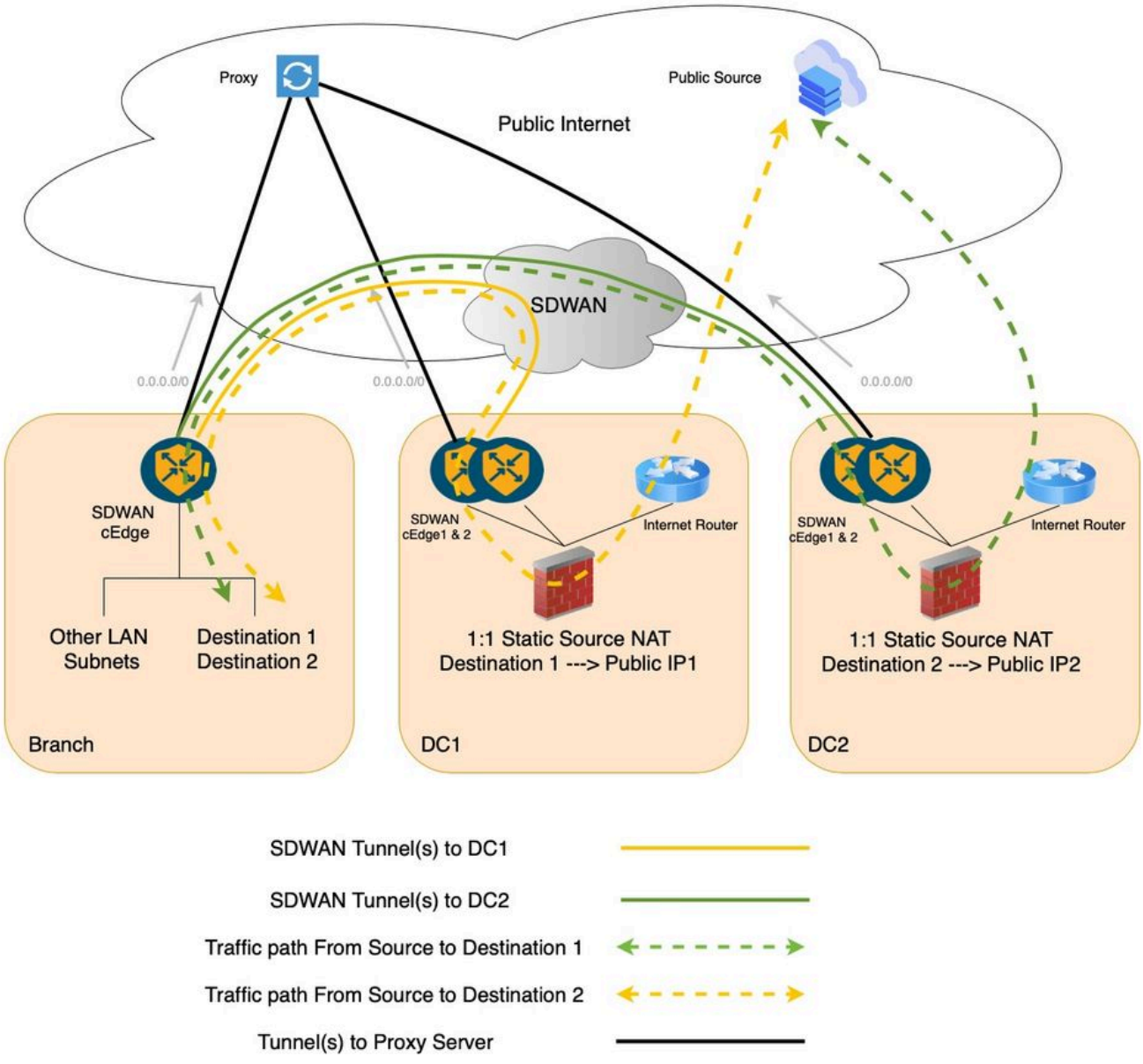
los DC hace que el cliente solicite que se utilicen en lugar de la conexión entrante directa con el sitio de la sucursal.

- La subred 1 del servidor en la sucursal debe ser accesible a través de DC1 y la subred 2 del servidor en la sucursal debe ser accesible a través de DC2 desde Internet.
- No se debe enrutar ninguna IP pública dentro de la red del cliente.
- Las subredes 1 y 2 del servidor alojado de la sucursal se configuran con IP privadas y la traducción de IP privada a pública debe realizarse en los respectivos FW de DC.
- No debe haber ningún cambio de ruteo subyacente.

---

Nota: Si no se realizan cambios en el flujo de tráfico en el DC o en el sitio de la sucursal, el tráfico de reenvío de Internet pasará a través de los firewalls del DC para llegar a los servidores en el sitio de la sucursal. Por otro lado, el tráfico de retorno pasará directamente a través del router SDWAN Proxy at Branch (proxy en la sucursal) (utilizando la ruta predeterminada) para llegar a la fuente de Internet. Esto es un flujo asimétrico de tráfico.

---



# Posibles soluciones

Puede haber dos soluciones posibles para los requisitos anteriores:

1. Ingeniería de tráfico personalizada con política de datos centralizada en la que se producen agujeros negros en el tráfico en caso de fallo del enlace DC LAN.
2. Inserción de servicio con política de datos centralizada en la que el tráfico no se bloquea en caso de fallo del enlace DC LAN.

## 1. Ingeniería de tráfico personalizada con política de datos centralizada

Si se tienen en cuenta las políticas de datos de ingeniería de tráfico personalizado en virtud de la política de datos centralizados, una para la sucursal y otra para el DC, la política de datos de sucursal envía el tráfico de la sucursal al DC mediante el uso de los tacos remotos y la segunda política de datos enruta aún más el flujo dentro del DC desde el perímetro hacia el firewall (FW). Sin embargo, con la opción de tloc remoto configurada en la sucursal, el router SDWAN de la sucursal no es consciente del fallo del enlace LAN del router SDWAN del DC 1. Es decir, si el enlace LAN en el router SDWAN 1 de DC falla, el router de la sucursal no detecta y sigue reenviando ese tráfico al router SDWAN 01 de DC. Por lo tanto, el tráfico fácilmente sufre agujeros negros en el router SDWAN 1 de DC.

Configuración (Con Política De Datos Personalizada)

Aplicado en el router SDWAN del DC desde la dirección del túnel:

```
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>
      !
     !
```

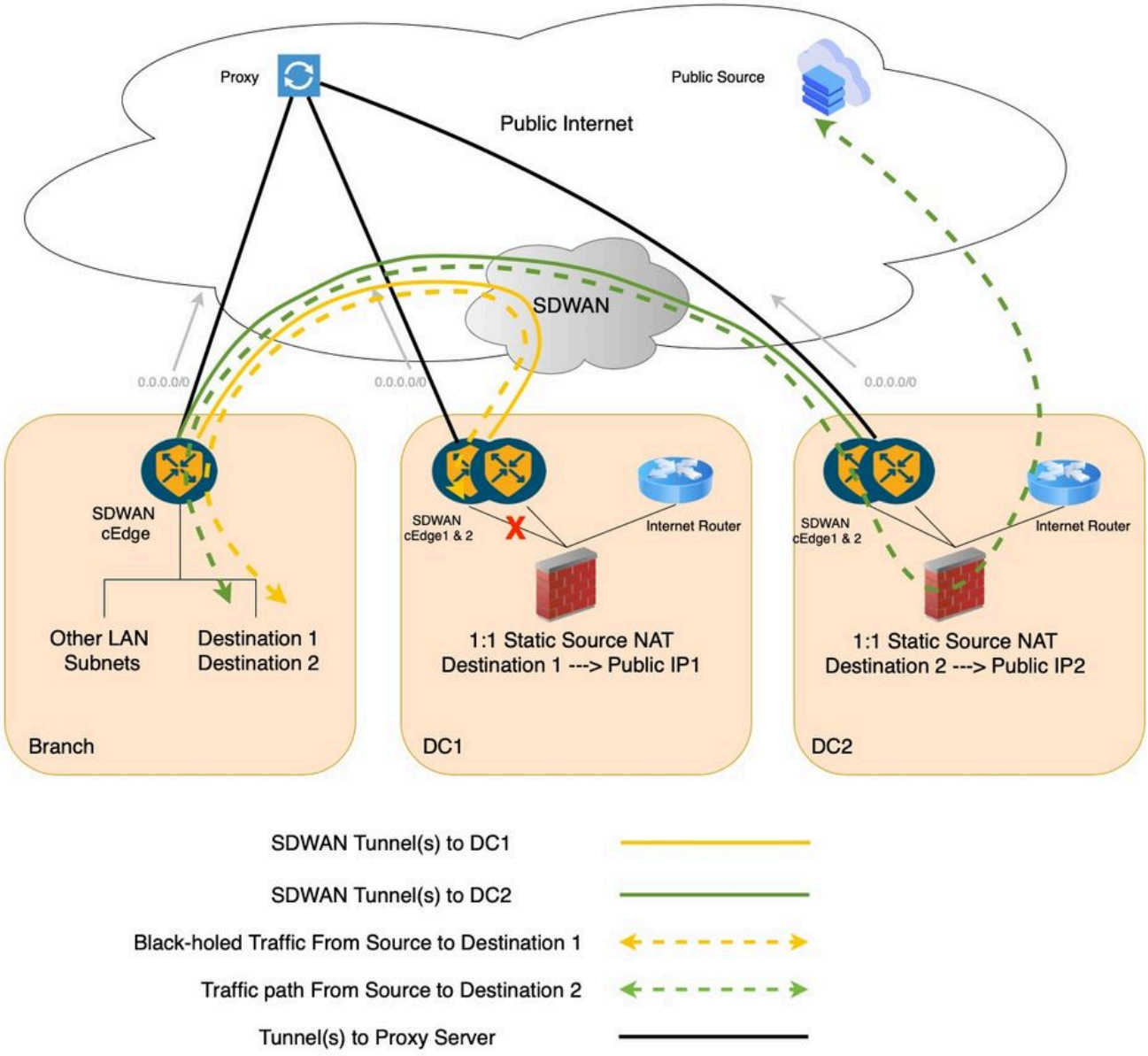
Aplicado en el router SDWAN de la sucursal desde la dirección no de servicio:

```
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
!
```

Flujo de tráfico con política de datos personalizada (caso de fallo de enlace LAN del router DC SDWAN 1)

Agujeros negros de tráfico en el router 1 de la SDWAN del DC en caso de que falle el enlace LAN del router 1 de la SDWAN del DC.




## 2. Inserción de servicios con política de datos centralizada

El encadenamiento de servicios de Cisco SDWAN es inherentemente muy flexible y totalmente automatizado. En una configuración WAN heredada. Si tiene que insertar un firewall en la ruta de flujo de tráfico específico, normalmente se asocia a una gran cantidad de configuraciones manuales en cada salto. Por el contrario, el proceso de inserción del servicio Cisco SD-WAN es tan sencillo como hacer coincidir el tráfico interesante con un control centralizado o una política de datos, establecer el servicio de firewall como un salto siguiente y, a continuación, aplicar la política a una lista de sitios de destino a través de una única transacción de protocolo de configuración de red (NETCONF) desde Cisco SDWAN Manager al controlador Cisco SDWAN.

Estos son los pasos para insertar un firewall como servicio en nuestro ejemplo de configuración:

1. Defina el firewall como un servicio en los dispositivos DC cEdge. Esto se puede lograr mediante plantillas de funciones de VPN, así como inicio de sesión directo en los dispositivos. El seguimiento en el servicio está habilitado de forma predeterminada, lo que significa que si el firewall de DC se vuelve inalcanzable desde el router principal DC SDWAN cEdge1, todo el servicio se desactivará y el tráfico se replegará al router secundario cEdge2 de DC.

2. Crear y aplicar una política de datos centralizada para insertar el servicio de FW en la ruta de tráfico bidireccionalmente.

Configuración (Con Inserción De Servicio)

Configurado en routers DC SDWAN:

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

La configuración anterior en los routers SDWAN del DC define un servicio del tipo 'Firewall' que se anuncia al controlador SDWAN de Cisco. El router SDWAN del DC deja de anunciar lo mismo cuando el alcance del servicio de firewall se apaga o el propio firewall se desactiva.

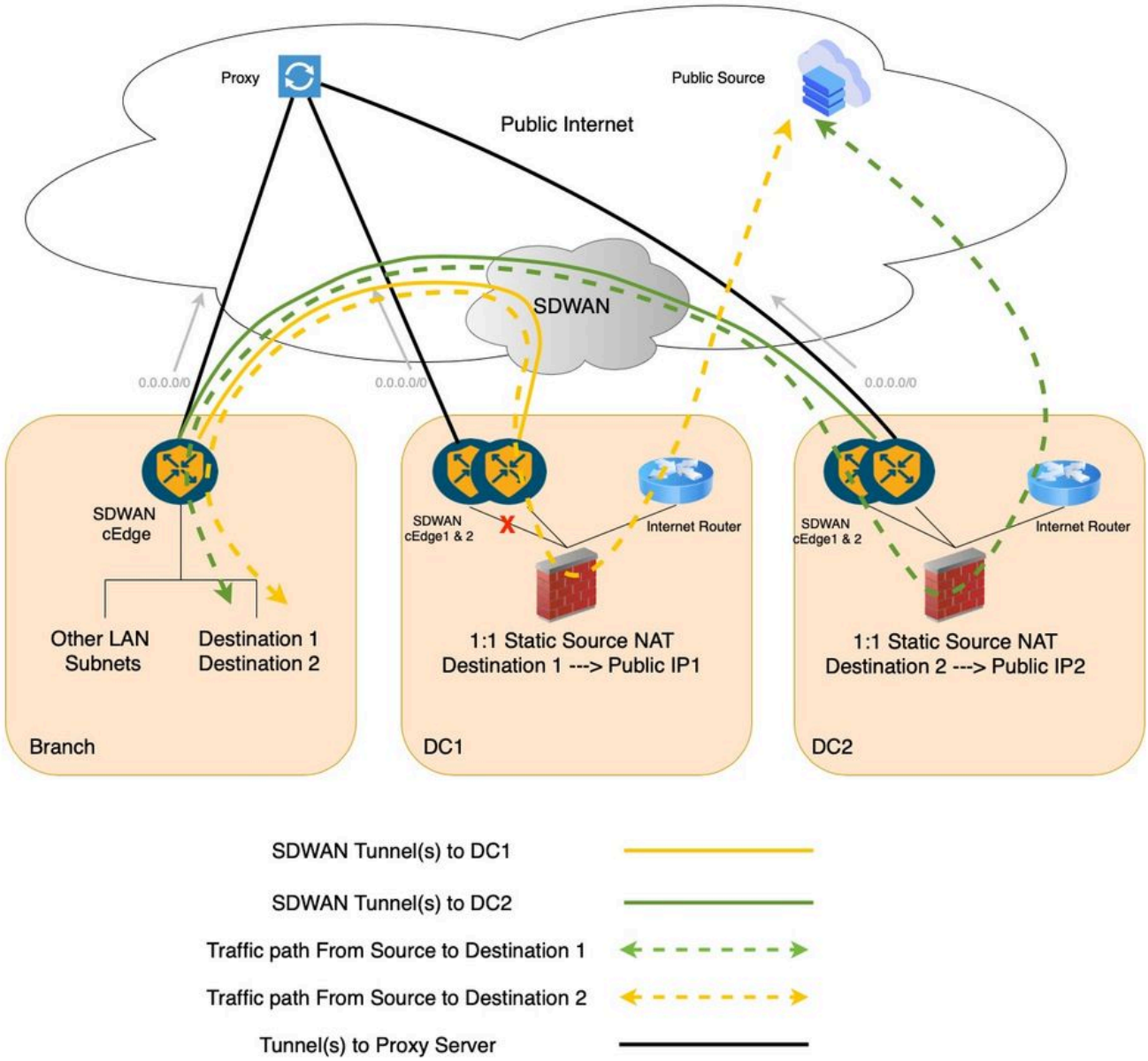
Una política de encadenamiento de servicios se define como aplicada en el router SDWAN de sucursal desde la dirección de servicio:

```
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
!
```

## Flujo de tráfico con inserción de servicios (caso de fallo de enlace LAN del router DC SDWAN 1)

El tráfico conmuta por error al router DC SDWAN 2 en caso de que se produzca un fallo en el enlace LAN del router DC SDWAN 1.




Estos requisitos previos de políticas o listas predefinidas se definen en el Cisco Catalyst SDWAN Manager como se muestra a modo de referencia:

```
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
  !
  !
```

## Detalles del flujo de tráfico para una mejor comprensión

Flujo de tráfico exterior a interior

Origen de Internet (MS Teams) > DC1 FW (NAT) > DC1 cEdge01 > Branch cEdge01 > Server Subnet 1.

Origen de Internet (MS Teams) > DC2 FW (NAT) > DC2 cEdge01 > Branch cEdge01 > Server Subnet 2.

Para este tráfico, la influencia se realiza en los saltos respectivos de la siguiente manera:

Fuente de Internet (MS Teams) > DC1 FW.

Fuente de Internet (MS Teams) > DC2 FW.

Los DC1 y DC2 anuncian los respectivos grupos de IP públicas a Internet a través del CPE de Internet en los DC.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

Routing de firewall para subred interna.

DC1 cEdge01 > Branch cEdge01.

DC2 cEdge01 > Branch cEdge01.

Routing SDWAN de Cisco mediante superposición de protocolo de gestión de superposición

(OMP).

Branch cEdge01 > Server Subnet 1.

Branch cEdge01 > Server Subnet 2.

Routing de router de sucursal para subred interna.

Flujo de tráfico interno a externo

Subred de servidor 1 > Sucursal cEdge 01 > DC1 cEdge01 > DC1 FW (NAT) > Origen de Internet (MS Teams).

Subred de servidor 2 > Sucursal cEdge 01 > DC2 cEdge01 > DC2 FW (NAT) > Origen de Internet (MS Teams).

Para este tráfico, la influencia se realiza en los saltos respectivos de la siguiente manera:

Server Subnet 1 (Subred de servidor 1) > Branch Edge 01.

Server Subnet 2 > Branch Edge 01.

Routing interno desde el lado del servidor.

Branch cEdge 01 > DC1 cEdge01.

Branch cEdge 01 > DC2 cEdge01.

Uso de la política de datos centralizada (encadenamiento de servicios) para influir en la ruta del tráfico.

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

Uso de las etiquetas de servicio para influir en la ruta de tráfico desde SDWAN cEdge a los respectivos FW en los DC.

DC1 FW (NAT) > Origen de Internet (MS Teams).

DC2 FW (NAT) > Origen de Internet (MS Teams).

El tráfico IP privado originado desde el servidor es NAT'ed para salir del FW para alcanzar Internet vía CPE.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).