중앙 집중식 데이터 정책을 사용한 서비스 삽입: 독특한 트래픽 조작 활용 사례

목차

소개

이 문서에서는 인터넷에서 SDWAN 브랜치 사이트에 호스팅된 서버로 이동하는 인바운드 트래픽의 흐름을 제어하는 데 서비스 체이닝을 사용하는 예시 시나리오에 대해 설명합니다.

배경 정보

또한 이 문서에서는 서비스 체이닝을 사용하여 DC(데이터 센터) LAN 링크 장애를 쉽게 추적하여 브랜치 SDWAN 라우터에 Datapolicy를 사용하여 트래픽 경로를 변경하도록 통지할 수 있음을 보여 줍니다. Datapolicy는 달리 사용할 수 없으며 DC에서 트래픽이 쉽게 블랙홀을 통과하지 못합니다.

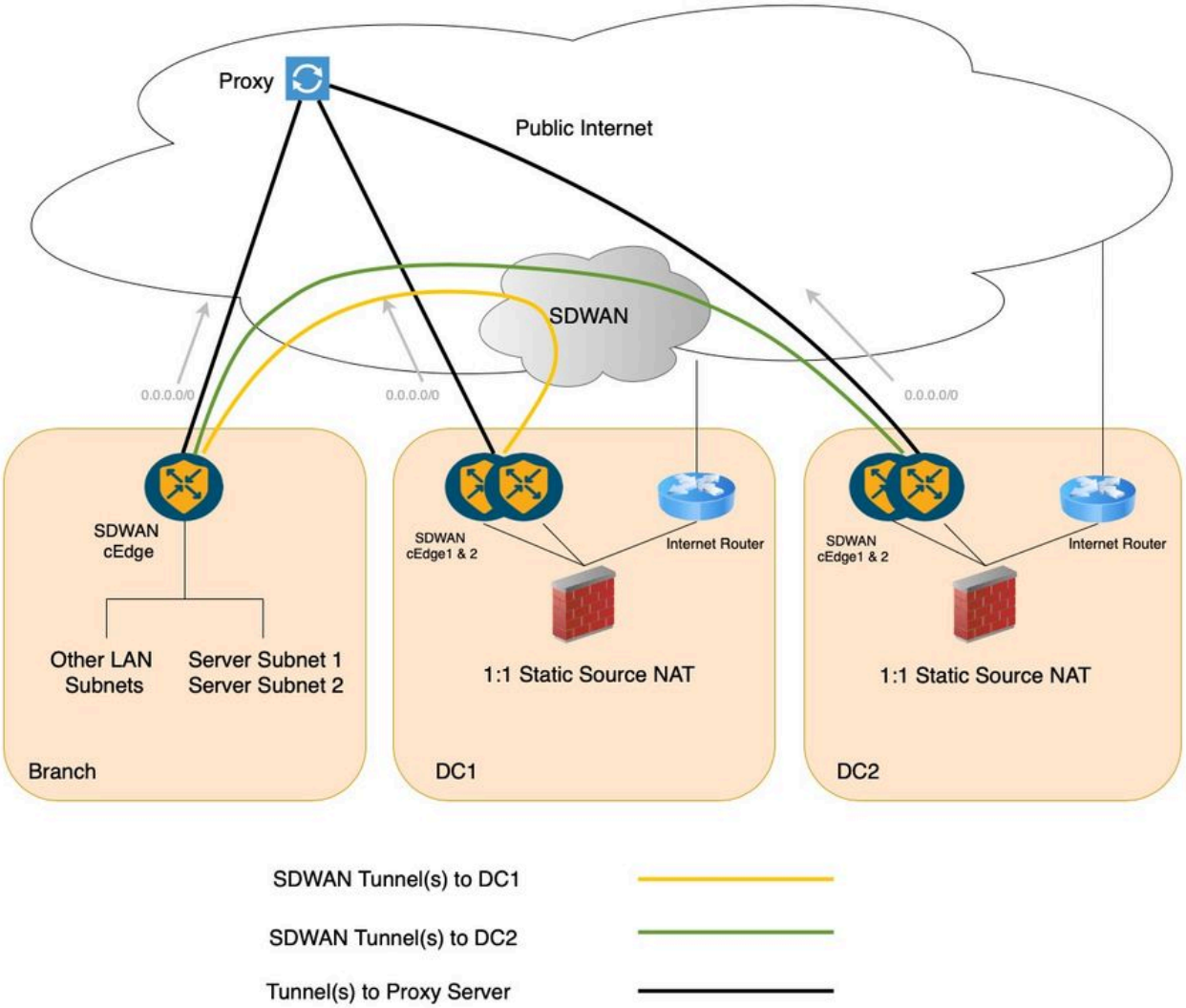
여기서 인바운드 트래픽은 관리 및 보안을 위해 DC 방화벽을 통해 라우팅됩니다.

토폴로지 예

다음 다이어그램에 나와 있는 것처럼 이 시나리오를 묘사하기 위해 듀얼 DC 설정과 브랜치 사이트가 있는 표준 SDWAN 구축을 고려했습니다. 여러 갈래가 있을 수 있으나, 단순함을 위해 한 갈래만 그려졌다. DC와 브랜치 사이트는 Secure SDWAN Overlay, 즉 SDWAN Secure IPSec 터널을 통해 통신합니다. 이 기존 설정에서는 DC와 브랜치 사이트 모두 서비스 VRF(Virtual Routing and Forwarding)의 프록시 서버에 터널을 가지고 있으며 서비스 VRF/VPN(Virtual Private Network)의 기본 경로가 이 프록시를 가리킵니다.

이 토폴로지 설정은 두 개의 서버 서브넷, 즉 서버 서브넷 1과 서버 서브넷 2가 호스팅되는 브랜치

사이트로 구성됩니다. 두 개의 데이터 센터가 있습니다. 각 데이터 센터 방화벽은 인터넷에서 각 브랜치 서버 서브넷에 연결할 수 있도록 1:1 NAT(Static Network Address Translation)를 수행합니다. 정확히 말해, 데이터 센터 1 방화벽은 서버 서브넷 1에 대해 1:1 고정 NAT를 수행하고 데이터 센터 2 방화벽은 서버 서브넷 2에 대해 동일한 작업을 수행합니다.

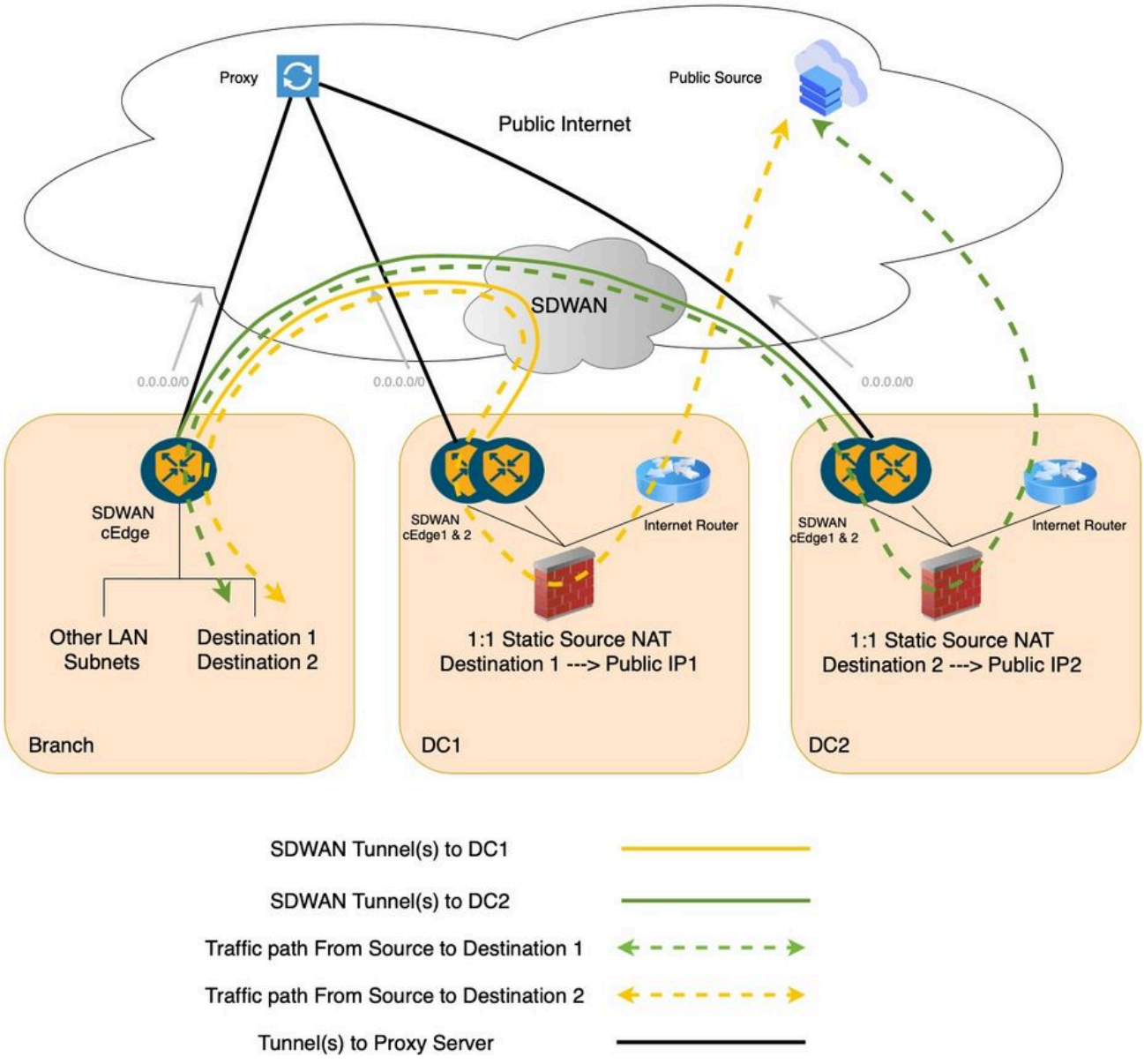


고객 요구 사항

앞서 설명한 대로 고객의 요구 사항을 염두에 두고 다음과 같이 설정할 수 있습니다.

- MS Teams와 같은 공용 애플리케이션은 지사에서 호스팅되는 이러한 서버에 액세스해야 합니다. 앞에서 설명한 것처럼 DC에서 상태 기반 FW를 사용할 수 있으므로 고객은 브랜치 사이트에 대한 직접 인바운드 연결 대신 FW를 사용하도록 요청합니다.
- 지사의 서버 서브넷 1은 DC1을 통해 연결할 수 있어야 하며 지사의 서버 서브넷 2는 인터넷에서 DC2를 통해 연결할 수 있어야 합니다.
- 고객 네트워크 내에서 공용 IP를 라우팅해서는 안 됩니다.
- 브랜치 호스팅 서버 서브넷 1 및 2는 프라이빗 IP로 구성되며 프라이빗-퍼블릭 IP 변환은 각 DC FW에서 이루어져야 합니다.
- 언더레이 라우팅 변경이 없어야 합니다.

참고: DC 또는 브랜치 사이트에서 트래픽 흐름에 대한 변경 사항이 없는 경우, 지사의 서버에 연결하기 위해 인터넷의 전달 트래픽은 DC 방화벽을 통과합니다. 한편 반환 트래픽은 인터넷 소스에 도달하기 위해 Branch SDWAN 라우터의 프록시(기본 경로 사용)를 직접 통과합니다. 이는 비대칭 트래픽 흐름입니다.



가능한 솔루션

앞서 언급한 요구 사항을 해결할 수 있는 솔루션은 두 가지가 있습니다.

1. DC LAN 링크 장애 시 트래픽 블랙홀이 발생하는 중앙 집중식 데이터 정책을 통한 맞춤형 트래픽 엔지니어링
2. DC LAN 링크 장애 시 트래픽이 블랙홀(blackhole)하지 않는 중앙 집중식 데이터 정책을 사용하는 서비스 삽입.

1. 중앙 집중식 데이터 정책을 통한 맞춤형 트래픽 엔지니어링

중앙 집중식 데이터 정책에서 사용자 지정 트래픽 엔지니어링 데이터 정책을 고려하는 경우, 하나는 브랜치에 대한 것이고 다른 하나는 DC에 대한 것입니다. 브랜치 데이터 정책은 원격 tlocs를 사용하여 브랜치에서 DC로 트래픽을 전송하고, 두 번째 데이터 정책은 cEdge에서 방화벽(FW)으로 DC 내의 흐름을 추가로 라우팅합니다. 그러나 브랜치에 remote-tloc 옵션이 구성되어 있으면 브랜치 SDWAN 라우터는 DC SDWAN 라우터 1 LAN 링크 오류를 인식하지 못합니다. 즉, DC SDWAN 라우터 1의 LAN 링크가 실패하면 브랜치 라우터는 해당 트래픽을 인식하지 못하고 DC SDWAN 라우터 01로 전달합니다. 따라서 DC SDWAN 라우터 1에서 트래픽이 쉽게 블랙홀(Black Hole)이 됩니다.

컨피그레이션(사용자 지정 데이터 정책 사용)

터널 방향에서 DC SDWAN 라우터에 적용됨:

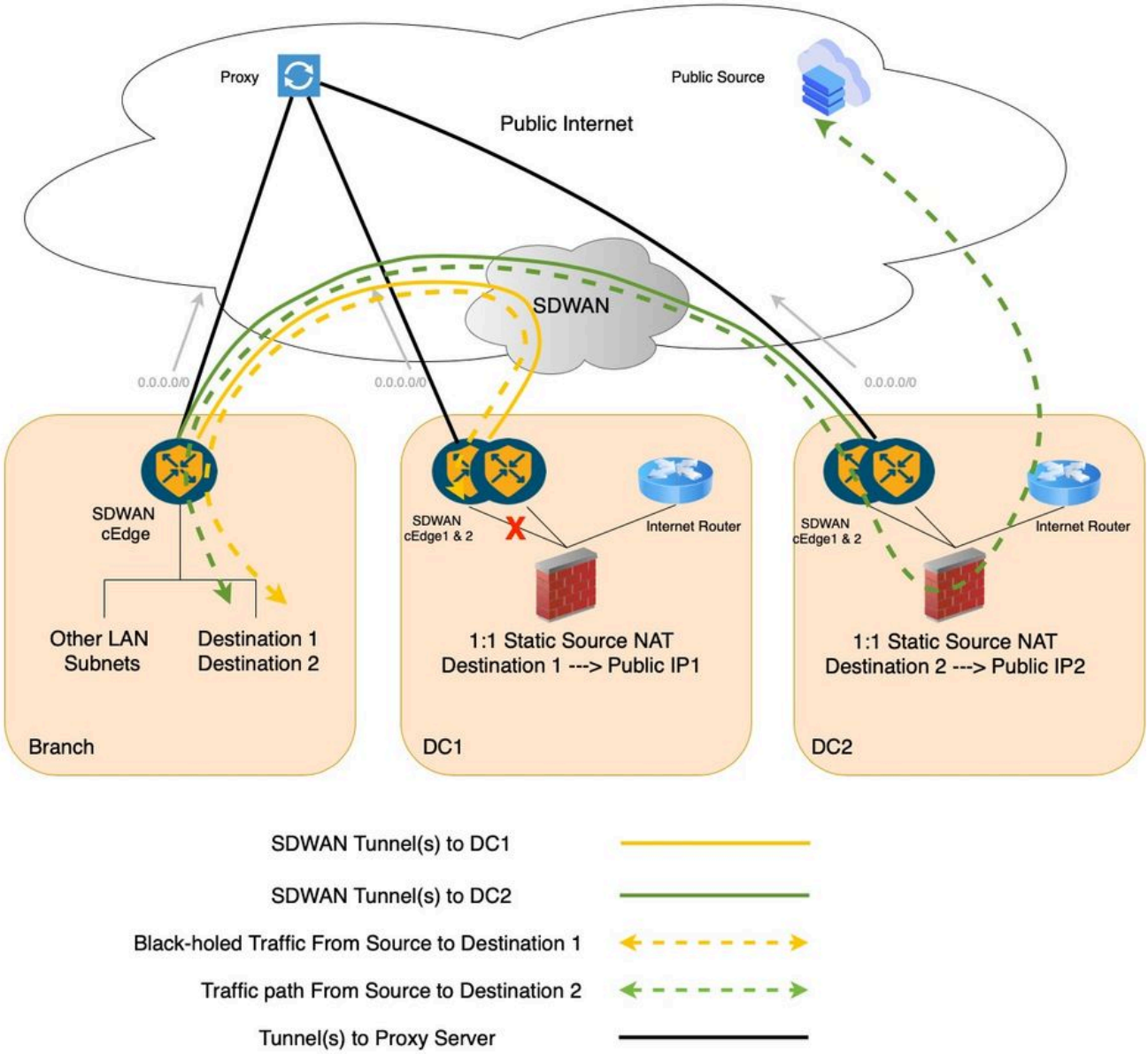
```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
       next-hop <Firewall_IP>
      !
     !
```

브랜치 SDWAN 라우터에 적용됨 from-service 방향:

```
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
  !
```

사용자 지정 데이터 정책을 사용하는 트래픽 흐름(DC SDWAN 라우터 1LAN 링크 실패 사례)

DC SDWAN 라우터 1 LAN 링크 장애의 경우 DC SDWAN 라우터 1의 트래픽 블랙홀.



2. 중앙 집중식 데이터 정책으로 서비스 삽입

Cisco SDWAN 서비스 체이닝은 본질적으로 매우 유연하고 완전히 자동화되어 있습니다. 기존 WAN 설정에서. 특정 트래픽 흐름의 경로에 방화벽을 삽입해야 하는 경우 일반적으로 모든 홉에서 많은 수동 컨피그레이션과 연결됩니다. 이와 달리 Cisco SD-WAN 서비스 삽입 프로세스는 중앙 집중식 제어 또는 데이터 정책과 흥미로운 트래픽을 매칭하고, 방화벽 서비스를 다음 홉으로 설정한 다음, Cisco SDWAN Manager에서 Cisco SDWAN 컨트롤러로의 단일 NETCONF(Network Configuration Protocol) 트랜잭션을 통해 대상 사이트 목록에 정책을 적용하는 것만큼 간단합니다.

컨피그레이션 예에서는 Firewall as a service를 삽입하는 단계를 설명합니다.

1. DC cEdge 디바이스에서 방화벽을 서비스로 정의합니다. 이는 VPN 기능 템플릿은 물론 디바이스에 대한 직접 로그인을 사용하여 구현할 수 있습니다. 서비스에 대한 추적은 기본적으로 활성화되어 있습니다. 즉, DC 방화벽이 DC SDWAN 기본 라우터 cEdge1에서 연결할 수 없게 되면 전체 서비스가 다운되고 트래픽은 DC의 보조 라우터 cEdge2로 대체됩니다.

2. FW 서비스를 양방향으로 트래픽 경로에 삽입하려면 중앙 집중식 데이터 정책을 구축하고 적용합니다.

구성(서비스 삽입 포함)

DC SDWAN 라우터에서 구성:

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

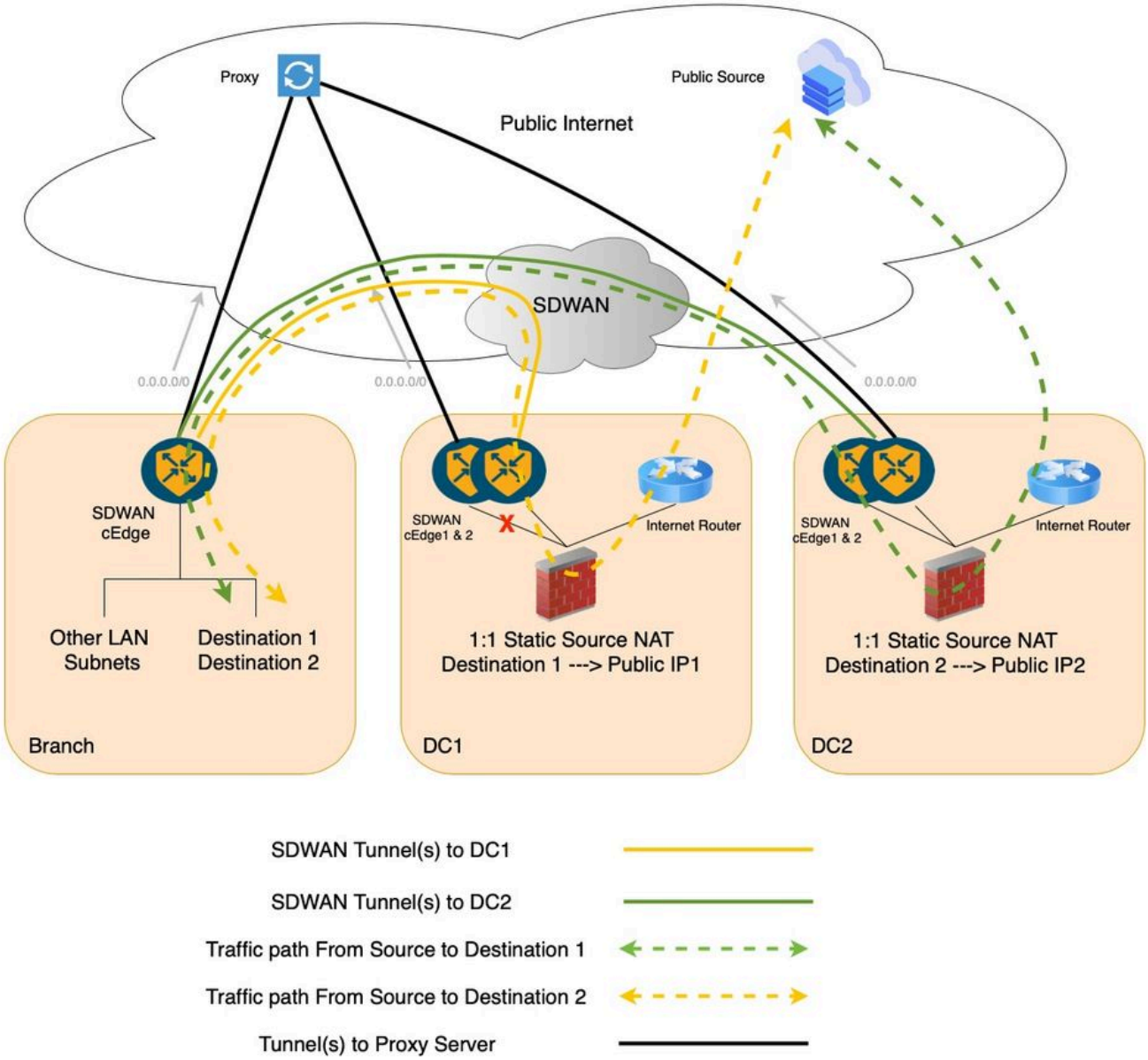
DC SDWAN 라우터의 이전 컨피그레이션은 Cisco SDWAN 컨트롤러에 보급되는 '방화벽' 유형의 서비스를 정의합니다. DC SDWAN 라우터는 방화벽 서비스에 대한 연결 기능이 꺼지거나 방화벽 자체가 다운되면 동일한 광고를 중단합니다.

서비스 체이닝 정책은 브랜치 SDWAN 라우터 from-service 방향에 적용되는 것으로 정의됩니다.

```
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
  !
```

서비스 삽입을 통한 트래픽 흐름(DC SDWAN 라우터 1 LAN 링크 실패 사례)

DC SDWAN 라우터 1 LAN 링크 장애 시 트래픽이 DC SDWAN 라우터 2로 장애 조치됩니다.



이러한 정책 사전 요구 사항 또는 사전 정의 목록은 참조용으로 표시된 대로 Cisco Catalyst SDWAN Manager에서 정의됩니다.

```
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
!
!
```

이해를 돕기 위한 트래픽 흐름 세부사항

외부-내부 트래픽 흐름

인터넷 소스(MS Teams) > DC1 FW(NAT) > DC1 cEdge01 > Branch cEdge01 > 서버 서브넷 1.

인터넷 소스(MS Teams) > DC2 FW(NAT) > DC2 cEdge01 > Branch cEdge01 > 서버 서브넷 2.

이 트래픽의 영향은 다음과 같이 각 홉에서 이루어집니다.

인터넷 소스(MS Teams) > DC1 FW.

인터넷 소스(MS Teams) > DC2 FW.

DC1 및 DC2는 DC에서 인터넷 CPE를 통해 각 공용 IP 풀을 인터넷에 광고합니다.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

내부 서브넷에 대한 방화벽 라우팅

DC1 cEdge01 > Branch cEdge01

DC2 cEdge01 > Branch cEdge01

OMP(Overlay Management Protocol) 오버레이를 통한 Cisco SDWAN 라우팅.

Branch cEdge01 > 서버 서브넷 1.

Branch cEdge01 > 서버 서브넷 2.

내부 서브넷에 대한 브랜치 라우터 라우팅

내부-외부 트래픽 흐름

서버 서브넷 1 > 브랜치 cEdge 01 > DC1 cEdge01 > DC1 FW (NAT) > 인터넷 소스 (MS Teams).

서버 서브넷 2 > 브랜치 cEdge 01 > DC2 cEdge01 > DC2 FW (NAT) > 인터넷 소스 (MS Teams).

이 트래픽의 영향은 다음과 같이 각 홉에서 이루어집니다.

서버 서브넷 1 > Branch cEdge 01.

서버 서브넷 2 > Branch cEdge 01.

서버 측의 내부 라우팅.

Branch cEdge 01 > DC1 cEdge01.

Branch cEdge 01 > DC2 cEdge01.

중앙 집중식 데이터 정책(서비스 체이닝)을 사용하여 트래픽 경로에 영향을 미칩니다.

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

SDWAN cEdge에서 DC의 각 FW로의 트래픽 경로에 영향을 주기 위해 서비스 레이블 사용

DC1 FW(NAT) > 인터넷 소스(MS Teams)

DC2 FW(NAT) > 인터넷 소스(MS Teams)

서버의 프라이빗 IP 소스 트래픽은 CPE를 통해 인터넷에 연결하기 위해 FW를 이그레스(egress)하기 위해 NAT됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.