Inserção de serviço usando política de dados centralizada: Um caso de uso único de manobra de tráfego

Contents

Introdução

Este documento descreve um exemplo de cenário em que o encadeamento de serviços é usado para controlar o fluxo de tráfego de entrada da Internet para servidores hospedados no local da filial SDWAN.

Informações de Apoio

O documento também mostra que, usando o encadeamento de serviços, como a falha de link de LAN do data center (DC) pode ser facilmente rastreada para notificar o roteador SDWAN da filial para alterar o caminho de tráfego usando a política de dados, o que não era possível de outra forma e sem a qual o tráfego facilmente bloqueia o DC.

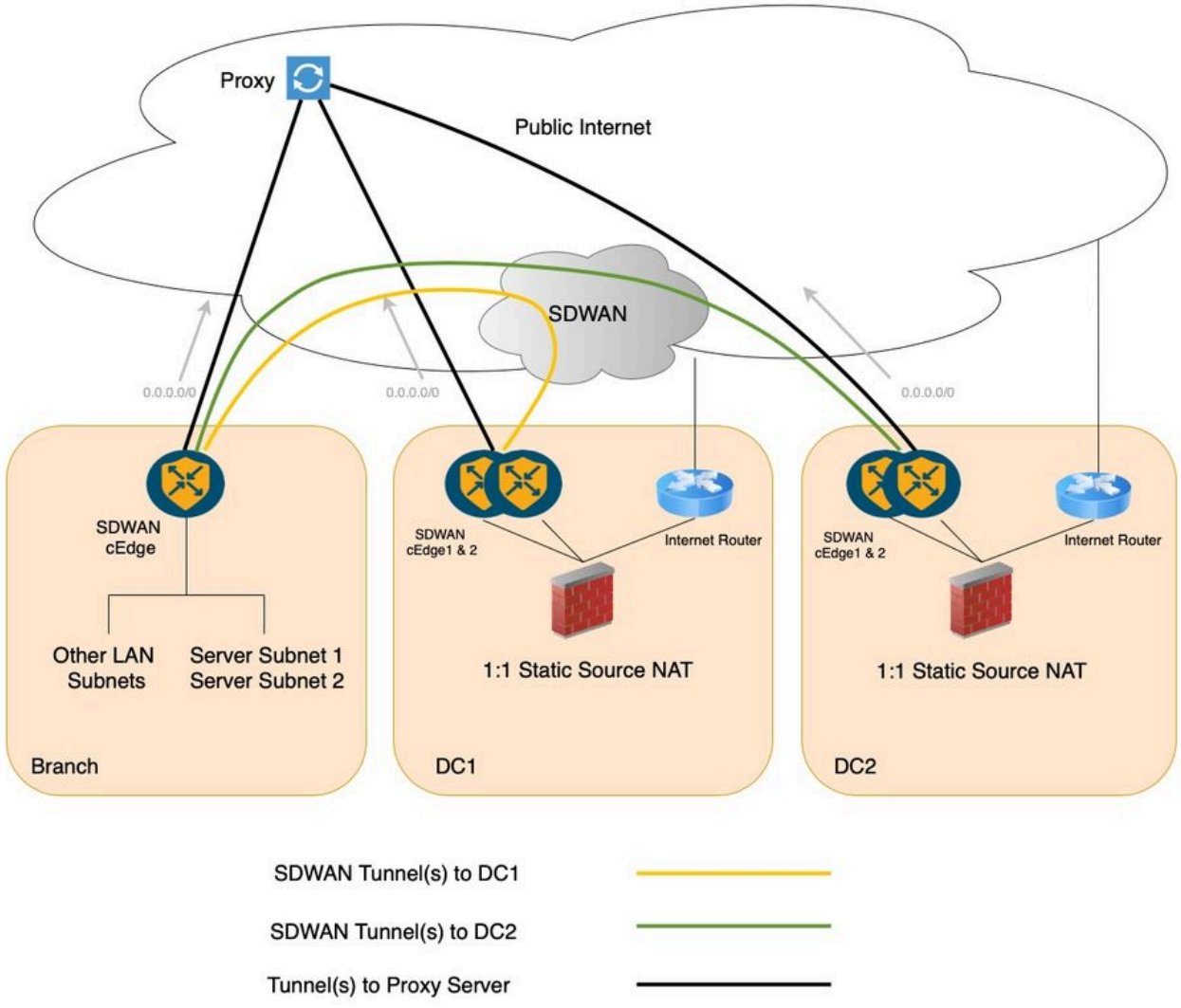
O tráfego de entrada aqui é roteado através dos firewalls DC para gerenciamento e segurança.

Exemplo de topologia

Uma implantação de SDWAN padrão com configuração de DC duplo e um local de filial foi considerada para retratar esse cenário como mostrado no próximo diagrama. Pode haver várias

ramificações, no entanto, por uma questão de simplicidade, apenas uma foi descrita. Os DCs e as filiais se comunicam através da Secure SDWAN Overlay, ou seja, através dos túneis SDWAN Secure IPSec. Nessa configuração existente, os DCs e o local da filial têm túnel(s) para os servidores proxy no serviço Virtual Routing and Forwarding (VRF) e a rota padrão no serviço VRF/Virtual Private Network (VPN) aponta para esse proxy.

Essa configuração de topologia consiste em um site de filial onde duas sub-redes de servidores, a sub-rede 1 e a sub-rede 2 do servidor, são hospedadas. Há dois data centers, em que cada um dos firewalls de data center executa a conversão estática de endereço de rede (NAT) 1:1 para permitir que a respectiva sub-rede do servidor de filial seja alcançável pela Internet. Para ser preciso, o firewall do data center 1 executa o NAT estático 1:1 para a sub-rede 1 do servidor e o firewall do data center 2 executa o mesmo para a sub-rede 2 do servidor.



Requisito do cliente

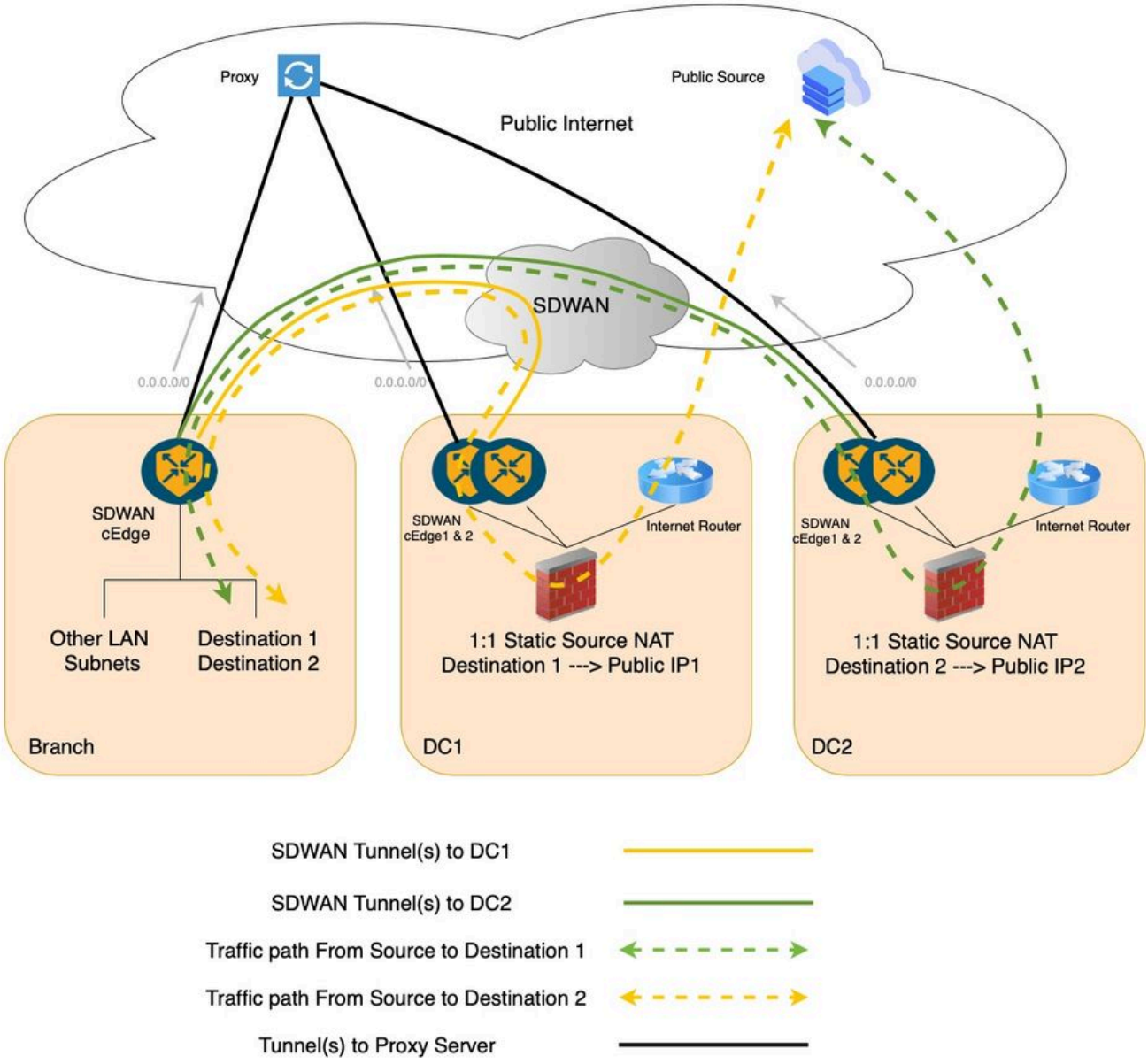
Com a configuração anterior em mente, o requisito do cliente pode ser mencionado:

- Um aplicativo público como as Equipes de MS precisa acessar esses servidores hospedados na Filial. Conforme mencionado anteriormente, a disponibilidade de FWs stateful nos DCs faz com que o cliente solicite que eles sejam usados em vez da conexão

de entrada direta com o local da filial.

- A Sub-rede 1 do Servidor na Filial deve estar acessível via DC1 e a Sub-rede 2 do Servidor na Filial deve estar acessível via DC2 a partir da Internet.
- Nenhum IP público deve ser roteado na rede do cliente.
- As sub-redes 1 e 2 do servidor hospedado na filial são configuradas com IPs privados e a conversão de IP privado para público deve ocorrer nos respectivos FWs DC.
- Não deve haver nenhuma alteração de roteamento subjacente.

Note: Se não houver alterações feitas no fluxo de tráfego no DC ou no local da filial, o tráfego de encaminhamento da Internet passará pelos firewalls do DC para acessar os servidores no local da filial. Por outro lado, o tráfego de retorno passará diretamente pelo roteador Proxy at Branch SDWAN (usando a rota padrão) para acessar a origem da Internet. Esse é um fluxo assimétrico de tráfego.



Soluções possíveis

Pode haver duas soluções possíveis para os requisitos anteriores:

1. Engenharia de tráfego personalizada com política de dados centralizada, onde o tráfego é bloqueado em caso de falha de link de LAN DC.
2. Inserção de serviço com política de dados centralizada, onde o tráfego não é interrompido em caso de falha do link da LAN do DC.

1. Engenharia de tráfego personalizada com política de dados centralizada

Se as políticas de dados de Engenharia de Tráfego Personalizada sob a política de Dados Centralizados forem consideradas, uma para a filial e outra para o DC, a política de dados da Filial enviará o tráfego da Filial para o DC usando toques remotos e a segunda política de dados roteará ainda mais o fluxo no DC a partir do cEdge para o Firewall (FW). Mas, com a opção de tloc remoto configurada na Filial, o roteador SDWAN da Filial não está ciente da falha do link de LAN do Roteador 1 SDWAN do DC. Ou seja, se o link da LAN no roteador 1 da SDWAN CC falhar, o roteador da Filial não reconhecerá e ainda encaminhará esse tráfego para o roteador 01 da SDWAN CC. Portanto, o tráfego facilmente causa buracos negros no roteador 1 da SDWAN CC.

Configuração (Com Política De Dados Personalizada)

Aplicado no roteador SDWAN DC na direção de túnel:

```
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>
      !
     !
```

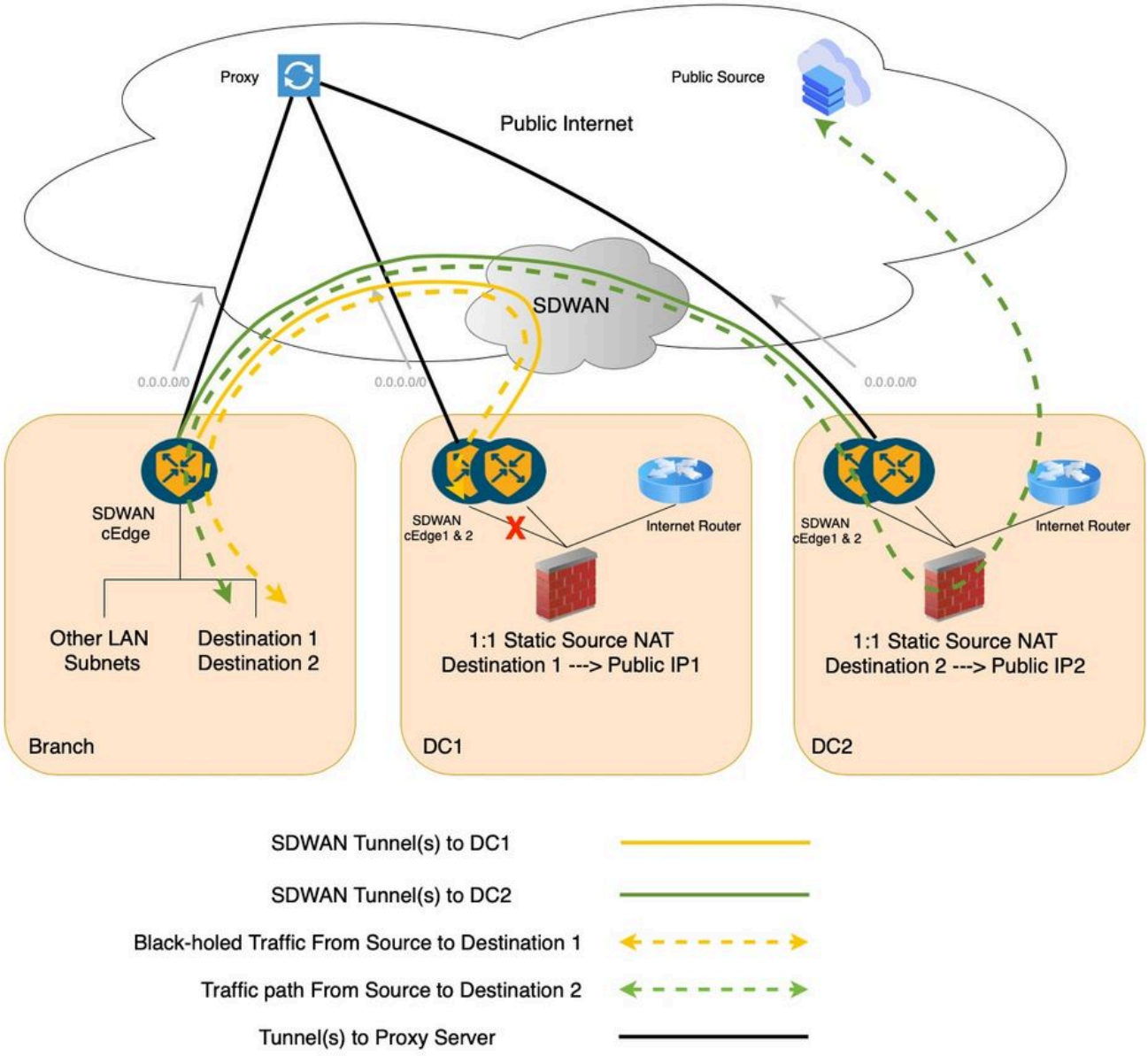
Aplicado no roteador SDWAN da filial a partir da direção de serviço:

```
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
!
```

Fluxo de tráfego com política de dados personalizada (caso de falha de link de LAN do roteador 1 SDWAN DC)

Os buracos de tráfego no roteador 1 da SDWAN CC em caso de falha no link da LAN do roteador 1 da SDWAN CC.



2. Inserção de serviço com política de dados centralizada

O encadeamento de serviços Cisco SDWAN é inerentemente muito flexível e totalmente automatizado. Em uma configuração de WAN antiga. Se você tiver que inserir um firewall no caminho de um fluxo de tráfego específico, ele geralmente está associado a muitas configurações manuais em cada salto. Em contraste, o processo de inserção do serviço Cisco SD-WAN é tão simples quanto corresponder tráfego interessante com um controle centralizado ou uma política de dados, definir o serviço de firewall como um próximo salto e, em seguida, aplicar a política a uma lista de sites de destino por meio de uma única transação de Network Configuration Protocol (NETCONF) do Cisco SDWAN Manager para o Cisco SDWAN Controller.

Aqui estão as etapas para inserir um Firewall como um serviço em nosso exemplo de configuração:

1. Defina Firewall como um serviço nos dispositivos DC Edge. Isso pode ser obtido usando modelos de recursos de VPN, bem como login direto nos dispositivos. O rastreamento no serviço é habilitado por padrão, o que significa que se o firewall de DC se tornar inalcançável a partir do roteador cEdge1 primário DC SDWAN, o serviço inteiro será desativado e o tráfego retornará ao roteador cEdge2 secundário de DC.

2. Crie e aplique uma política de dados centralizada para inserir o serviço de FW no caminho de tráfego bidirecionalmente.

Configuração (Com Inserção De Serviço)

Configurado em roteadores SDWAN DC:

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

A configuração anterior em DC SDWAN Routers define um serviço do tipo 'Firewall' que é anunciado para o Cisco SDWAN Controller. O roteador DC SDWAN pára de anunciar o mesmo quando o alcance do serviço de firewall é desativado ou o próprio firewall é desativado.

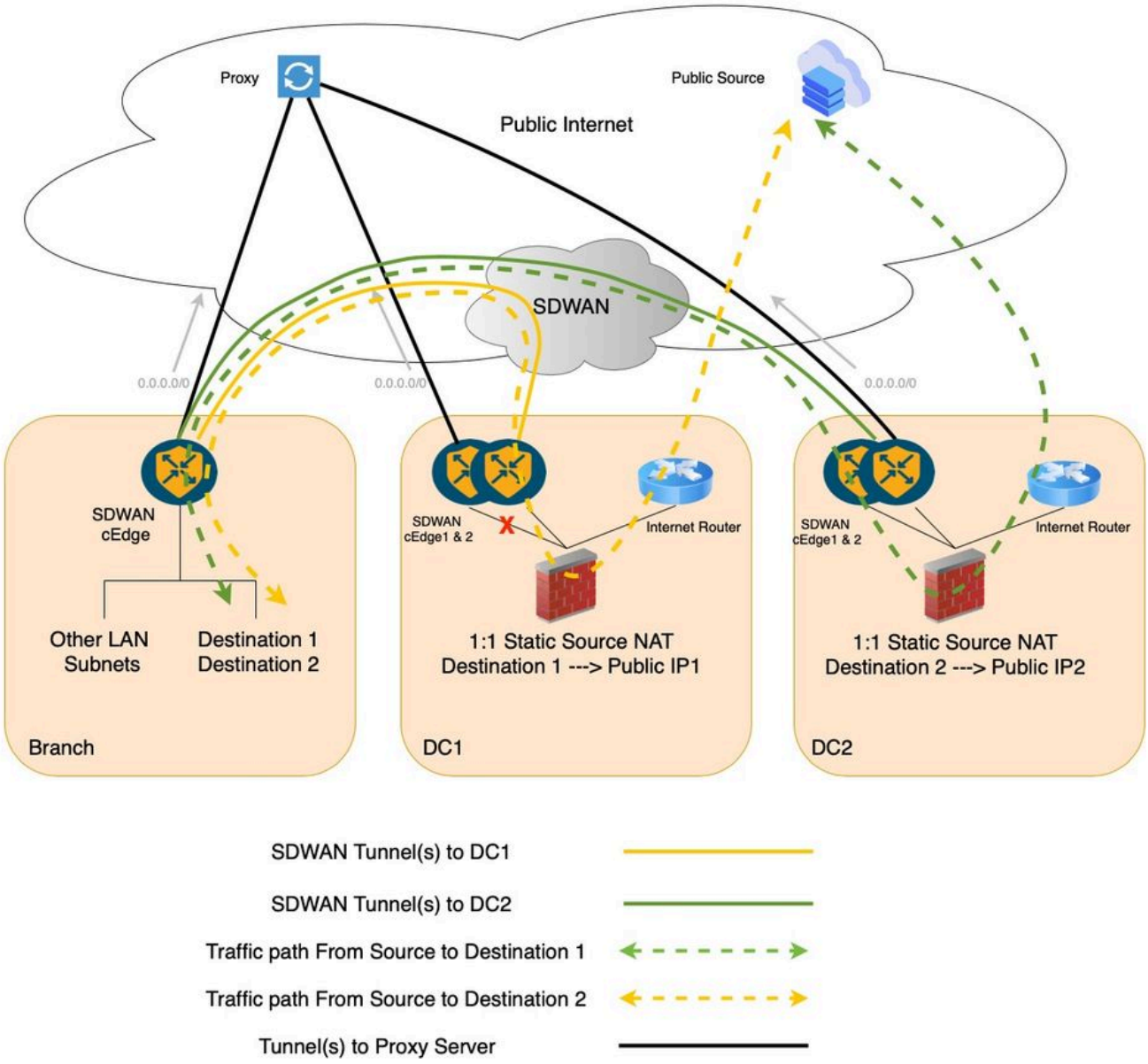
Uma política de encadeamento de serviços é definida como aplicada no roteador SDWAN da filial a partir da direção de serviço:

```
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
!
```

Fluxo de tráfego com inserção de serviço (caso de falha de link de LAN do roteador 1 da SDWAN DC)

O tráfego falha para o Roteador 2 SDWAN DC em caso de falha do link de LAN do Roteador 1 SDWAN DC.



Esses pré-requisitos de política ou listas predefinidas são definidos no Cisco Catalyst SDWAN Manager como mostrado para referência:

```
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
  !
  !
```

Detalhes do fluxo de tráfego para melhor compreensão

Fluxo de tráfego externo para interno

Fonte da Internet (Equipes MS) > DC1 FW (NAT) > DC1 cEdge01 > Branch cEdge01 > Sub-rede de servidor 1.

Fonte da Internet (Equipes MS) > DC2 FW (NAT) > DC2 cEdge01 > Branch cEdge01 > Sub-rede 2 do Servidor.

Para esse tráfego, a influência é feita nos respectivos saltos da seguinte maneira:

Fonte de Internet (Equipes MS) > DC1 FW.

Fonte de Internet (Equipes MS) > DC2 FW.

DC1 e DC2 Anunciam o respectivo pool de IP público à Internet através do Internet CPE nos DCs.

DC1 FW > DC1 cEdge01

DC2 FW > DC2 cEdge01

Roteamento de firewall para sub-rede interna.

DC1 cEdge01 > Branch cEdge01.

DC2 cEdge01 > Branch cEdge01.

Roteamento Cisco SDWAN através de sobreposição de protocolo de gerenciamento de sobreposição (OMP - Overlay Management Protocol).

Branch Edge01 > Sub-rede de servidor 1.

Branch Edge01 > Sub-rede 2 do servidor.

Roteamento do roteador da filial para a sub-rede interna.

Fluxo de tráfego interno para externo

Sub-rede do servidor 1 > Branch cEdge 01 > DC1 cEdge01 > DC1 FW (NAT) > Internet Source (MS Teams).

Sub-rede do servidor 2 > Branch Edge 01 > DC2 cEdge01 > DC2 FW (NAT) > Internet Source (MS Teams).

Para esse tráfego, a influência é feita nos respectivos saltos da seguinte maneira:

Sub-rede do servidor 1 > Branch Edge 01.

Sub-rede 2 do servidor > Branch Edge 01.

Roteamento interno do lado do servidor.

Branch Edge 01 > DC1 cEdge01.

Branch Edge 01 > DC2 cEdge01.

Usar a política de dados centralizada (encadeamento de serviços) para influenciar o caminho do tráfego.

DC1 cEdge01 > FW DC1.

DC2 cEdge01 > FW DC2.

Usar rótulos de serviço para influenciar o caminho de tráfego do SDWAN cEdge para o respectivo FW em DCs.

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

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

O tráfego de origem IP privada do servidor é submetido à NAT para sair do FW a fim de acessar a Internet via CPE.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.