Insertion de service à l'aide de la politique de données centralisée : Un exemple d'utilisation unique de manoeuvre de trafic

Table des matières

Introduction

Ce document décrit un exemple de scénario dans lequel le Service Chaining est utilisé pour contrôler le flux du trafic entrant d'Internet vers les serveurs hébergés sur le site de la filiale SDWAN.

Informations générales

Le document montre également qu'en utilisant le chaînage de services, il est facile de suivre la défaillance de la liaison LAN du data center (DC) pour notifier le routeur SDWAN de la filiale de modifier le chemin du trafic à l'aide de la stratégie de données, ce qui n'est pas possible autrement et sans quoi le trafic peut facilement créer des trous noirs dans le DC.

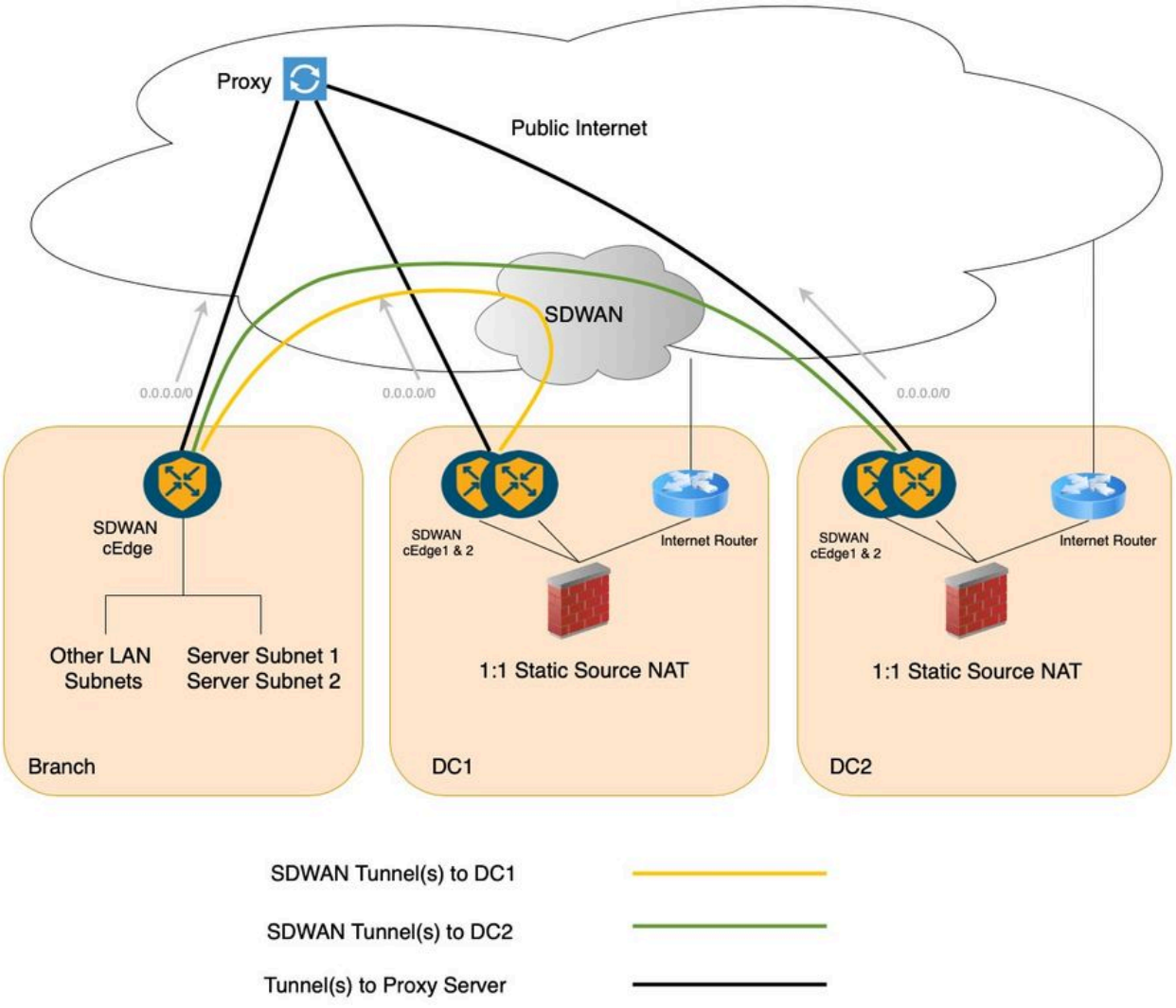
Le trafic entrant ici est acheminé via les pare-feu DC pour la gestion et la sécurité.

Exemple de topologie

Un déploiement SDWAN standard avec une configuration à double data center et un site de filiale a été envisagé pour illustrer ce scénario, comme illustré dans le schéma suivant. Il peut y avoir plusieurs branches, cependant, par souci de simplicité, une seule a été représentée. Les data

centers et les filiales communiquent via Secure SDWAN Overlay, c'est-à-dire via les tunnels SDWAN Secure IPSec. Dans cette configuration existante, les contrôleurs de domaine et le site de la succursale disposent d'un ou de plusieurs tunnels vers les serveurs proxy dans le service VRF (Virtual Routing and Forwarding) et la route par défaut dans le service VRF/VPN (Virtual Private Network) pointe vers ce proxy.

Cette configuration de topologie se compose d'un site de filiale où deux sous-réseaux de serveurs, le sous-réseau de serveur 1 et le sous-réseau de serveur 2 sont hébergés. Il existe deux data centers, où chacun des pare-feu de data center effectue une traduction d'adresses de réseau (NAT) statique 1:1 afin de permettre au sous-réseau du serveur de filiale respectif d'être accessible à partir d'Internet. Afin d'être précis, le pare-feu du data center 1 effectue la NAT statique 1:1 pour le sous-réseau 1 du serveur et le pare-feu du data center 2 effectue la même opération pour le sous-réseau 2 du serveur.



Besoin du client

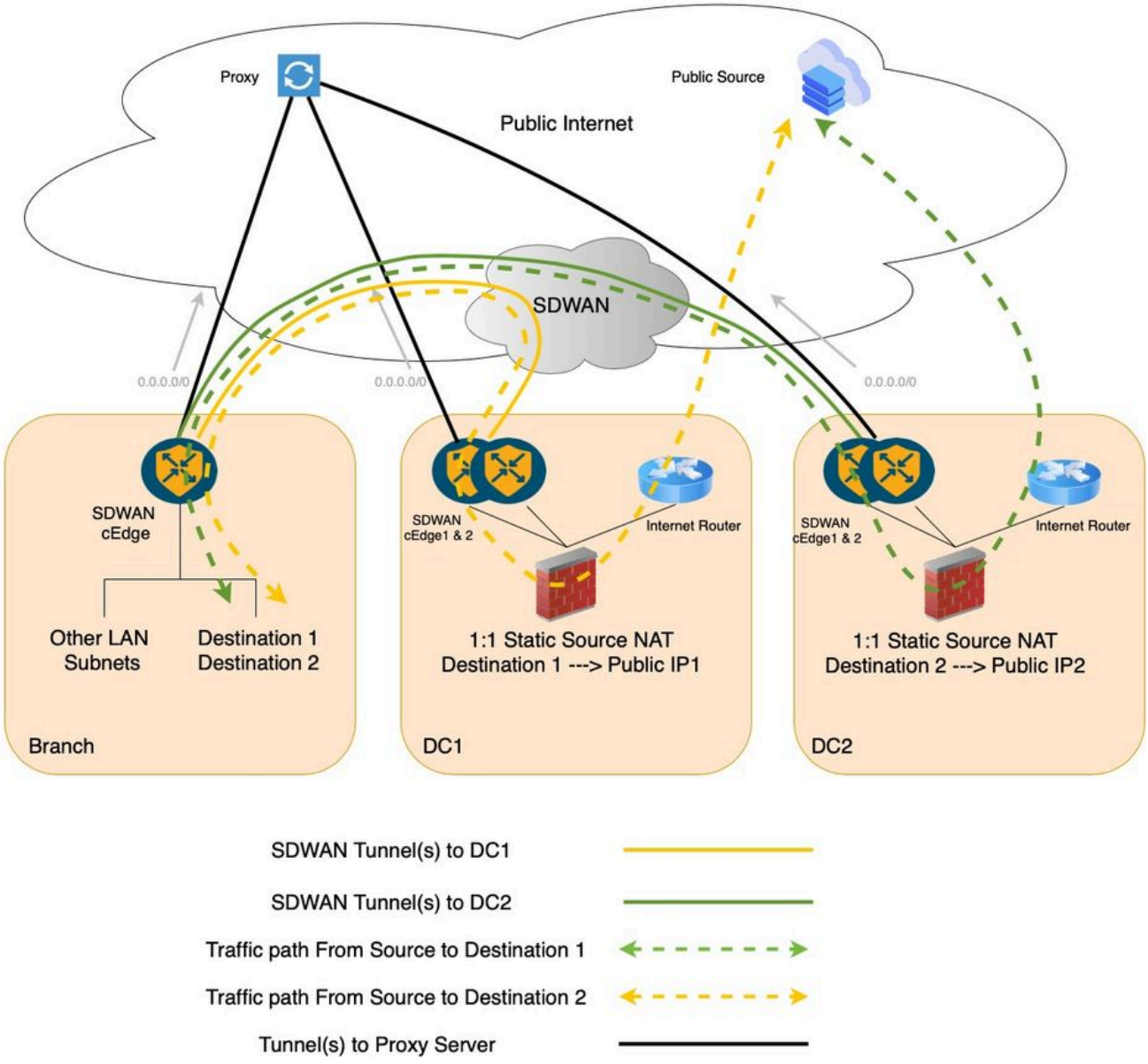
Avec la configuration précédente à l'esprit, les exigences du client peuvent être comme mentionné :

- Les applications publiques telles que MS Teams doivent accéder à ces serveurs hébergés

dans Branch. Comme indiqué précédemment, la disponibilité de pare-feu avec état dans les contrôleurs de domaine fait que le client demande à ce qu'ils soient utilisés au lieu d'une connexion entrante directe au site de la filiale.

- Le sous-réseau de serveur 1 de Branch doit être accessible via DC1 et le sous-réseau de serveur 2 de Branch doit être accessible via DC2 à partir d'Internet.
- Aucune adresse IP publique ne doit être routée au sein du réseau du client.
- Les sous-réseaux 1 et 2 du serveur hébergé par la filiale sont configurés avec des adresses IP privées et la traduction d'adresses IP privées en adresses IP publiques doit avoir lieu dans les FW du data center respectifs.
- Il ne doit pas y avoir de modifications de routage sous-jacentes.

Remarque : Si aucune modification n'est apportée au flux de trafic dans le data center ou le site de la filiale, le trafic de transfert provenant d'Internet passe par les pare-feu du data center afin d'atteindre les serveurs du site de la filiale. D'autre part, le trafic de retour passera directement par le proxy du routeur SDWAN de la filiale (en utilisant la route par défaut) afin d'atteindre la source Internet. Il s'agit d'un flux de trafic asymétrique.



Solutions possibles

Il existe deux solutions possibles pour les besoins antérieurs :

1. Ingénierie de trafic personnalisée avec politique de données centralisée où le trafic crée des trous noirs en cas de défaillance de la liaison LAN CC.
2. Insertion de service avec politique de données centralisée lorsque le trafic ne fait pas de trou noir en cas de défaillance de la liaison LAN DC.

1. Ingénierie de trafic personnalisée avec politique de données centralisée

Si des politiques de données d'ingénierie de trafic personnalisées sont prises en compte dans le cadre de la politique de données centralisées, l'une pour la filiale et l'autre pour le data center, la politique de données de filiale envoie le trafic de filiale au data center à l'aide de tlocs distants et la deuxième politique de données achemine le flux dans le data center depuis le cEdge vers le pare-feu (FW). Cependant, avec l'option de tloc distant configurée dans la filiale, le routeur SDWAN de

filiale ignore la défaillance de la liaison LAN du routeur SDWAN 1 du data center. En d'autres termes, si la liaison LAN du routeur SDWAN CC 1 tombe en panne, le routeur Branch n'en est pas conscient et transfère toujours ce trafic au routeur SDWAN CC 01. D'où la facilité avec laquelle le trafic crée des trous noirs au niveau du routeur SDWAN CC 1.

Configuration (avec politique de données personnalisée)

Appliqué sur le routeur SDWAN CC à partir de la direction du tunnel :

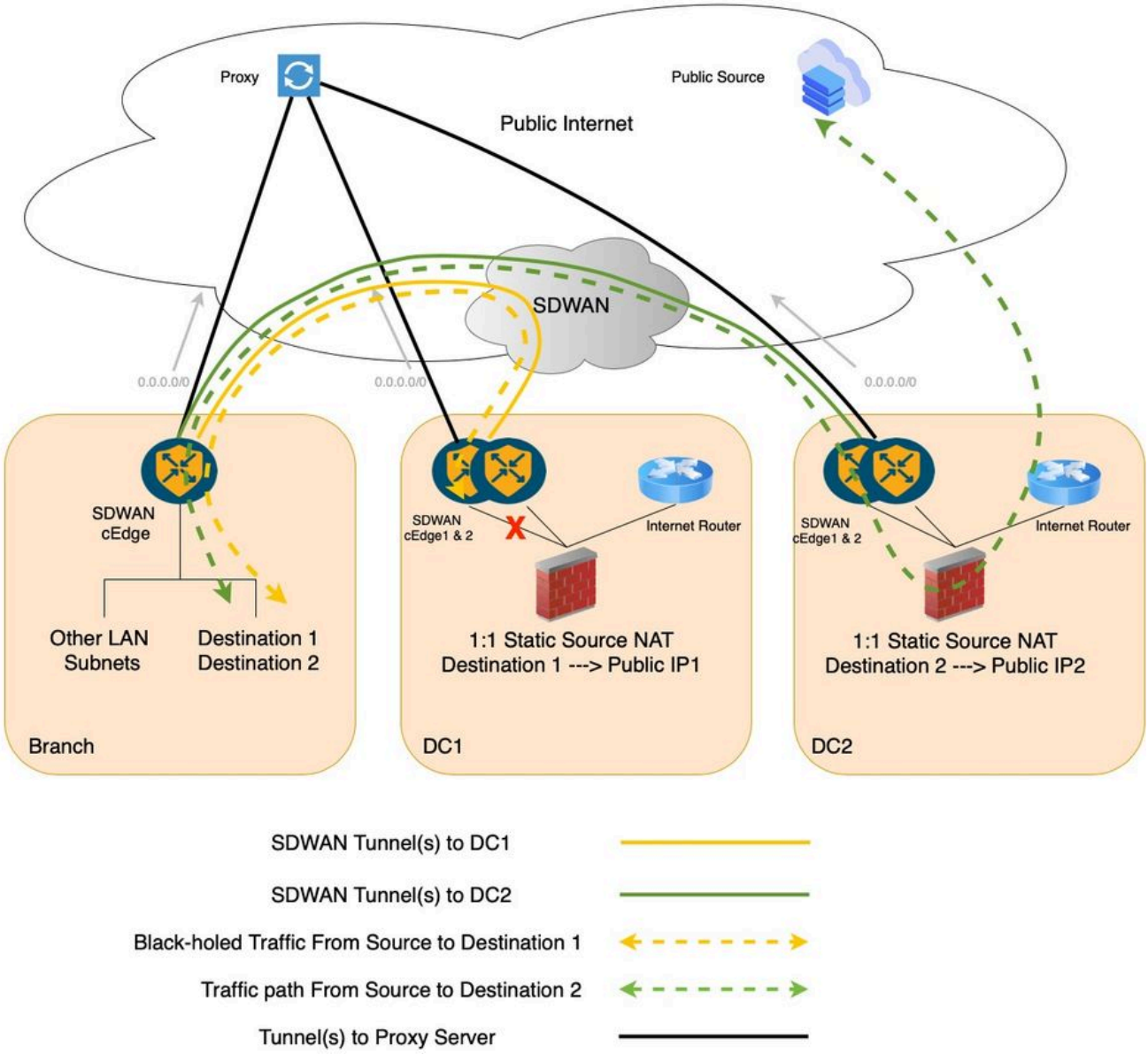
```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
       next-hop <Firewall_IP>
      !
     !
```

Appliqué sur le routeur SDWAN de filiale depuis la direction de service :

```
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
  !
```

Flux de trafic avec politique de données personnalisée (cas de défaillance de liaison LAN du routeur SDWAN DC 1)

Les trous noirs du trafic au niveau du routeur SDWAN CC 1 en cas de défaillance de la liaison LAN du routeur SDWAN CC 1.



2. Insertion de service avec politique de données centralisée

Le chaînage des services Cisco SDWAN est par nature très flexible et entièrement automatisé. Dans une configuration WAN héritée. Si vous devez insérer un pare-feu dans le chemin d'un flux de trafic spécifique, il est généralement associé à de nombreuses configurations manuelles à chaque saut. En revanche, le processus d'insertion de service SD-WAN de Cisco est aussi simple que de faire correspondre le trafic intéressant avec un contrôle centralisé ou une politique de données, de définir le service de pare-feu comme saut suivant, puis d'appliquer la politique à une liste de sites cibles via une transaction NETCONF (Network Configuration Protocol) unique du gestionnaire SDWAN de Cisco au contrôleur SDWAN de Cisco.

Voici les étapes à suivre pour insérer un pare-feu en tant que service dans notre exemple de configuration :

1. Définissez le pare-feu en tant que service sur les périphériques DC cEdge. Cela peut être réalisé en utilisant des modèles de fonctionnalités VPN ainsi qu'une connexion directe aux périphériques. Le suivi sur le service est activé par défaut, ce qui signifie que si le pare-feu DC

devient inaccessible à partir du routeur principal DC SDWAN cEdge1, l'ensemble du service sera désactivé et le trafic reviendra au routeur secondaire cEdge2 de DC.

2. Créez et appliquez une politique de données centralisée pour insérer le service FW dans le chemin de trafic bidirectionnellement.

Configuration (avec insertion de service)

Configuré sur les routeurs SDWAN CC :

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

La configuration précédente des routeurs SDWAN DC définit un service de type « pare-feu » qui est annoncé au contrôleur SDWAN Cisco. Le routeur SDWAN de data center cesse d'annoncer la même chose lorsque l'accessibilité au service de pare-feu s'arrête ou que le pare-feu lui-même s'arrête.

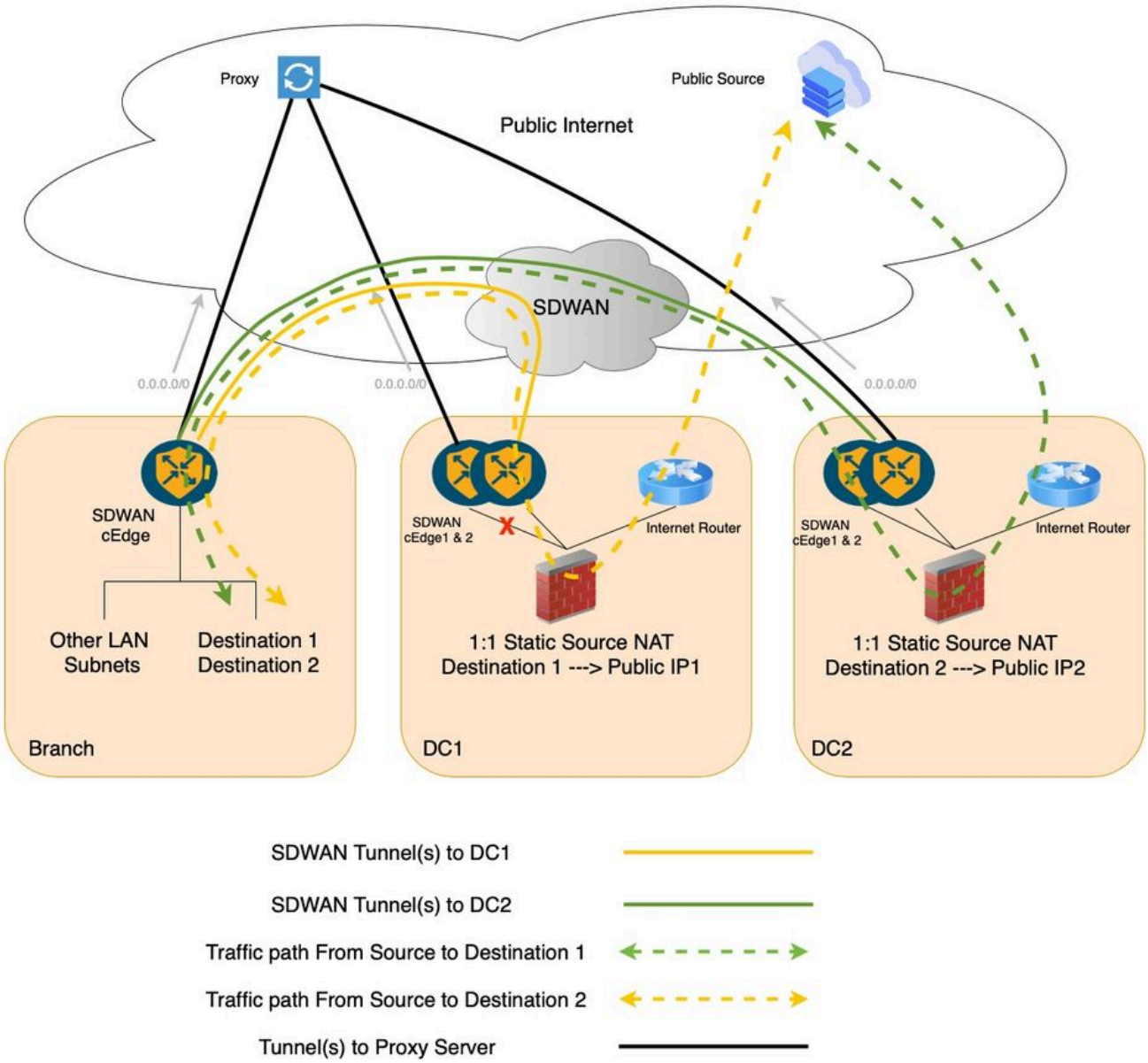
Une stratégie de chaînage de services est définie comme étant appliquée sur le routeur SDWAN de la filiale depuis la direction de service :

```
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
  !
```

Flux de trafic avec insertion de service (cas de défaillance de la liaison LAN du routeur SDWAN 1 CC)

Le trafic bascule vers le routeur SDWAN CC 2 en cas de défaillance de la liaison LAN du routeur

SDWAN CC 1.



Les conditions préalables ou listes prédéfinies suivantes sont définies sur le Cisco Catalyst SDWAN Manager, comme indiqué à titre de référence :

```
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
!
!
```

Détails du flux de trafic pour une meilleure compréhension

Flux du trafic extérieur vers le trafic intérieur

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

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

Pour ce trafic, l'influence se fait dans les sauts respectifs comme suit :

Source Internet (MS Teams) > DC1 FW.

Source Internet (MS Teams) > DC2 FW.

Les DC1 et DC2 annoncent le pool d'adresses IP publiques respectif à Internet via l'équipement d'abonné Internet au niveau des DC.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

Routage du pare-feu pour le sous-réseau interne.

DC1 cEdge01 > Branch cEdge01.

DC2 cEdge01 > Branch cEdge01.

Routage Cisco SDWAN via la superposition OMP (Overlay Management Protocol).

BranchEdge01 > Serveur Sous-réseau 1.

BranchEdge01 > Sous-réseau du serveur 2.

Routage du routeur de filiale pour le sous-réseau interne.

Flux de trafic interne vers externe

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

Server Subnet 2 > Branch cEdge 01 > DC2 cEdge 01 > DC2 FW (NAT) > Internet Source (MS Teams).

Pour ce trafic, l'influence se fait dans les sauts respectifs comme suit :

Sous-réseau 1 du serveur > Branch Edge 01.

Sous-réseau 2 du serveur > BranchEdge 01.

Routage interne côté serveur.

Branch cEdge 01 > DC1 cEdge 01.

Branch cEdge 01 > DC2 cEdge 01.

Utilisation de la stratégie de données centralisée (chaînage de services) pour influencer le chemin du trafic.

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

Utilisation des étiquettes de service afin d'influencer le chemin du trafic depuis SDWAN cEdge vers le pare-feu correspondant au niveau des data centers.

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

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

Le trafic provenant du serveur IP privé est soumis à la fonction NAT pour sortir du pare-feu afin d'accéder à Internet via CPE.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.