Service-invoeging met behulp van gecentraliseerd gegevensbeleid: een unieke verkeersmanoeuvreerbare use-case

Inhoud

Inleiding

In dit document wordt een voorbeeldscenario beschreven waarbij Service Chaining wordt gebruikt om de stroom van inkomend verkeer van internet naar servers op de SDWAN-vestigingssite te beheren.

Achtergrondinformatie

Het document laat ook zien dat door het gebruik van Service Chaining hoe het datacenter (DC) LAN link Failure kan gemakkelijk worden gevolgd om de Branch SDWAN Router op de hoogte van het verkeerspad met behulp van Datapopolicy, die anders niet mogelijk is geweest en zonder welke het verkeer gemakkelijk zwarte gaten in de DC te veranderen.

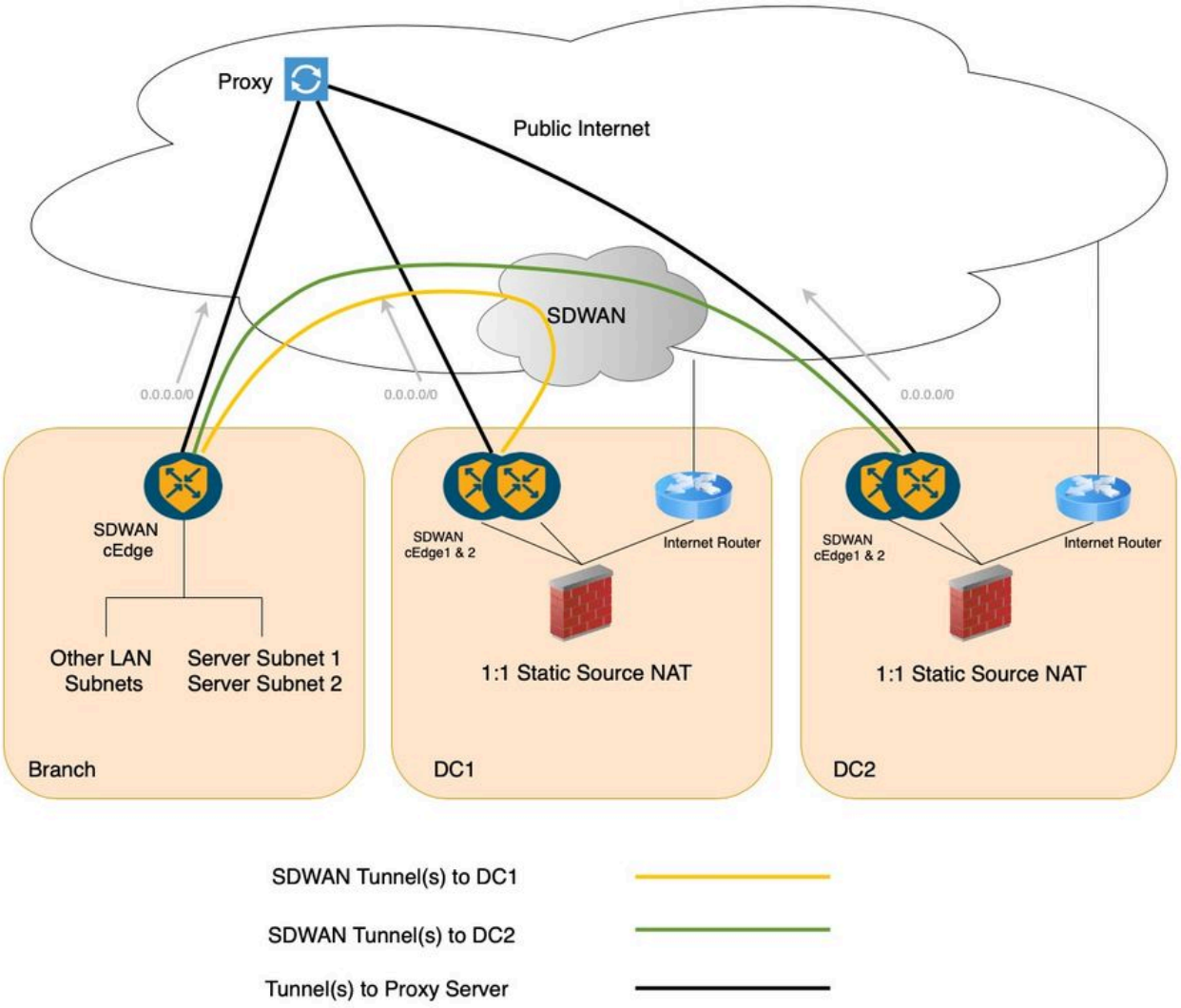
Het inkomende verkeer wordt hier gerouteerd via de DC Firewalls voor beheer en beveiliging.

Voorbeeldtopologie

Er is een standaard SDWAN-implementatie met dubbele DC-installatie en een aftakking overwogen om dit scenario weer te geven, zoals in het volgende diagram wordt weergegeven. Er kunnen echter meerdere takken zijn, omwille van de eenvoud is er slechts één afgebeeld. De DC's

en vestigingen communiceren via Secure SDWAN Overlay, dat wil zeggen via de SDWAN Secure IPSec-tunnels. In deze bestaande configuratie hebben zowel de DC's als de Branch-site tunnel(s) naar de proxyservers in de service Virtual Routing and Forwarding (VRF) en de standaardroute in de service VRF / Virtual Private Network (VPN) wijst naar deze proxy.

Deze topologieset bestaat uit een vertakte site waar twee subnetten van servers, Server Subnet 1 en Server Subnet 2 worden gehost. Er zijn twee datacenters, waar elk van de firewalls van het datacenter 1:1 statische netwerkadresvertaling (NAT) uitvoert om het respectieve subnet van de brancheserver via internet bereikbaar te maken. Om precies te zijn, voert Data Center 1 Firewall de 1:1 statische NAT uit voor Server Subnet 1 en voert Data Center 2 Firewall hetzelfde uit voor Server Subnet 2.



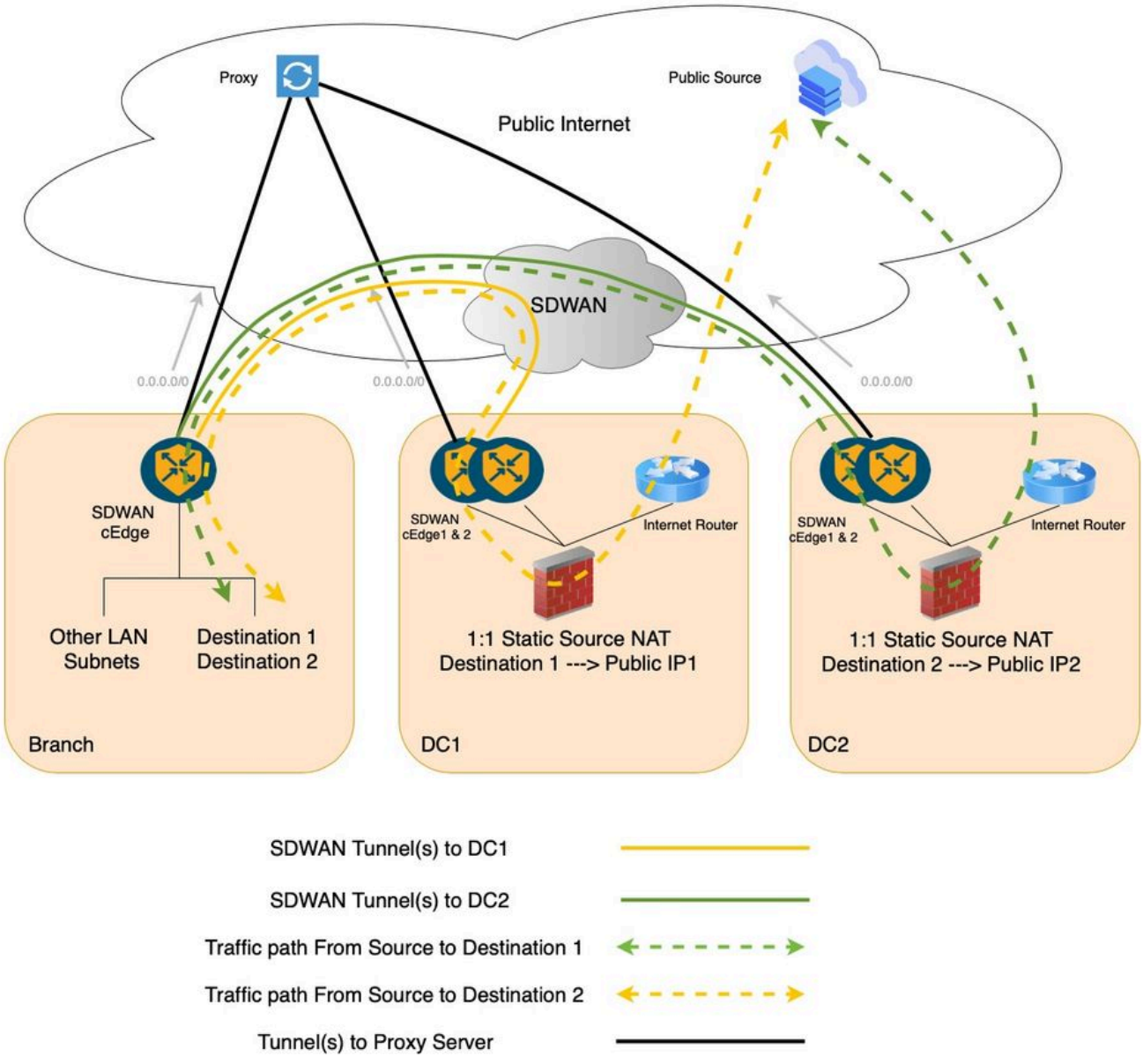
klantbehoefte

Met de eerdere installatie in het achterhoofd kan de vereiste van de klant worden vermeld als:

- Openbare toepassingen zoals MS Teams hebben toegang tot deze servers die in Branch worden gehost. Zoals eerder vermeld, zorgt de beschikbaarheid van stateful FW's in de DC's ervoor dat de klant vraagt om ze te gebruiken in plaats van directe inkomende verbinding met de vestiging.

- Het Server Subnet 1 in de Branch moet bereikbaar zijn via DC1 en het Server Subnet 2 in de Branch moet bereikbaar zijn via DC2 vanaf internet.
- Openbare IP-adressen mogen niet binnen het klantennetwerk worden gerouteerd.
- De subnetten 1 en 2 van de door de branch gehoste server worden geconfigureerd met privé-IP's en de vertaling van privé naar publiek IP moet plaatsvinden in de respectieve DC-FW's.
- Er mogen geen onderliggende routeringswijzigingen zijn.

Opmerking: Als er geen wijzigingen zijn aangebracht in de verkeersstroom op de DC- of Branch-site, gaat het doorgestuurde verkeer van internet door de DC Firewalls om de servers op de Branch-site te bereiken. Aan de andere kant zal het retourverkeer rechtstreeks door de Proxy bij Branch SDWAN-router gaan (met behulp van de standaardroute) om de internetbron te bereiken. Dit is een asymmetrische verkeersstroom.



Mogelijke oplossingen

Er zijn twee mogelijke oplossingen voor de eerdere vereisten:

1. Aangepaste verkeerstechniek met gecentraliseerd gegevensbeleid waarbij het verkeer zwarte gaten vertoont in het geval van een storing in de DC LAN-verbinding.
2. Service-invoeging met gecentraliseerd gegevensbeleid waarbij het verkeer geen zwart gat maakt in het geval van een storing in de DC LAN-verbinding.

1. Custom Traffic Engineering met gecentraliseerd gegevensbeleid

Als het gegevensbeleid voor aangepaste verkeerstechniek in het kader van het beleid voor gecentraliseerde gegevens wordt overwogen, een voor de tak en een andere voor de DC, verzendt het gegevensbeleid voor de tak het verkeer van de tak naar de DC met behulp van externe tlocs en routeert het tweede gegevensbeleid de stroom binnen DC verder van de cEdge naar de firewall (FW). Maar als de optie voor extern gebruik is geconfigureerd in de Branch, is de Branch SDWAN-router niet op de hoogte van het falen van de LAN-verbinding van de DC SDWAN Router 1. Dat wil zeggen, als de LAN-verbinding op de DC SDWAN Router 1 mislukt, is de Branch-router zich niet bewust en stuurt hij dat verkeer nog steeds door naar de DC SDWAN Router 01. Vandaar het verkeer gemakkelijk zwarte gaten bij DC SDWAN Router 1.

Configuratie (met aangepast gegevensbeleid)

Toegepast op DC SDWAN Router uit-tunnelrichting:

```
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>
      !
     !
```

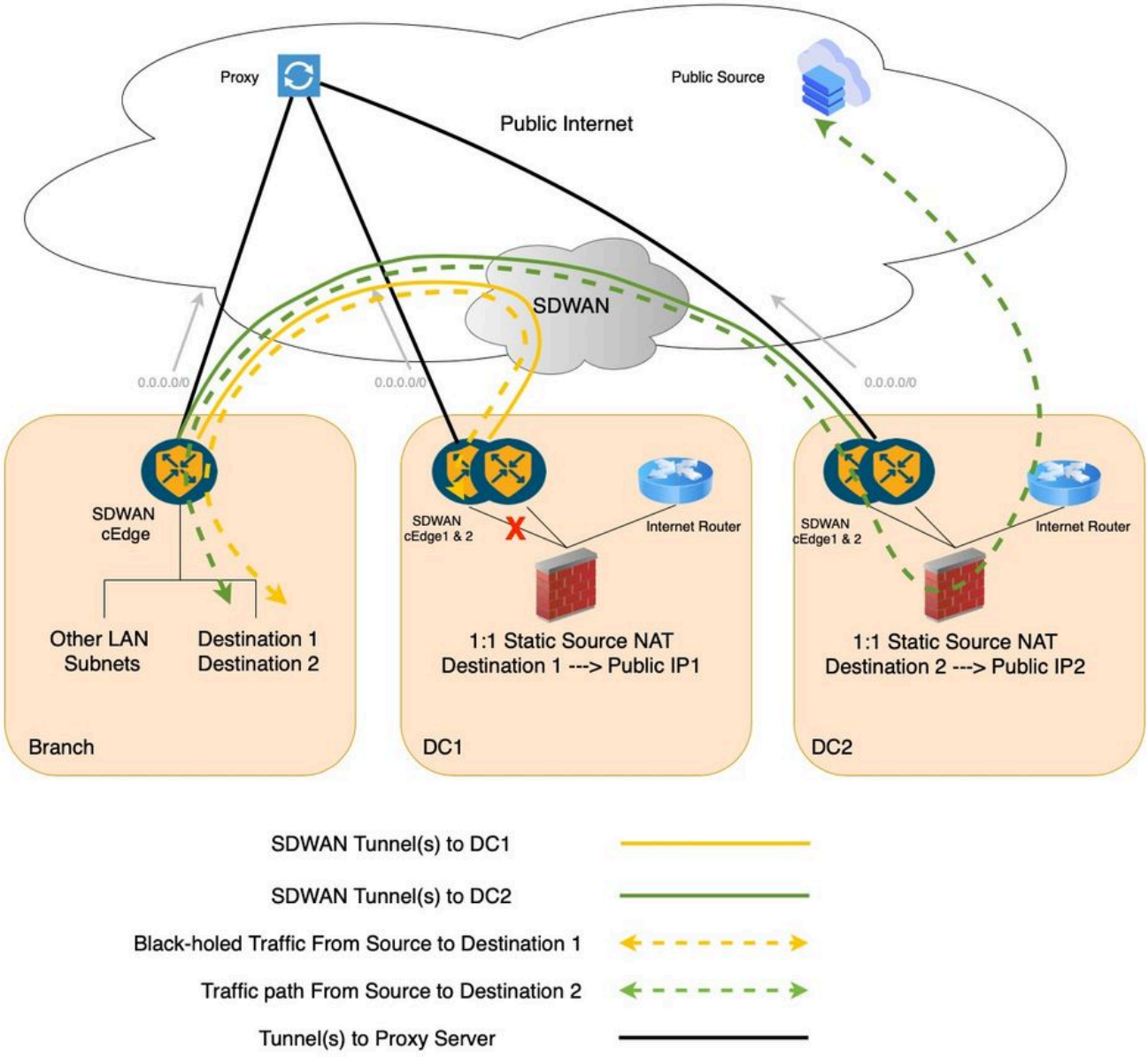
Toegepast op Branch SDWAN-router vanuit servicerichting:

```
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
!
```

Verkeersstroom met aangepast gegevensbeleid (DC SDWAN Router 1LAN Link Failure Case)

De zwarte gaten in het verkeer bij DC SDWAN Router 1 in het geval van DC SDWAN Router 1 LAN-verbindingsfout.



2. Service-invoeging met gecentraliseerd gegevensbeleid

Cisco SDWAN service chaining is inherent zeer flexibel en volledig geautomatiseerd. In een verouderde WAN-configuratie. Als u een firewall in het pad van een specifieke verkeersstroom moet plaatsen, wordt deze meestal geassocieerd met veel handmatige configuratie bij elke hop. Het Cisco SD-WAN-serviceinvoegproces is daarentegen net zo eenvoudig als het matchen van interessant verkeer met een gecentraliseerd besturings- of gegevensbeleid, het instellen van de firewallservice als een volgende stap en het vervolgens toepassen van het beleid op een lijst met doellocaties via een enkele Network Configuration Protocol (NETCONF) -transactie van de Cisco SDWAN Manager naar de Cisco SDWAN Controller.

Hier zijn de stappen voor het invoegen van een firewall als een service in ons configuratievoorbeeld:

1. Firewall definiëren als een service op de DC cEdge-apparaten. Dit kan worden bereikt met behulp van VPN-functiesjablonen en directe aanmelding bij de apparaten. De tracking op de service is standaard ingeschakeld, wat betekent dat als de DC Firewall onbereikbaar wordt vanaf de primaire DC SDWAN-router cEdge1, de hele service wordt uitgeschakeld en het verkeer terugvalt naar de secundaire router cEdge2 van DC.

2. Een gecentraliseerd gegevensbeleid maken en toepassen om de FW-service bi-directioneel in het verkeerspad in te voegen.

Configuratie (met service-invoeging)

Geconfigureerd op DC SDWAN Routers:

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

De eerdere configuratie bij DC SDWAN Routers definieert een service van het type 'Firewall' die wordt geadverteerd aan de Cisco SDWAN Controller. De DC SDWAN-router stopt met adverteren wanneer de bereikbaarheid van de firewallservice afgaat of de firewall zelf afneemt.

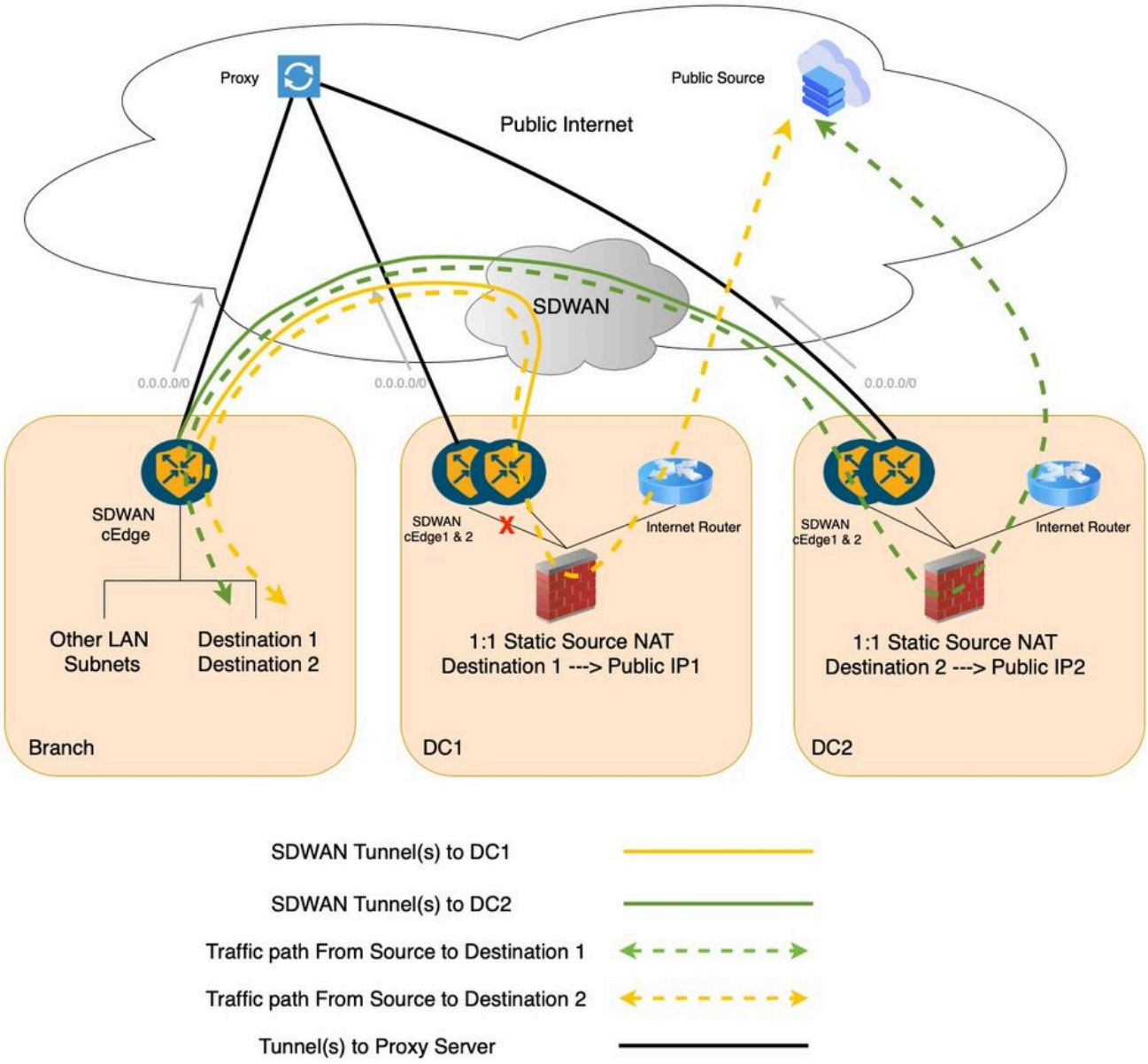
Een service-chaining-beleid wordt gedefinieerd als toegepast op Branch SDWAN Router vanuit de servicerichting:

```
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
!
```

Verkeersstroom met service-invoeging (DC SDWAN Router 1 LAN Link Failure Case)

Het verkeer kan niet worden overgezet naar DC SDWAN Router 2 in het geval van een storing in de LAN-verbinding van DC SDWAN Router 1.



Deze beleidsvereisten of vooraf gedefinieerde lijsten worden gedefinieerd in Cisco Catalyst SDWAN Manager, zoals weergegeven ter referentie:

```
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
  !
  !
```

Verkeersstroomdetails voor een beter begrip

Van buiten naar binnen verkeersstroom

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.

Voor deze verkeersbeïnvloeding wordt in de betreffende hop als volgt gedaan:

Internet Source (MS Teams) > DC1 FW.

Internet Source (MS Teams) > DC2 FW.

De DC1 en DC2 adverteren de respectievelijke openbare IP-pool via het internet CPE op DC's.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

Firewallroutering voor intern subnet.

DC1 cEdge01 > Branch cEdge01.

DC2 cEdge01 > Branch cEdge01.

Cisco SDWAN Routing via Overlay Management Protocol (OMP) overlay.

Branch cEdge01 > Serversubnet 1.

Branch cEdge01 > Server Subnet 2.

Branch Router routering voor intern subnet.

Binnen naar buiten verkeersstroom

Server Subnet 1 > Branch cEdge 01 > DC1 cEdge01 > DC1 FW (NAT) > Internet Source (MS Teams).

Server Subnet 2 > Branch cEdge 01 > DC2 cEdge01 > DC2 FW (NAT) > Internet Source (MS Teams).

Voor deze verkeersbeïnvloeding wordt in de betreffende hop als volgt gedaan:

Server Subnet 1 > Branch cEdge 01.

Server Subnet 2 > Branch cEdge 01.

Interne routering vanaf de server.

Branch cEdge 01 > DC1 cEdge01.

Branch cEdge 01 > DC2 cEdge01.

Het gebruik van gecentraliseerd gegevensbeleid (Service Chaining) om het verkeerspad te beïnvloeden.

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

Het gebruik van servicelabels om het verkeerspad van SDWAN cEdge naar de respectieve FW bij DC's te beïnvloeden.

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

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

Privé IP-bronverkeer van Server is NAT'ed om de FW te verlaten om via CPE internet te bereiken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.