Serviceeinfügung mithilfe einer zentralisierten Datenrichtlinie: Ein einzigartiger Fallbeispiel für das Manövrieren von Datenverkehr

Inhalt

Einleitung

In diesem Dokument wird ein Beispielszenario beschrieben, in dem die Serviceverkettung verwendet wird, um den Fluss des eingehenden Datenverkehrs aus dem Internet zu Servern zu steuern, die in der SDWAN-Außenstelle gehostet werden.

Hintergrundinformationen

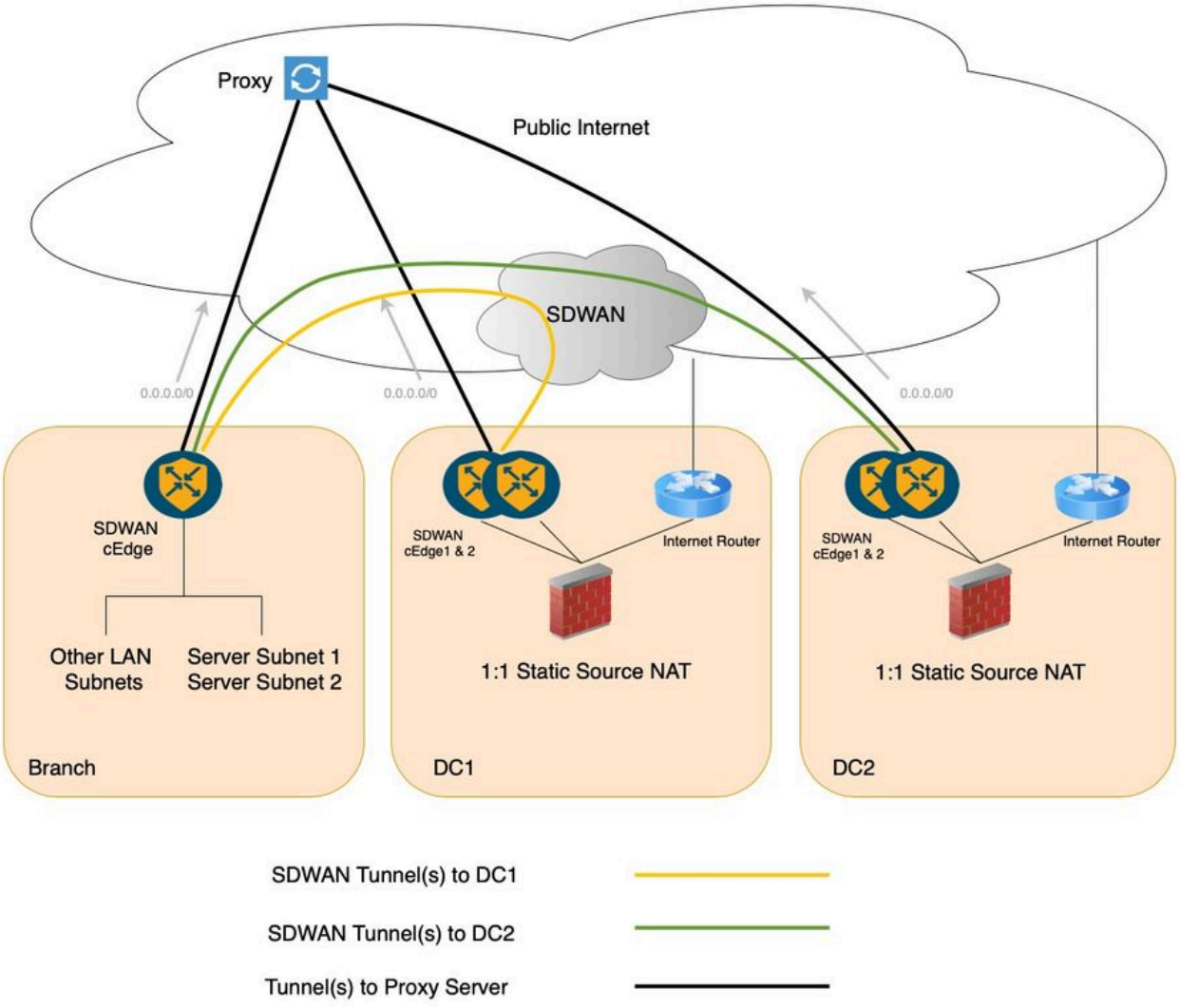
Das Dokument zeigt außerdem, dass durch die Verwendung von Service Chaining der LAN-Link im Rechenzentrum (DC) auf einfache Weise nachverfolgt werden kann, um den SDWAN-Router der Außenstelle zu benachrichtigen, den Datenverkehrspfad mithilfe der Datenrichtlinie zu ändern. Dies war andernfalls nicht möglich, und ohne diese lässt sich der Datenverkehr im Rechenzentrum leicht "Blackholes" (Blackholes) zuweisen.

Der eingehende Datenverkehr wird hier aus Verwaltungs- und Sicherheitsgründen durch die Firewalls des Rechenzentrums geleitet.

Beispieltopologie

Eine SDWAN-Standardbereitstellung mit dualer Rechenzentrums-Konfiguration und einer Außenstelle wurde in Betracht gezogen, um dieses Szenario wie im nächsten Diagramm dargestellt darzustellen. Es können mehrere Zweige vorhanden sein, jedoch ist der Einfachheit halber nur eine dargestellt. Die Rechenzentren und Zweigstellen kommunizieren über Secure SDWAN Overlay, d. h. über die SDWAN Secure IPSec-Tunnel. In dieser bestehenden Konfiguration verfügen sowohl die Rechenzentren als auch die Außenstellen über Tunnel zu den Proxyservern im Service Virtual Routing and Forwarding (VRF), und die Standardroute im Service VRF/Virtual Private Network (VPN) verweist auf diesen Proxy.

Diese Topologie-Konfiguration besteht aus einer Außenstelle, in der zwei Server-Subnetze, Server-Subnetz 1 und Server-Subnetz 2 gehostet werden. Es gibt zwei Rechenzentren, in denen jede der Rechenzentrums-Firewalls eine statische Network Address Translation (NAT) im Verhältnis 1:1 durchführt, damit das jeweilige Zweigstellen-Server-Subnetz vom Internet aus erreichbar ist. Die Firewall von Rechenzentrum 1 führt für das Server-Subnetz 1 die statische 1:1-NAT durch, und die Firewall von Rechenzentrum 2 führt für das Server-Subnetz 2 die gleiche NAT durch.



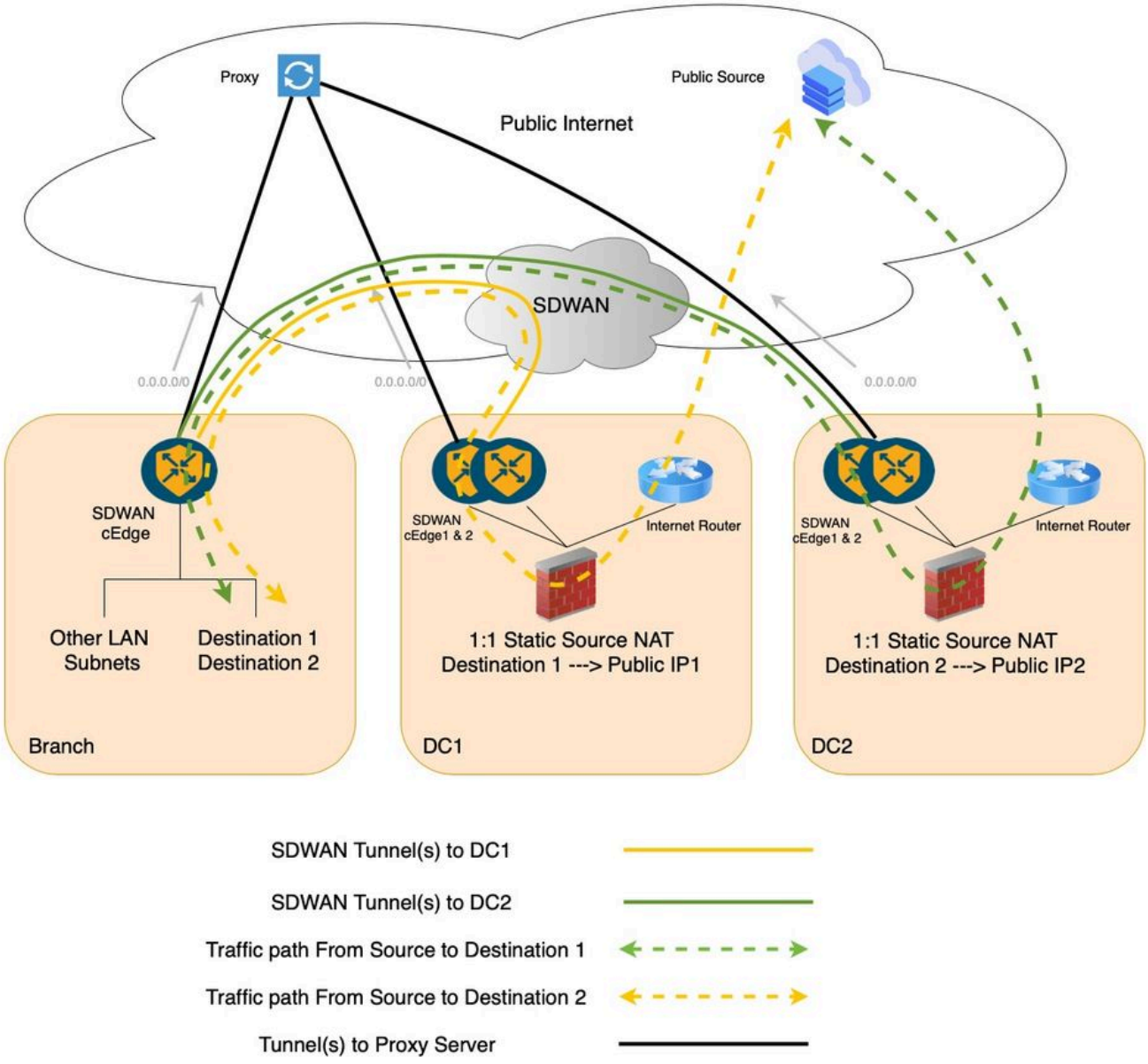
Kundenanforderungen

Wenn Sie die frühere Konfiguration berücksichtigen, kann die Anforderung des Kunden wie folgt

lauten:

- Öffentliche Anwendungen wie MS Teams müssen auf diese Server zugreifen, die in Zweigstellen gehostet werden. Wie bereits erwähnt, veranlasst die Verfügbarkeit von Stateful FWs in den Rechenzentren den Kunden, diese anstelle der direkten eingehenden Verbindung mit der Außenstelle zu verwenden.
- Das Server-Subnetz 1 in der Außenstelle muss über DC1 erreichbar sein, und das Server-Subnetz 2 in der Außenstelle muss über DC2 aus dem Internet erreichbar sein.
- Es darf keine öffentliche IP innerhalb des Kundennetzwerks geroutet werden.
- Die in der Außenstelle gehosteten Server-Subnetze 1 und 2 sind mit privaten IPs konfiguriert, und die Umwandlung von privater in öffentliche IP muss in den entsprechenden FWs des Rechenzentrums erfolgen.
- Es dürfen keine Änderungen am Underlay-Routing vorgenommen werden.

Anmerkung: Wenn keine Änderungen am Datenverkehrsfluss im Rechenzentrum oder in der Außenstelle vorgenommen werden, durchläuft der Weiterleitungsdatenverkehr aus dem Internet die Firewalls im Rechenzentrum, um die Server in der Außenstelle zu erreichen. Andererseits wird der zurückkehrende Datenverkehr direkt über den Proxy am SDWAN-Router der Außenstelle geleitet (unter Verwendung der Standardroute), um zur Internetquelle zu gelangen. Ein asymmetrischer Datenverkehrsfluss.



Mögliche Lösungen

Es gibt zwei mögliche Lösungen für die früheren Anforderungen:

1. Individuelles Traffic Engineering mit zentralisierter Datenrichtlinie, bei dem der Datenverkehr bei einem Ausfall der LAN-Verbindung im Rechenzentrum unterbrochen wird.
2. Serviceeinbindung mit zentralisierter Datenrichtlinie, bei der der Datenverkehr bei einem Ausfall der LAN-Verbindung im Rechenzentrum nicht ausfällt.

1. Benutzerdefinierte Datenverkehrsplanung mit zentralisierter Datenrichtlinie

Wenn benutzerdefinierte Datenverkehrsrichtlinien gemäß der Richtlinie für zentrale Daten berücksichtigt werden, eine für die Außenstelle und eine andere für das Rechenzentrum, sendet die Datenrichtlinie für die Außenstelle den Datenverkehr von der Außenstelle an das Rechenzentrum mithilfe von Remote-Datenpunkten, und die zweite Datenrichtlinie leitet den Datenfluss innerhalb des Rechenzentrums weiter vom cEdge zur Firewall (FW). Da jedoch die

Option "remote-tloc" in der Außenstelle konfiguriert ist, erkennt der SDWAN-Router der Außenstelle nicht, LAN-Verbindungsausfall bei SDWAN-Router 1 des Rechenzentrums Das heißt, wenn die LAN-Verbindung am SDWAN-Router 1 des Rechenzentrums ausfällt, ist der Zweigstellen-Router nicht informiert und leitet diesen Datenverkehr weiterhin an den SDWAN-Router 01 des Rechenzentrums weiter. Daher kann der Datenverkehr leicht zu Schwarzen Löchern am SDWAN-Router 1 des Rechenzentrums führen.

Konfiguration (mit benutzerdefinierter Datenrichtlinie)

Anwendung auf DC SDWAN-Router aus Tunnelrichtung:

```
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>
      !
     !
```

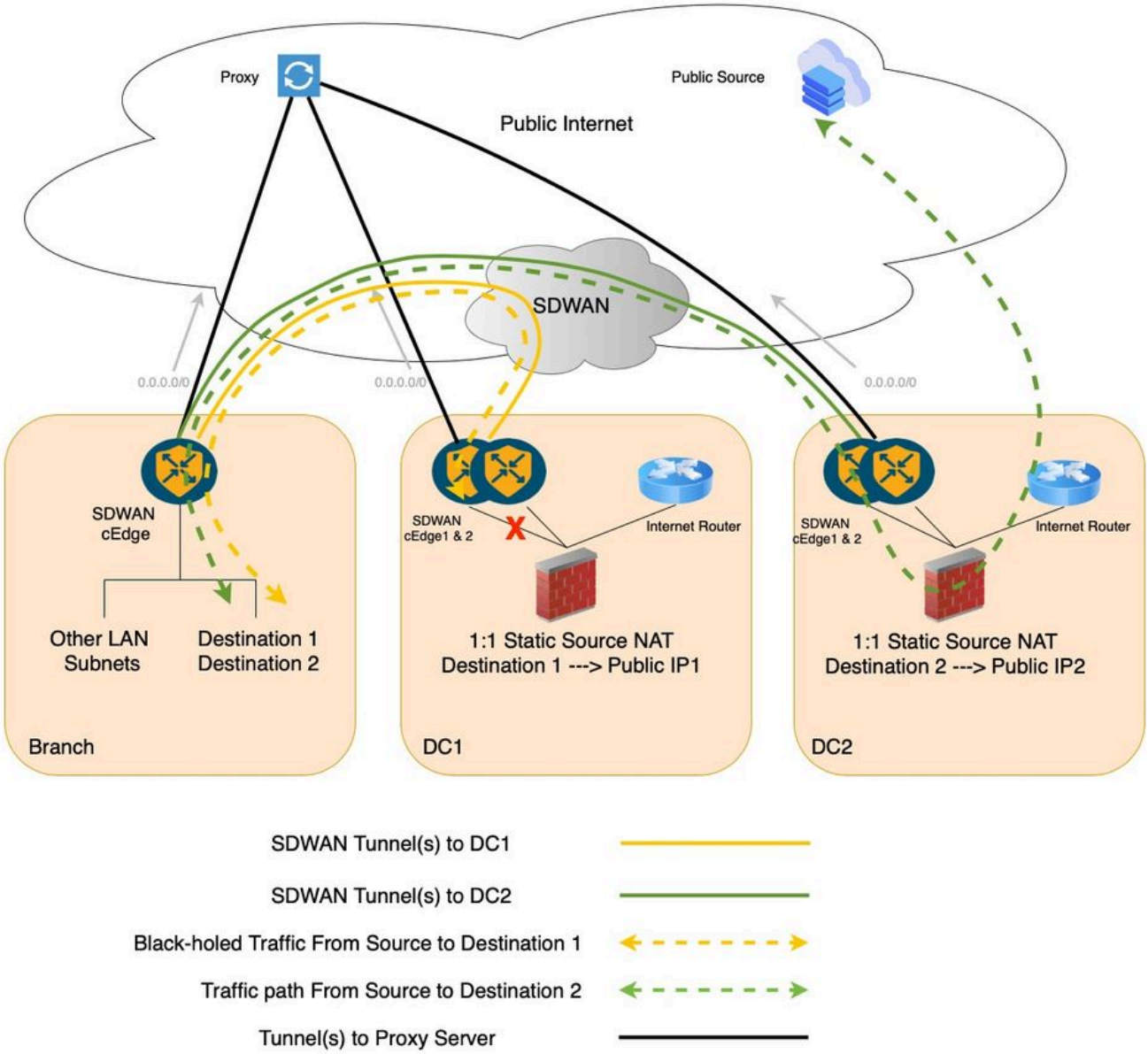
Anwendung auf Zweigstellen-SDWAN-Router aus Dienstrichtung:

```
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
  !
```

Datenverkehrsfluss mit benutzerdefinierter Datenrichtlinie (Fall eines SDWAN-Routers mit 1 LAN-Link im Rechenzentrum)

Die schwarzen Löcher im Datenverkehr am SDWAN-Router 1 des Rechenzentrums bei einem

Ausfall der LAN-Verbindung am SDWAN-Router 1.



2. Serviceeinbindung mit zentralisierter Datenrichtlinie

Die Verkettung von Cisco SDWAN-Services ist von Natur aus sehr flexibel und vollständig automatisiert. In einer älteren WAN-Konfiguration. Wenn Sie eine Firewall in den Pfad eines bestimmten Datenverkehrsflusses einfügen müssen, ist dies in der Regel mit einer Vielzahl manueller Konfigurationen an jedem Hop verbunden. Im Gegensatz dazu ist der Einfügeprozess von Cisco SD-WAN-Services so einfach wie der Abgleich von interessantem Datenverkehr mit einer zentralisierten Kontroll- oder Datenrichtlinie, das Festlegen des Firewall-Service als nächsten Hop und die anschließende Anwendung der Richtlinie auf eine Zielstandortliste über eine einzige Network Configuration Protocol (NETCONF)-Transaktion vom Cisco SDWAN Manager zum Cisco SDWAN Controller.

So fügen Sie eine Firewall als Service in unserem Konfigurationsbeispiel ein:

1. Definieren Sie die Firewall als Service auf den DC-cEdge-Geräten. Dies kann mithilfe von VPN-

Funktionsvorlagen sowie durch direkte Anmeldung bei den Geräten erreicht werden. Die Nachverfolgung für den Dienst ist standardmäßig aktiviert. Dies bedeutet, dass der gesamte Service ausfällt, wenn die DC-Firewall vom primären DC SDWAN-Router cEdge1 nicht erreichbar ist, und der Datenverkehr auf den sekundären Router cEdge2 von DC zurückgreift.

2. Erstellen und wenden Sie eine zentrale Datenrichtlinie an, um den FW-Service bidirektional in den Datenverkehrspfad einzufügen.

Konfiguration (mit Service-Einfügung)

Konfiguration auf SDWAN-Routern des RZ:

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

In der früheren Konfiguration der SDWAN-Router in Rechenzentren wurde ein Service vom Typ "Firewall" definiert, der dem Cisco SDWAN-Controller angekündigt wird. Der SDWAN-Router des Rechenzentrums wirbt nicht mehr wie gewohnt, wenn die Erreichbarkeit des Firewall-Services ausfällt oder die Firewall selbst ausfällt.

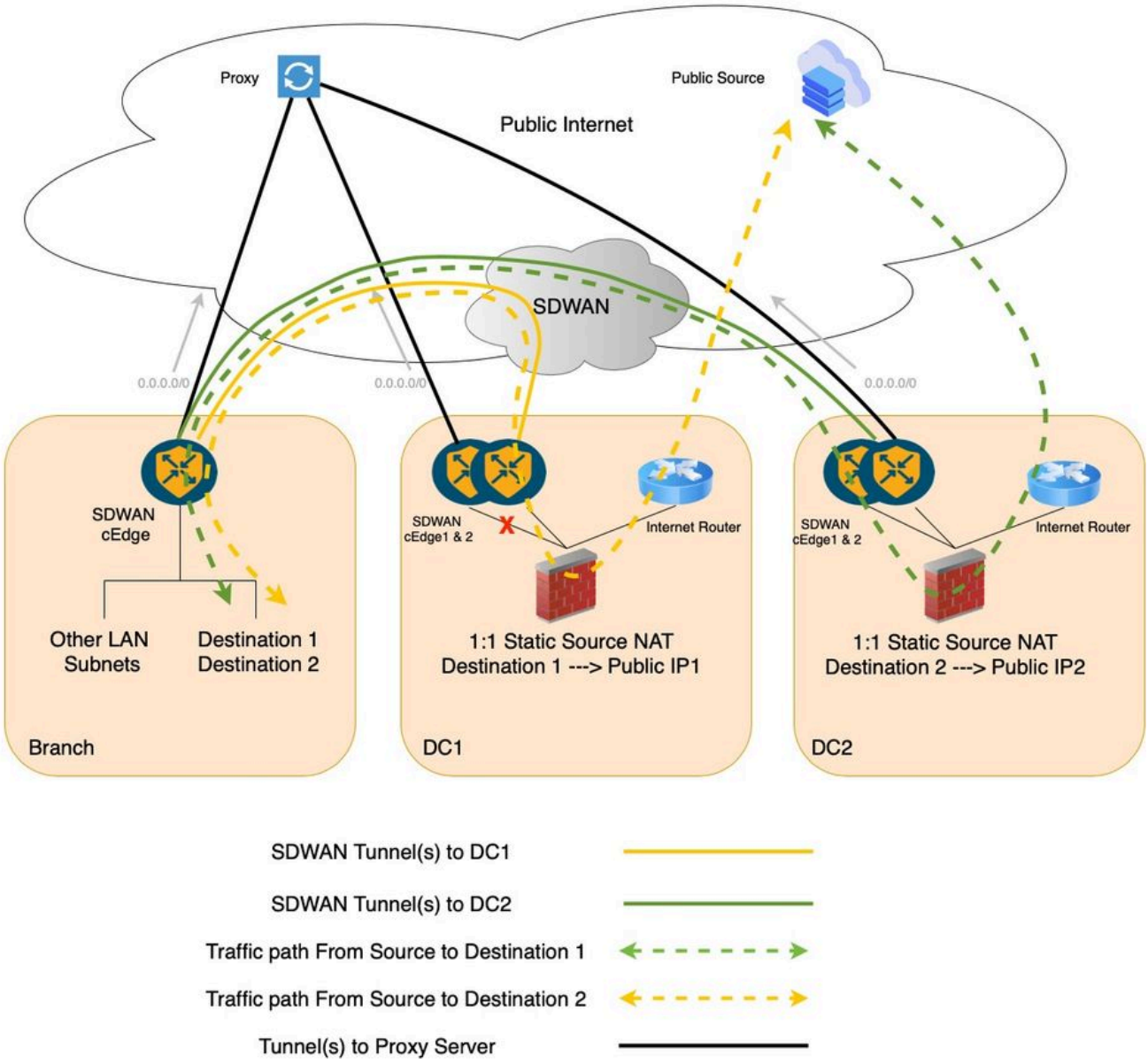
Eine Richtlinie für die Verkettung von Services wird definiert, wenn sie auf den SDWAN-Router der Außenstelle von der Servicerichtung aus angewendet wird:

```
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
  !
```

Datenverkehrsfluss bei Diensteinfügung (SDWAN-Router 1 des RZ, Fall eines LAN-

Verbindungsausfalls)

Der Datenverkehr wird auf den SDWAN-Router 2 des Rechenzentrums umgeleitet, falls die LAN-Verbindung des SDWAN-Routers 1 ausfällt.



Diese Richtlinienvoraussetzungen oder vordefinierten Listen sind im Cisco Catalyst SDWAN Manager definiert, wie als Referenz dargestellt:

```
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
!
!
```

Details zum Datenverkehrsfluss für besseres Verständnis

Datenverkehrsfluss von außen nach innen

Internetquelle (MS-Teams) > DC1 FW (NAT) > DC1 cEdge01 > Branch cEdge01 > Server-Subnetz 1.

Internetquelle (MS-Teams) > DC2 FW (NAT) > DC2 cEdge01 > Außenstelle cEdge01 > Server-Subnetz 2.

Für diesen Datenverkehr erfolgt die Beeinflussung in den jeweiligen Hops wie folgt:

Internetquelle (MS-Teams) > DC1 FW.

Internetquelle (MS-Teams) > DC2 FW.

Die Rechenzentren in DC1 und DC2 geben den jeweiligen öffentlichen IP-Pool über Internet-CPE in den Rechenzentren an das Internet weiter.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

Firewall-Routing für internes Subnetz.

DC1 cEdge01 > Branch cEdge01.

DC2 cEdge01 > Branch cEdge01.

Cisco SDWAN-Routing über Overlay Management Protocol (OMP)

cEdge01 der Außenstelle > Server-Subnetz 1.

cEdge01 der Außenstelle > Server-Subnetz 2.

Zweigstellen-Router-Routing für internes Subnetz

Datenverkehrsfluss von innen nach außen

Server-Subnetz 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).

Für diesen Datenverkehr erfolgt die Beeinflussung in den jeweiligen Hops wie folgt:

Server-Subnetz 1 > Branch cEdge 01

Server-Subnetz 2 > Branch cEdge 01

Internes Routing auf Serverseite.

cEdge 01 > DC1 cEdge01 verzweigen.

cEdge 01 > DC2 cEdge01 verzweigen.

Verwendung zentraler Datenrichtlinien (Serviceverkettung) zur Beeinflussung des Datenverkehrspfads

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

Verwendung von Service Labels zur Beeinflussung des Datenverkehrspfads vom SDWAN-cEdge zu den entsprechenden FWs in Rechenzentren

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

DC2 FW (NAT) > Internetquelle (MS-Teams).

Aus privaten IP-Quellen stammender Datenverkehr vom Server wird per NAT an die FW geleitet, damit er über CPE ins Internet gelangt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.