Inserimento servizi mediante criteri dati centralizzati: Un caso di utilizzo esclusivo di Traffic Maneuvering

Sommario

Introduzione

Questo documento descrive uno scenario di esempio in cui il concatenamento dei servizi viene utilizzato per controllare il flusso del traffico in entrata da Internet ai server ospitati nel sito di succursale SDWAN.

Premesse

Il documento mostra anche che utilizzando il concatenamento dei servizi è possibile tenere facilmente traccia dell'errore del collegamento LAN del centro dati (DC) per notificare al router SDWAN della filiale di modificare il percorso del traffico utilizzando la politica dei dati, il che non è possibile altrimenti e senza la quale il traffico oscura facilmente il DC.

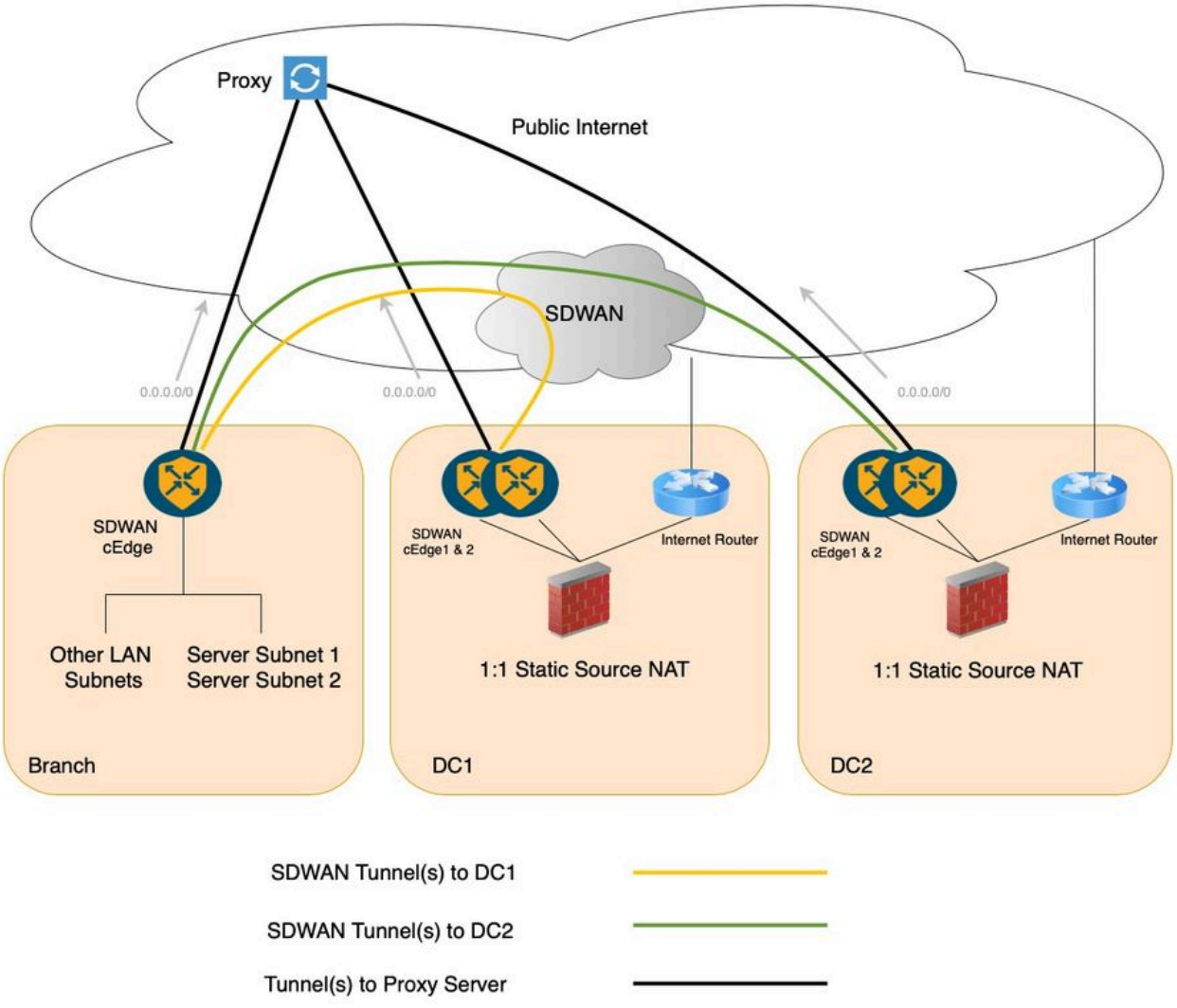
Il traffico in entrata viene instradato attraverso i firewall del controller di dominio per la gestione e la sicurezza.

Topologia di esempio

Per illustrare questo scenario, è stata presa in considerazione un'installazione SDWAN standard

con configurazione a doppio controller di dominio e un sito di succursale, come illustrato nel diagramma successivo. Possono esistere più rami, tuttavia, per semplicità ne è stato raffigurato solo uno. I controller di dominio e i siti di succursale comunicano tramite l'overlay SDWAN protetto, ovvero tramite i tunnel IPSec protetti di SDWAN. In questa configurazione esistente sia i controller di dominio che il sito di succursale dispongono di tunnel per i server proxy nel servizio di Routing e inoltro virtuale (VRF) e il percorso predefinito nel servizio di VRF/VPN punta a questo proxy.

L'impostazione della topologia è costituita da un sito di succursale in cui sono ospitate due subnet di server, Subnet server 1 e Subnet server 2. Esistono due centri dati, in cui ciascun firewall del centro dati esegue un NAT (Static Network Address Translation) con rapporto 1:1 per consentire di raggiungere la rispettiva subnet del server di succursale da Internet. Per essere precisi, il firewall del data center 1 esegue il NAT statico 1:1 per la subnet server 1 e il firewall del data center 2 esegue lo stesso per la subnet server 2.



Requisiti del cliente

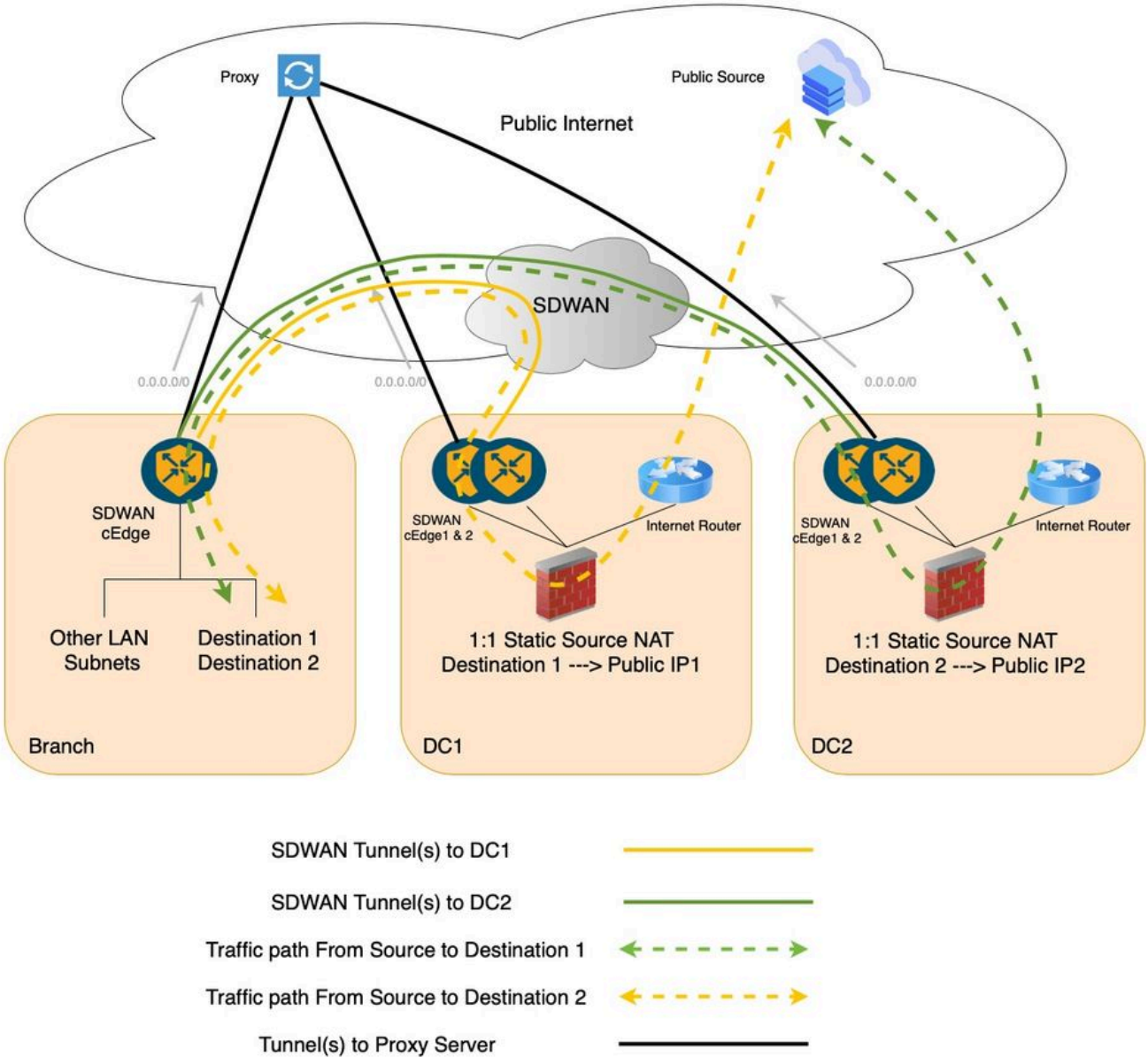
Con la configurazione precedente in mente il cliente può essere come detto:

- L'applicazione pubblica come MS Teams deve accedere a questi server ospitati in Branch.

Come accennato in precedenza, la disponibilità di FW stateful nei controller di dominio richiede al cliente di utilizzarli invece di una connessione diretta in entrata al sito della filiale.

- La subnet server 1 nella diramazione deve essere raggiungibile tramite DC1 e la subnet server 2 nella diramazione deve essere raggiungibile tramite DC2 da Internet.
- Nessun indirizzo IP pubblico deve essere instradato all'interno della rete del cliente.
- Le subnet del server ospitato dalla filiale 1 e 2 sono configurate con IP privati e la conversione da IP privato a IP pubblico deve essere eseguita nei rispettivi firmware dei controller di dominio.
- Non devono essere presenti modifiche del routing di underlay.

Nota: Se non vengono apportate modifiche al flusso di traffico nel controller di dominio o nel sito di succursale, il traffico di inoltro da Internet passerà attraverso i firewall del controller di dominio per raggiungere i server nel sito di succursale. D'altra parte, il traffico di ritorno passerà direttamente attraverso il proxy sul router SDWAN della filiale (usando il percorso predefinito) per raggiungere l'origine Internet. Questo è un flusso asimmetrico di traffico.



Soluzioni possibili

Le soluzioni possibili per i requisiti precedenti possono essere due:

1. Progettazione personalizzata del traffico con criteri di dati centralizzati in cui il traffico è bloccato in caso di errore del collegamento LAN CC.
2. Service Insertion con criteri di gestione centralizzata dei dati in cui il traffico non subisce interruzioni in caso di errore del collegamento LAN del controller di dominio.

1. Progettazione personalizzata del traffico con criteri di dati centralizzati

Se si considerano i criteri dati di Custom Traffic Engineering nel criterio Dati centralizzati, uno per la filiale e un altro per il controller di dominio, il criterio dati della filiale invia il traffico dalla filiale al controller di dominio utilizzando tlocs remoti e il secondo criterio dati instrada ulteriormente il flusso nel controller di dominio dal server cEdge al firewall (FW). Tuttavia, con l'opzione remote-tloc configurata nella filiale, il router SDWAN della filiale non è in grado di rilevare l'errore del

collegamento LAN del router 1 DC SDWAN. In altre parole, se il collegamento LAN al router 1 DC SDWAN non riesce, il router di succursale non è in grado di rilevare il traffico e lo inoltra al router 01 DC SDWAN. Di conseguenza, il traffico può facilmente generare buchi neri nel router 1 DC SDWAN.

Configurazione (con criteri dati personalizzati)

Applicato su router DC SDWAN in direzione tunnel esterno:

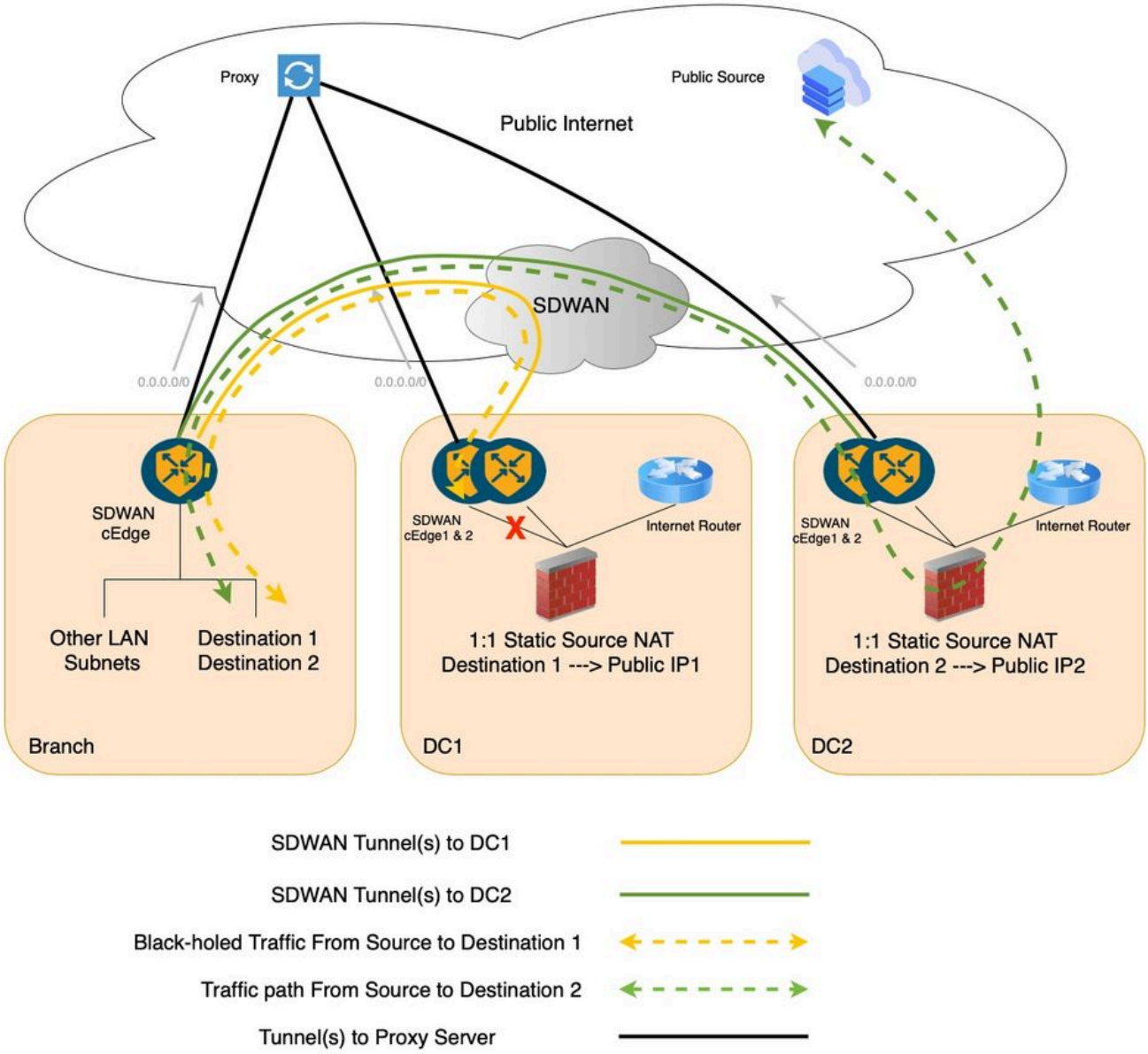
```
data-policy <PolicyName>
vpn-list <VPN_Name>
  sequence 1
     match
      source-data-prefix-list <BranchSiteServerSubnet>
     destination-data-prefix-list <PublicIPSubnet>
     !
     action accept
      set
       next-hop <Firewall_IP>
      !
     !
```

Applicato al router SDWAN della filiale in direzione da-servizio:

```
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
  !
```

Flusso di traffico con criteri dati personalizzati (caso di errore di collegamento 1LAN del router SDWAN DC)

Il traffico è bloccato sul router 1 DC SDWAN in caso di errore del collegamento LAN al router 1 DC SDWAN.



2. Inserimento di servizi con criteri dati centralizzati

Il concatenamento dei servizi Cisco SDWAN è intrinsecamente molto flessibile e completamente automatizzato. In una configurazione WAN legacy. Se è necessario inserire un firewall nel percorso di un flusso di traffico specifico, in genere viene associato a un elevato numero di configurazioni manuali in ogni hop. Al contrario, il processo di inserimento dei servizi Cisco SD-WAN è semplice quanto abbinare il traffico interessante a un controllo centralizzato o a un criterio dei dati, impostare il servizio firewall come hop successivo e quindi applicare il criterio a un elenco di siti di destinazione tramite una singola transazione NETCONF (Network Configuration Protocol) tra Cisco SDWAN Manager e il controller Cisco SDWAN.

Di seguito sono riportati i passaggi per l'inserimento di un firewall come servizio nell'esempio di configurazione:

1. Definire il firewall come servizio sui dispositivi cEdge DC. A tale scopo, è possibile utilizzare modelli di funzionalità VPN e accedere direttamente ai dispositivi. Il rilevamento sul servizio è abilitato per impostazione predefinita, ovvero se il firewall controller di dominio diventa

irraggiungibile dal router primario DC SDWAN cEdge1, l'intero servizio non sarà disponibile e il traffico tornerà al router secondario cEdge2 del controller di dominio.

2. Creare e applicare un criterio dati centralizzato per inserire il servizio FW nel percorso del traffico in modo bidirezionale.

Configurazione (Con Inserimento Servizio)

Configurato sui router SDWAN DC:

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

La configurazione precedente nei router SDWAN del controller di dominio definisce un servizio del tipo 'Firewall' che viene annunciato al controller Cisco SDWAN. Il router SDWAN DC interrompe l'annuncio quando la raggiungibilità al servizio firewall si interrompe o il firewall stesso si interrompe.

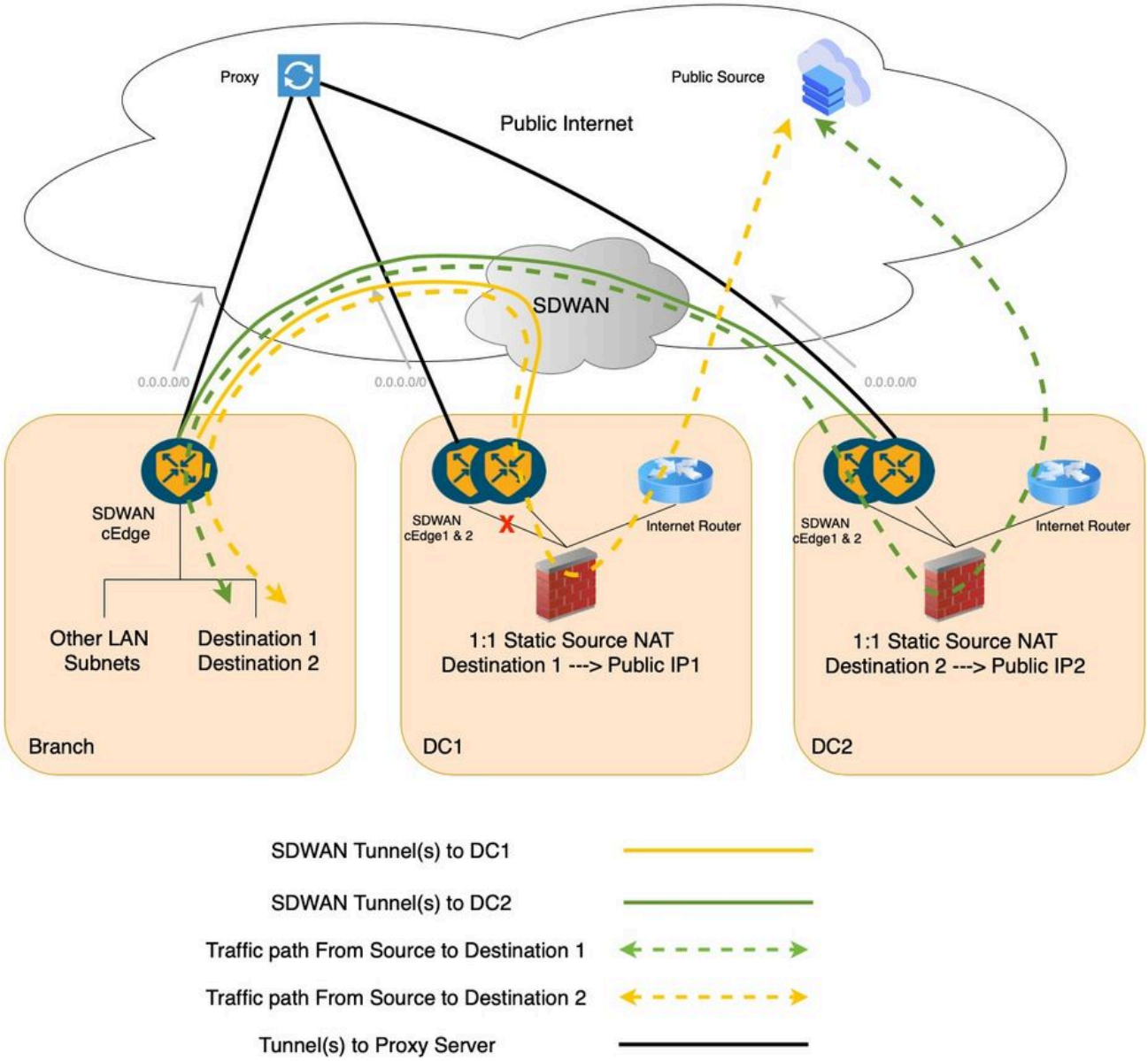
Un criterio di concatenamento dei servizi è definito come applicato al router SDWAN del ramo dalla direzione del servizio:

```
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
  !
```

Flusso di traffico con inserimento servizi (caso di errore di collegamento LAN 1 router SDWAN DC)

Failover del traffico sul router 2 DC SDWAN in caso di errore del collegamento LAN del router 1

DC SDWAN.



I seguenti prerequisiti per i criteri o elenchi predefiniti sono definiti su Cisco Catalyst SDWAN Manager come mostrato di seguito:

```
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
!
!
```

Dettagli sul flusso di traffico per una migliore comprensione

Flusso del traffico dall'esterno all'interno

Origine Internet (MS Teams) > DC1 FW (NAT) > DC1 cEdge01 > Branch cEdge01 > Subnet server 1.

Origine Internet (MS Teams) > DC2 FW (NAT) > DC2 cEdge01 > Branch cEdge01 > Subnet server 2.

Per questo motivo, l'influenza del traffico viene esercitata sui rispettivi hop come segue:

Origine Internet (MS Teams) > DC1 FW.

Origine Internet (MS Teams) > DC2 FW.

I controller di dominio DC1 e DC2 pubblicizzano i rispettivi pool IP pubblici a Internet tramite CPE Internet nei controller di dominio.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

Routing del firewall per la subnet interna.

DC1 cEdge01 > Diramazione cEdge01.

DC2 cEdge01 > Diramazione cEdge01.

Routing Cisco SDWAN tramite overlay Management Protocol (OMP).

Branch cEdge01 > Subnet server 1.

Branch cEdge01 > Subnet server 2.

Routing del router di succursale per la subnet interna.

Flusso del traffico interno-esterno

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

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

Per questo motivo, l'influenza del traffico viene esercitata sui rispettivi hop come segue:

Subnet server 1 > Branch cEdge 01.

Subnet server 2 > Branch cEdge 01.

Routing interno dal lato server.

Branch cEdge 01 > DC1 cEdge01.

Branch cEdge 01 > DC2 cEdge01.

Utilizzo dei criteri dati centralizzati (concatenamento dei servizi) per influenzare il percorso del traffico.

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

Utilizzo di etichette di servizio per influenzare il percorso del traffico da SDWAN cEdge al rispettivo FW nei controller di dominio.

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

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

Il traffico privato IP originato dal server è NAT's in uscita dal FW per raggiungere Internet tramite CPE.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).