一元化されたデータポリシーを使用したサービスの挿入：ユニークなトラフィック操作の使用例

内容

はじめに

このドキュメントでは、サービスチェーンを使用して、インターネットからSDWANブランチサイトでホストされるサーバへの着信トラフィックのフローを制御するシナリオ例について説明します。

バックグラウンド情報

また、このドキュメントでは、データセンター(DC)のLANリンク障害を追跡して、データポリシーを使用してトラフィックパスを変更するようブランチSDWANルータに通知する方法も、サービスチェーンを使用して示しています。この方法がなければ不可能であり、DC内のトラフィックを簡単にブラックホール化できます。

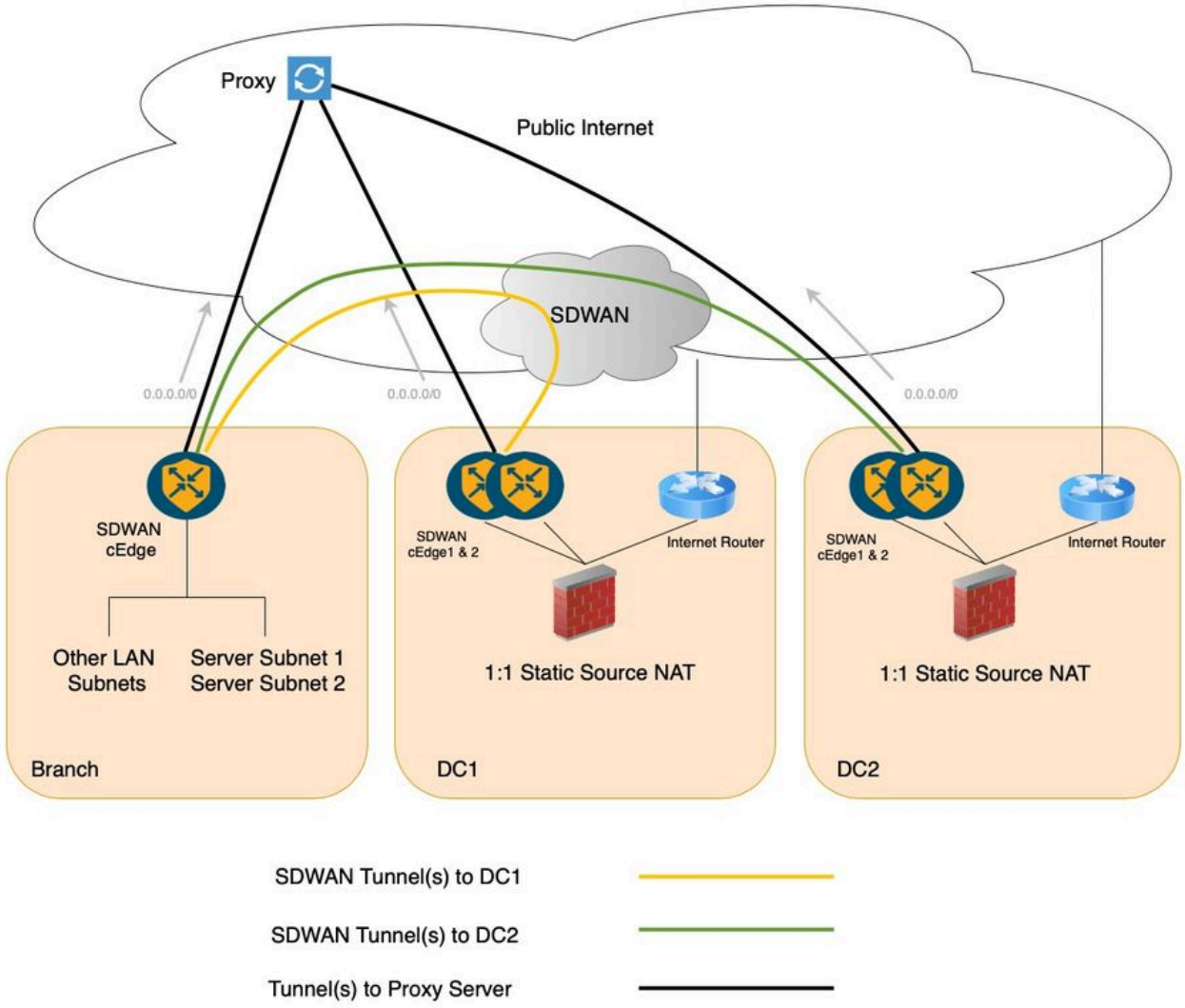
ここでの着信トラフィックは、管理とセキュリティのためにDCファイアウォール経由でルーティングされます。

トポロジの例

次の図に示すように、このシナリオを描くために、デュアルDC設定とブランチサイトを使用する標準的なSDWAN展開が検討されています。ただし、複数のブランチを作成することは可能です

。簡単にするために、1つのブランチだけを図示します。DCとブランチサイトは、セキュアSDWANオーバーレイ経由、つまりSDWANセキュアIPSecトンネル経由で通信します。この既存のセットアップでは、DCとブランチサイトの両方に、サービスVirtual Routing and Forwarding(VRF)内のプロキシサーバへのトンネルがあり、サービスVRF/Virtual Private Network(VPN)内のデフォルトルートはこのプロキシを指しています。

このトポロジ設定は、2つのサーバサブネット（サーバサブネット1とサーバサブネット2）がホストされているブランチサイトで構成されます。2つのデータセンターがあり、それぞれのブランチサーバサブネットにインターネットから到達できるように、それぞれのデータセンターファイアウォールが1:1のスタティックネットワークアドレス変換(NAT)を実行します。正確に言うと、データセンター1ファイアウォールはサーバサブネット1に対して1:1スタティックNATを実行し、データセンター2ファイアウォールはサーバサブネット2に対して同じNATを実行します。



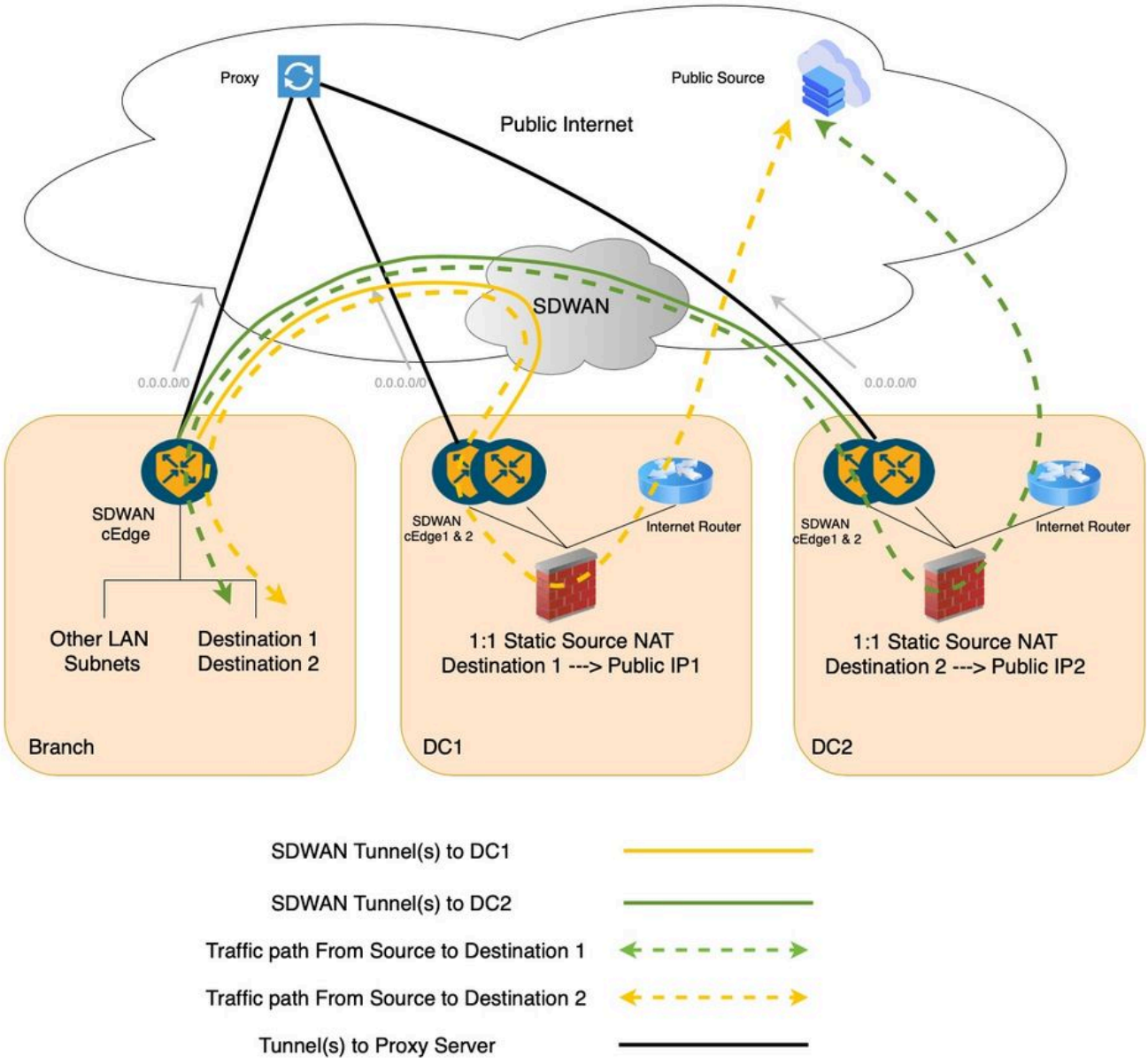
お客様の要件

以前の設定を念頭において、お客様からの要件は次のとおりです。

- MS Teamsなどのパブリックアプリケーションは、ブランチでホストされるこれらのサーバにアクセスする必要があります。前述のとおり、DCでステートフルFWを使用できることは、ブランチサイトへの直接着信接続の代わりにそれらを使用するように顧客に要求します。

- ブランチのサーバサブネット1にはDC1経由で到達でき、ブランチのサーバサブネット2にはインターネットからDC2経由で到達できる必要があります。
- お客様のネットワーク内でパブリックIPをルーティングすることはできません。
- ブランチホステッドサーバサブネット1および2はプライベートIPで設定され、プライベートからパブリックへのIP変換はそれぞれのDC FWで行われる必要があります。
- アンダーレイの経路を変更しないでください。

注:DCまたはブランチサイトのいずれかでトラフィックフローに変更がない場合、インターネットからの転送トラフィックは、ブランチサイトのサーバに到達するためにDCファイアウォールを通過します。一方、リターントラフィックはインターネットの送信元に到達するために、ブランチSDWANルータのプロキシを（デフォルトルートを使用して）直接通過します。これはトラフィックの非対称フローです。



考えられる解決策

以前の要件に対しては、次の2つの解決策が考えられます。

1. DC LANリンクに障害が発生した場合にトラフィックブラックホールが発生する、一元化されたデータポリシーによるカスタムトラフィックエンジニアリング。
2. DC LANリンクに障害が発生してもトラフィックがブラックホールに入らない、集中型データポリシーによるサービスの挿入。

1. 一元化されたデータポリシーを使用したカスタムトラフィックエンジニアリング

Centralized Data(CDN)ポリシーの下のCustom Traffic Engineering(CTE)データポリシーを検討する場合、ブランチ用とDC用の両方で、ブランチのデータポリシーはリモートブロックを使用してブランチからDCにトラフィックを送信し、2つ目のデータポリシーはcEdgeからファイアウォール(FW)に向けてDC内のフローをさらにルーティングします。 ただし、ブランチでremote-tlocオプションが設定されている場合、ブランチSDWANルータはDC SDWANルータ1 LANリンク障害を認識しません。つまり、DC SDWANルータ1のLANリンクに障害が発生した場合、ブランチルータは認識されず、そのトラフィックをDC SDWANルータ01に転送します。したがって、トラフィックはDC SDWANルータ1でブラックホールに簡単に陥ります。

構成（カスタムデータポリシーを使用）

DC SDWANルータのトンネル方向から適用：

```
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>
      !
     !
```

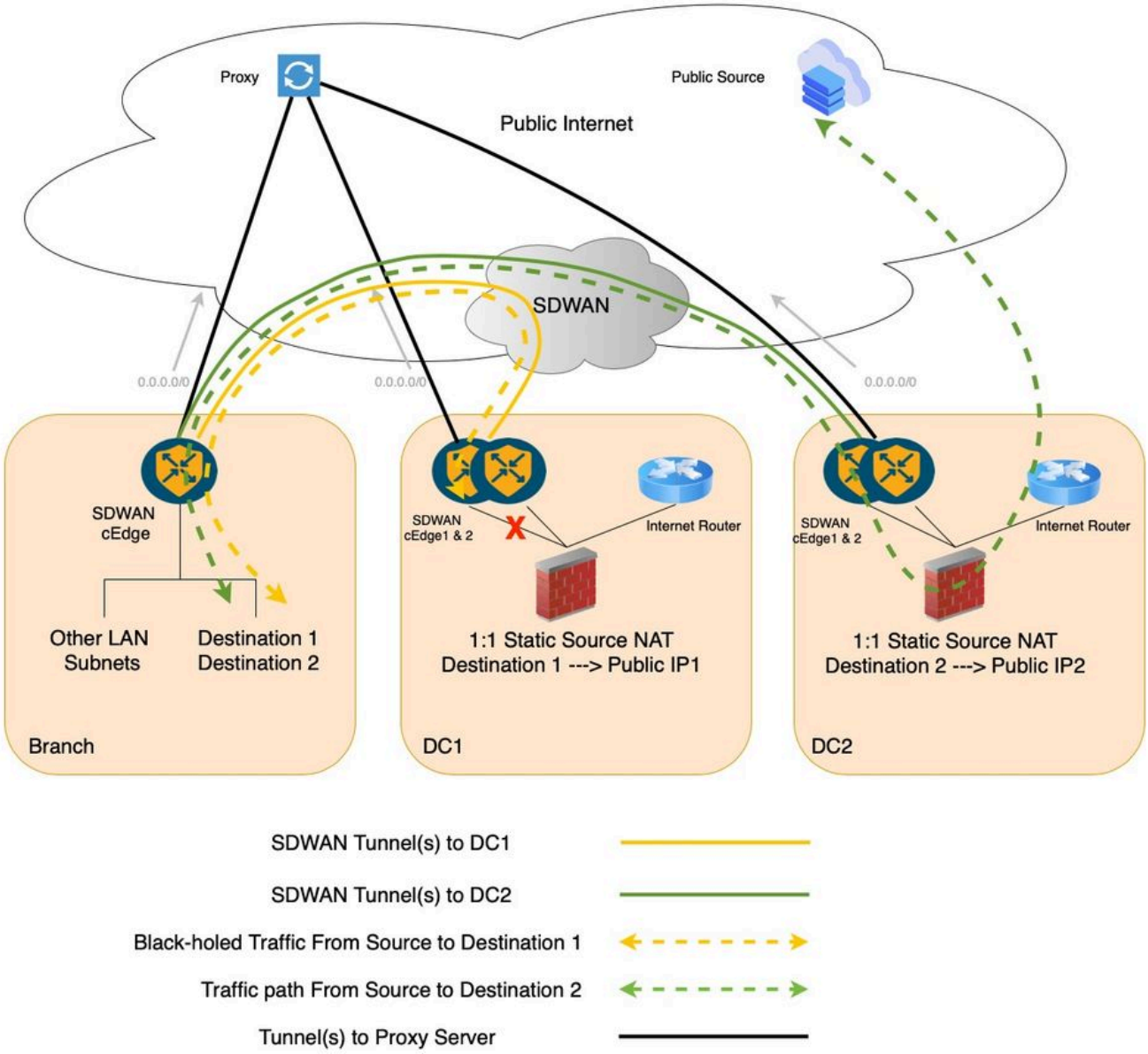
ブランチSDWANルータのサービス開始方向に適用：

```
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
!
```

カスタムデータポリシーを使用したトラフィックフロー(DC SDWANルータ1LANリンク障害の場合)

DC SDWANルータ1のLANリンクに障害が発生した場合の、DC SDWANルータ1のトラフィックブラックホール。



2. 一元化されたデータポリシーによるサービスの挿入

Cisco SDWANサービスチェーンは、本質的に非常に柔軟で、完全に自動化されています。レガシーWANセットアップの場合。特定のトラフィックフローのパスにファイアウォールを挿入する必要がある場合、通常は各ホップでの多数の手動設定に関連付けられます。 これに対し、Cisco

SD-WANサービスの挿入プロセスは、対象トラフィックを中央集中型の制御ポリシーまたはデータポリシーと照合し、ファイアウォールサービスをネクストホップとして設定し、Cisco SDWAN ManagerからCisco SDWAN Controllerへの単一のNetwork Configuration Protocol(NETCONF)トランザクションを介してポリシーをターゲットサイトリストに適用するという単純なものです。

設定例でFirewall as a serviceを挿入する手順を次に示します。

1. DC cEdgeデバイス上のサービスとしてファイアウォールを定義します。これは、デバイスへの直接ログインだけでなく、VPN機能テンプレートを使用して実現できます。サービスのトラッキングはデフォルトで有効になっています。つまり、DC SDWANプライマリルータcEdge1からDC Firewallに到達できなくなった場合、サービス全体がダウンし、トラフィックはDCのセカンダリルータcEdge2にフォールバックします。

2. 中央集中型データポリシーを構築して適用し、FWサービスを双方向のトラフィックパスに挿入します。

設定（サービス挿入時）

DC SDWANルータでの設定：

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

DC SDWANルータでの前述の設定では、Cisco SDWANコントローラにアドバタイズされる「ファイアウォール」タイプのサービスを定義しています。DC SDWANルータは、ファイアウォールサービスへの到達可能性が失われるか、またはファイアウォール自体がダウンすると、同じことをアドバタイズしなくなります。

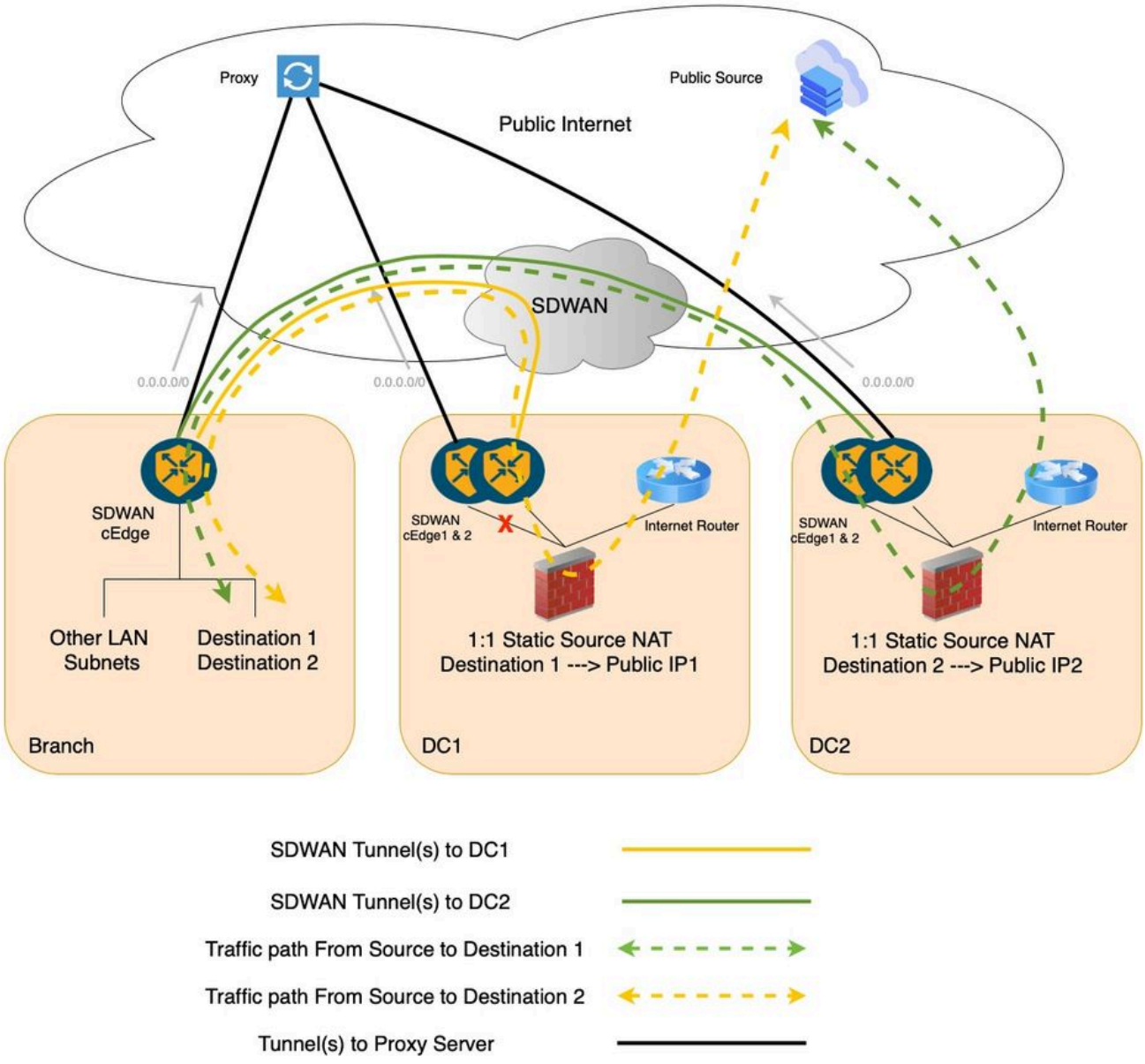
サービスチェーンポリシーは、ブランチSDWANルータのfrom-service方向に適用されるように定義されます。

```
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
  !
```

サービス挿入を伴うトラフィックフロー（DC SDWANルータ1 LANリンク障害の場合）

DC SDWANルータ1のLANリンクに障害が発生した場合、トラフィックはDC SDWANルータ2にフェールオーバーします。



Cisco Catalyst SDWAN Managerでは、次のポリシーの前提条件または事前定義されたリストが参照用に定義されています。

```
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
!
!
```

トラフィックフローの詳細を理解しやすくする

外部から内部へのトラフィックフロー

インターネットソース(MS Teams) > DC1 FW (NAT) > DC1 cEdge01 >ブランチcEdge01 >サーバサブネット1。

インターネットソース(MS Teams) > DC2 FW (NAT) > DC2 cEdge01 >ブランチcEdge01 >サーバサブネット2。

このトラフィックの影響は、次のように各ホップで行われます。

インターネットソース(MS Teams) > DC1 FW

インターネットソース(MS Teams) > DC2 FW

DC1とDC2は、それぞれのパブリックIPプールをDCのインターネットCPE経由でインターネットにアドバタイズします。

DC1 FW > DC1 cEdge01

DC2 FW > DC2 cEdge01

内部サブネットのファイアウォールルーティング。

DC1 cEdge01 >ブランチcEdge01

DC2 cEdge01 >ブランチcEdge01。

Overlay Management Protocol(OMP)オーバーレイによるCisco SDWANルーティング

ブランチcEdge01 >サーバサブネット1。

ブランチcEdge01 >サーバサブネット2。

内部サブネットのブランチルータルーティング。

内部から外部へのトラフィックフロー

サーバサブネット1 >ブランチcEdge 01 > DC1 cEdge01 > DC1 FW (NAT) >インターネットソース(MS Teams)。

サーバサブネット2 >ブランチcEdge 01 > DC2 cEdge01 > DC2 FW (NAT) >インターネットソース(MS Teams)。

このトラフィックの影響は、次のように各ホップで行われます。

サーバサブネット1 >ブランチcEdge 01

サーバサブネット2 >ブランチcEdge 01

サーバ側からの内部ルーティング。

ブランチcEdge 01 > DC1 cEdge01

ブランチcEdge 01 > DC2 cEdge01

一元化されたデータポリシー（サービスチェーン）を使用してトラフィックパスに影響を与える。

DC1 cEdge01 > DC1 FWです。

DC2 cEdge01 > DC2 FW。

サービスラベルを使用して、SDWAN cEdgeから各DCのFWへのトラフィックパスに影響を与える。

DC1 FW(NAT) >インターネットソース(MS Teams)。

DC2 FW(NAT) >インターネットソース(MS Teams)。

サーバからのプライベートIPソーストラフィックは、CPE経由でインターネットに到達するためにFWから出力されるようにNAT処理されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。