إدخال الخدمة باستخدام نهج البيانات المركزي: حالة إستخدام فريدة للمنوارة عبر حركة المرور

المحتويات

المقدمة

يصف هذا المستند سيناريو حيث يتم إستخدام سلسلة الخدمات للتحكم في تدفق حركة المرور الواردة من الإنترنت إلى الخوادم المستضافة في موقع فرع SDWAN.

معلومات أساسية

كما يوضح المستند أنه باستخدام تسلسل الخدمة كيف يمكن تعقب فشل إرتباط شبكة LAN لمركز البيانات (DC) بسهولة إلعالم موجه SDWAN الفرعي لتغيير مسار حركة المرور باستخدام DataApolicy، وهو ما ال يمكن تحقيقه بخالف ذلك وبدون يسهل على حركة المرور قطع الطريق في وحدة التحكم بالمجال.

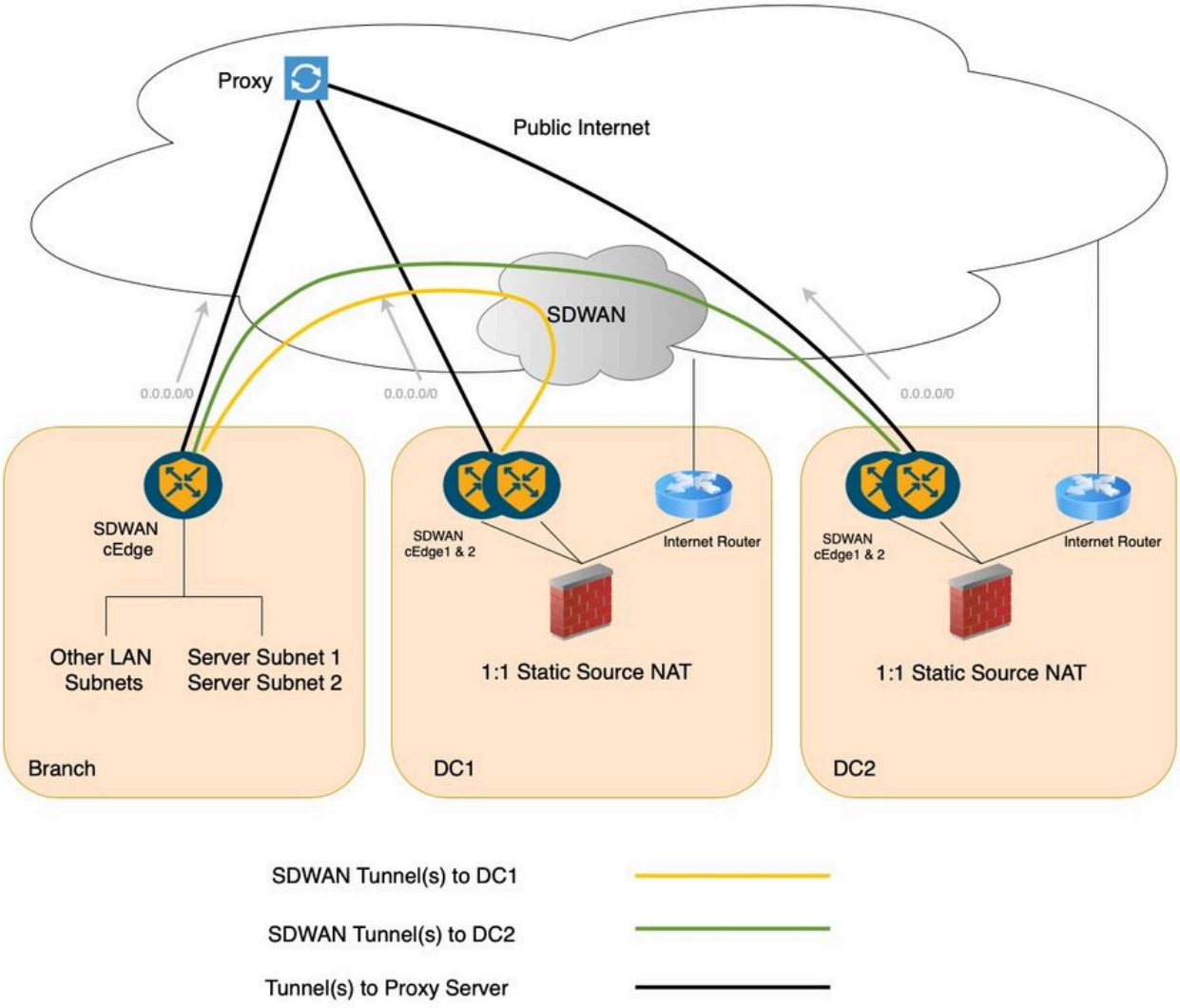
يتم توجيه حركة المرور الواردة هنا من خالل جدران حماية DC للإدارة والأمان.

مثال طبوولوجيا

تم النظر في إمكانية نشر SDWAN القياسية مع إعداد DC مزدوج وموقع فرعي من أجل تصوير هذا السيناريو كما هو موضح في الرسم التخطيطي التالي. ولكن يمكن ان يكون هناك فروع متعددة، ولأجل البساطة جرى تصوير واحد فقط. تتصل وحدات التحكم في الوصول (DC) ومواقع الفروع عبر تغشية SDWAN الآمنة، أي من خالل أنفاق IPSec الآمنة الخاصة بشبكة SDWAN. في هذا الإعداد الحالي، تتضمن كل من وحدة التحكم في الوصول (DCs) وموقع الفرع أنفاقا (أنفاق) إلى الخوادم الوكيل في خدمة التوجيه وإعادة التوجيه

الظاهري (VRF) ويشير المسار الافتراضي في الخدمة VRF/الشبكة الخاصة الظاهرية (VPN) إلى هذا الوكيل.

يتكون إعداد المخطط هذا من موقع فرعي يتم فيه إستضافة شبكتين فرعيتين للخوادم وشبكة الخادم الفرعية 1 وشبكة الخادم الفرعية 2. هناك مركزان للبيانات، حيث يقوم كل واحد من جدران حماية مركز البيانات بإجراء ترجمة عنوان الشبكة (NAT) الثابتة 1:1 للسماح بالوصول إلى الشبكة الفرعية للخادم الفرعي ذات الصلة من الإنترنت. لكي تكون أكثر دقة، يقوم جدار حماية مركز البيانات 1 بتنفيذ وحدة الشبكة (NAT) الثابتة 1:1 للشبكة الفرعية للخادم 1 ويقوم جدار حماية مركز البيانات 2 بتنفيذ الأمر نفسه للشبكة الفرعية للخادم 2.



متطلبات العميل

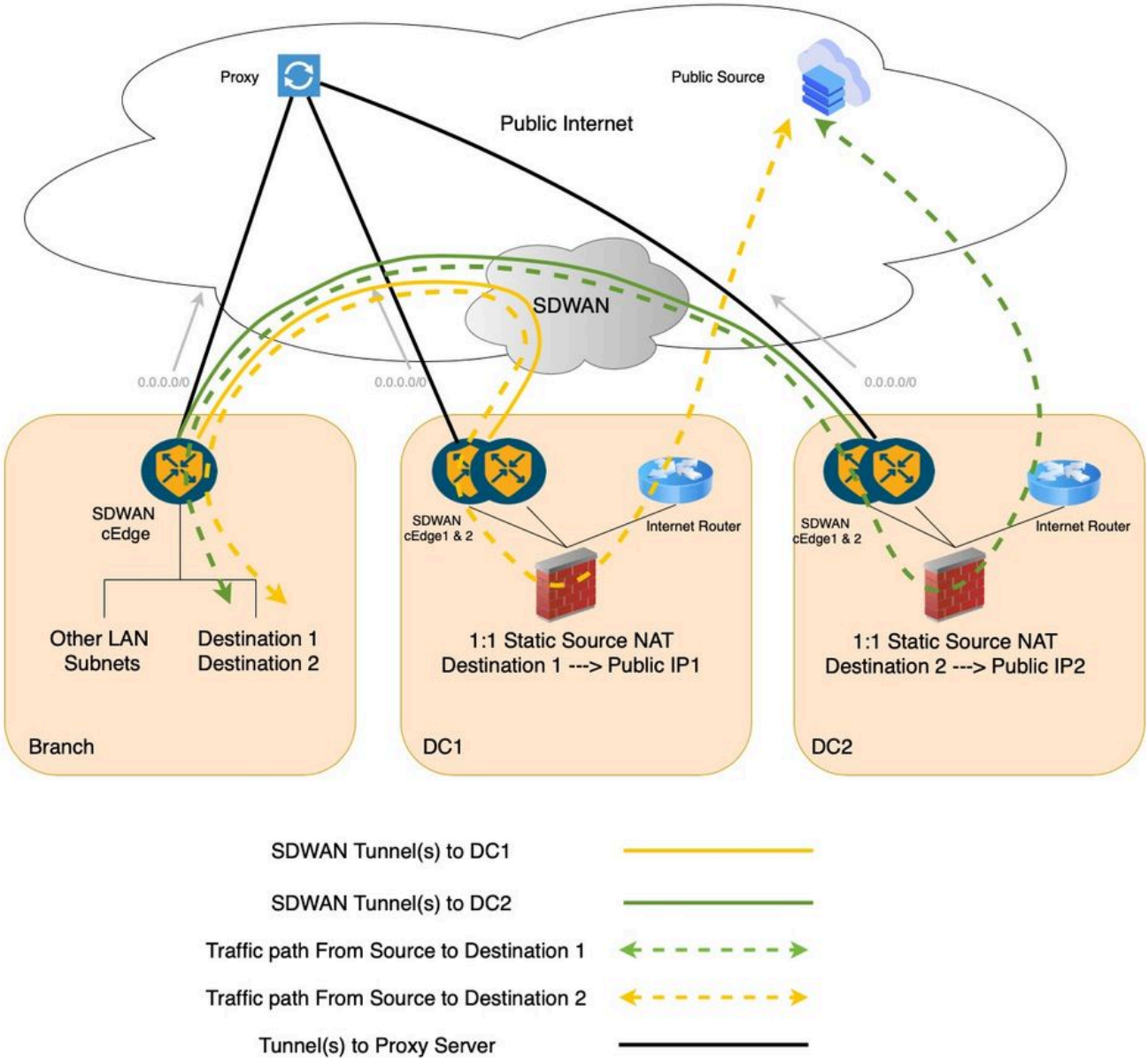
مع مراعاة الإعداد السابق، يمكن أن يكون الطلب المقدم من العميل كما هو مذكور:

- يجب على التطبيق العام مثل MS Teams الوصول إلى هذه الخوادم المستضافة في الفرع. وكما ذكرنا مسبقا، فإن توفر الأجهزة التي تحتوي على مواد ثابتة (FW) ذات حالة في مراكز البيانات يجعل العميل يطلب إستخدامها بدلا من الاتصال المباشر الوارد إلى موقع الفرع.
- يجب أن تكون الشبكة الفرعية للخادم 1 الموجودة في الفرع قابلة للوصول إليها عبر

DC1، كما يجب أن تكون الشبكة الفرعية للخادم 2 الموجودة في الفرع قابلة للوصول إليها عبر DC2 من الإنترنت.

- يجب عدم توجيه أي عنوان IP عام داخل شبكة العميل.
- تم تكوين الشبكات الفرعية للخادم المستضاف للفرع 1 و 2 باستخدام عناوين IP الخاصة ويجب أن تحدث ترجمة IP الخاصة إلى العامة في شبكات DC الخاصة.
- يجب ألا تكون هناك أي تغييرات تحشد أساسية.

ملاحظة: في حالة عدم إجراء أية تغييرات على تدفق حركة المرور سواء في موقع وحدة التحكم بالمجال (DC) أو موقع الفرع، سيتم نقل حركة المرور الأمامية من الإنترنت عبر جدران حماية وحدة التحكم بالمجال (DC) للوصول إلى الخوادم في موقع الفرع. من ناحية أخرى، سوف تمر حركة المرور العائدة مباشرة من خلال الوكيل في موجه SDWAN الفرعي (باستخدام المسار الافتراضي) للوصول إلى مصدر الإنترنت. هذا تدفق غير متماثل لحركة المرور.



الحلول الممكنة

قد يكون هناك حالان محتملان لتلبية المتطلبات السابقة:

1. هندسة حركة مرور مخصصة مع سياسة بيانات مركزية حيث يتم العثور على ثغرات حركة مرور البيانات في حالة فشل إرتباط شبكة LAN الخاصة بالتاي المستمر.
2. إدخال الخدمة مع نهج البيانات المركزي حيث ال يتم تعطيل حركة مرور البيانات في حالة فشل إرتباط شبكة LAN الخاصة بوحدة التحكم بالمجال DC.

1. هندسة حركة المرور المخصصة مع سياسة بيانات مركزية

إذا تم الأخذ في الاعتبار سياسات بيانات هندسة حركة المرور المخصصة في إطار نهج البيانات المركزية، واحدة للفرع وأخرى للتاي المستمر، فإن نهج البيانات الفرعية يرسل حركة مرور البيانات من الفرع إلى وحدة التحكم بالمجال عن بعد بينما يقوم نهج البيانات الثاني بتوجيه تدفق البيانات داخل وحدة التحكم بالمجال من cEdge إلى جدار الحماية (FW). ولكن، مع خيار وحدة التحكم عن بعد الذي تم تكوينه في الفرع، ال يدرك موجه SDWAN للفرع فشل في موجه DC SDWAN 1 LAN. وهذا يعني، في حالة فشل إرتباط شبكة LAN في موجه SDWAN DC 1، حينئذ، أن موجه الفرع ال يزال يقوم بتوجيهها إلى موجه SDWAN DC 01. وبالتالي، فإنه يتم نقل البيانات بسهولة إلى الثقوب السوداء في موجه DC SDWAN Router 1.

التكوين (باستخدام نهج البيانات المخصص)

يتم تطبيقها على موجه SDWAN من النفق:

```
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>
      !
     !
```

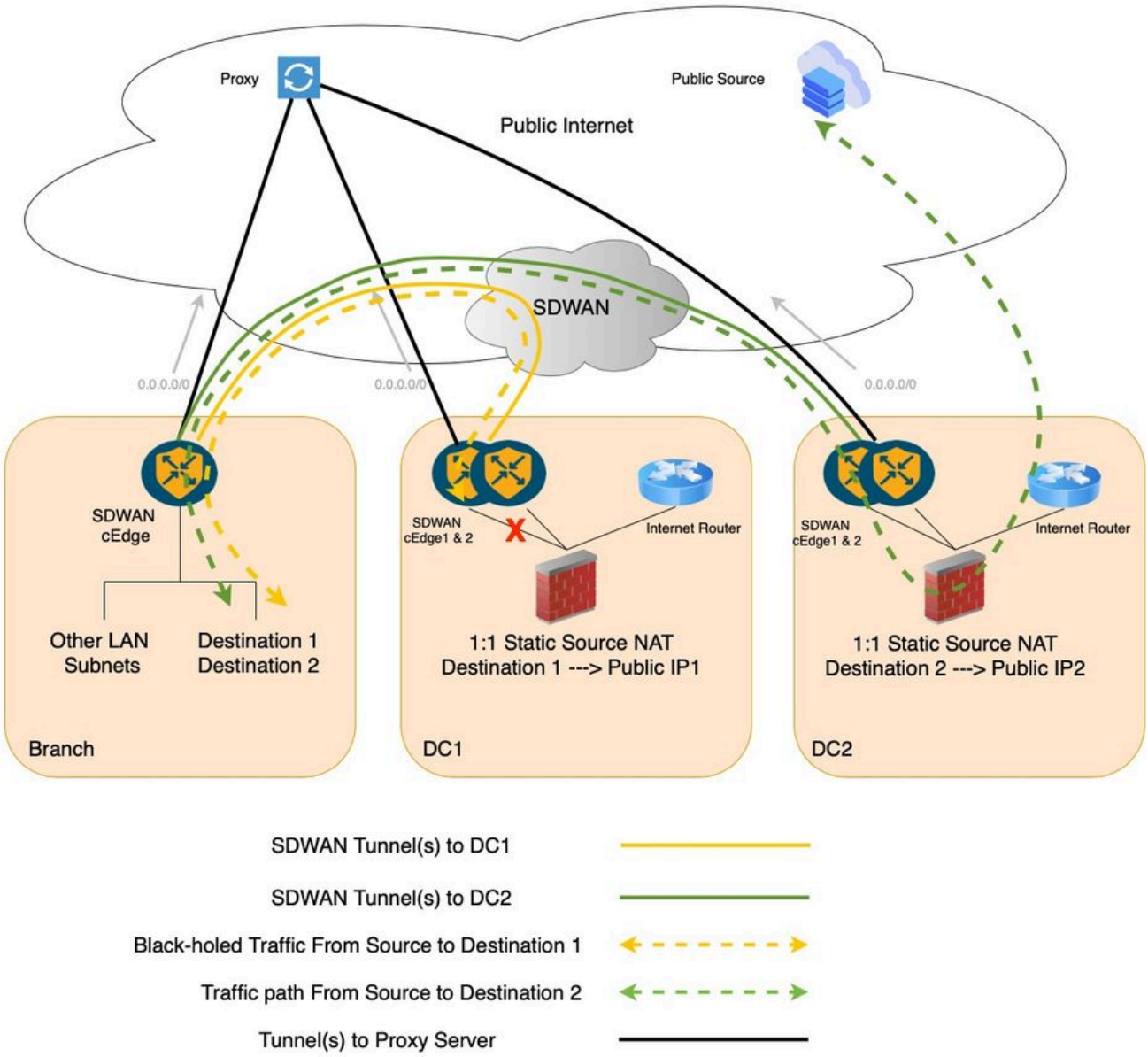
تم التطبيق على موجه SDWAN الفرعي من إتجاه الخدمة:

```
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
!
```

تدفق حركة المرور مع سياسة البيانات المخصصة (حالة فشل موجه DC SDWAN 1 LAN Link)

الفتحات المرورية في موجه SDWAN DC 1 في حالة فشل موجه DC SDWAN 1 LAN.



2. إدخال الخدمة مع سياسة البيانات المركزية

سلسلة خدمة SDWAN من Cisco تتسم بطبيعتها بمرونة كبيرة وتلقائية بالكامل. في

إعداد شبكة WAN القديمة. إذا تنك ةجاحب إلى إدراج جدار ةيامح يف راسم ةكرح رورم ددحم، فإنه يقترن ةداع بالعديد نم عمليات التكوين اليدوي في كل ةوطخ. على النقيض نم ذلك، فإن عملية إدخال ةمدخ SD-WAN نم Cisco يه ةطيسب لثم ةقباطم ةكرح رورم ةريثم اللاهتمام قيبطت مث ،ةيلاتلا تاوطخلا، ةيامحلا رادج ةمدخ نييعتو ،تانايب ةسايس وأ يزكرم مكحت عم (NETconf) دحاو ةكبش نيوكت لوكوتورب ةلماعم ربع ةفدهتسم عقاوم ةمئاق ىلع ةسايسلا نم إدارة SDWAN نم Cisco إلى وحدة التحكم SDWAN.

فيما يلي الخطوات الخاصة بإدراج جدار حماية كخدمة في المثال التكوين الخاص بنا:

1. تعريف جدار الحماية كخدمة على أجهزة DC cEdge. ويمكن تحقيق ذلك باستخدام قوالب ميزة الشبكة الخاصة الظاهرية (VPN) بالإضافة إلى تسجيل الدخول المباشر إلى الأجهزة. يتم تمكين التعقب على الخدمة بشكل افتراضي، مما يعني أنه إذا أصبح جدار حماية DC غير قابل للوصول إليه من DC SDWAN الرئيسي الموجه cEdge1، فستتعطل الخدمة بالكامل، وستتراجع حركة مرور البيانات إلى الموجه الثانوي cEdge2 من DC.

2. إنشاء سياسة بيانات مركزية وتطبيقها لإدراج خدمة FW في مسار حركة المرور بشكل ثنائي الإتجاه.

التكوين (مع إدخال الخدمة)

تم التكوين على موجهات DC SDWAN:

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

يحدد التكوين السابق في موجهات SDWAN لـ DC خدمة من النوع "جدار الحماية" التي يتم الإعلان عنها لوحدة التحكم في SDWAN من Cisco. يتوقف موجه SDWAN لـ DC عن الإعلان عن جدار الحماية أو يتوقف عن الخدمة إذا فقد إمكانية الوصول إلى جدار الحماية نفسه.

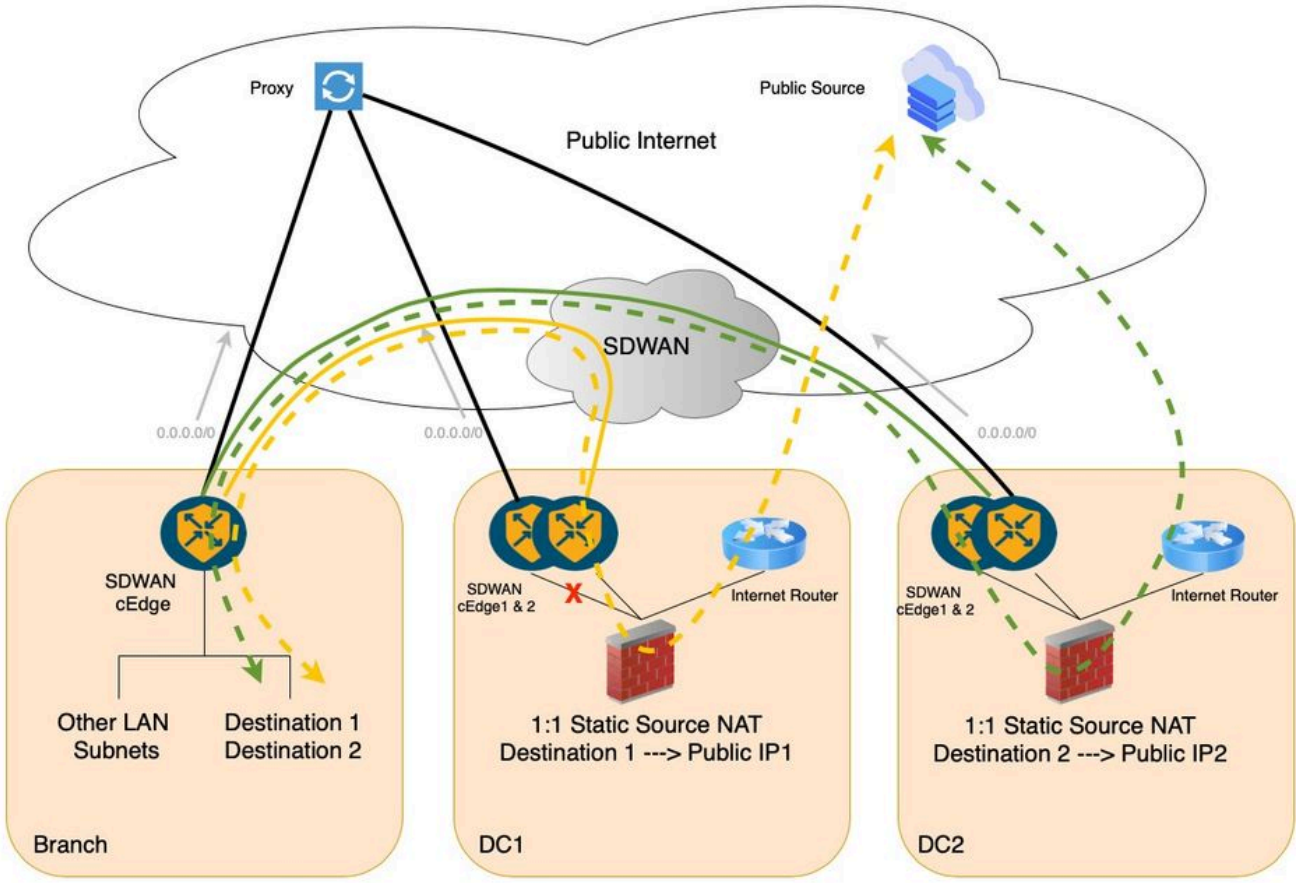
يتم تحديد سياسة سلسلة الخدمات كسياسة يتم تطبيقها على موجه SDWAN الفرعي من إتجاه الخدمة:

```
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
!
```

تدفق حركة المرور مع إدخال الخدمة (حالة فشل فشل موجه DC SDWAN 1 LAN Link)

يفشل حركة المرور إلى موجه SDWAN DC 2 في حالة فشل إرتباط موجه DC SDWAN 1 LAN.



يتم تحديد متطلبات النهج الأساسية هذه أو القوائم المحددة مسبقا على مدير Cisco Catalyst SDWAN كما هو موضح للمرجع:

```
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
!
!
```

تفاصيل تدفق حركة المرور للحصول على فهم أفضل

خارج إلى داخل تدفق حركة المرور

مصدر الإنترنت (MS Teams) > DC1 FW (NAT) > DC1 cEdge01 > Branch cEdge01 > الشبكة الفرعية للخادم 1.

مصدر إنترنت (MS Teams) > DC2 FW (NAT) > DC2 cEdge01 > Branch cEdge01 > الشبكة الفرعية للخادم 2.

ويتم هذا التأثير على حركة المرور في نقطتي الأراضي على النحو التالي:

مصدر الإنترنت (MS Teams) > DC1 FW.

مصدر الإنترنت (MS Teams) > DC2 FW.

إعلان DC1 و DC2 عن تجمع IP العام الخاص إلى الإنترنت عبر Internet CPE في DCs.

DC1 FW > DC1 cEdge01.

DC2 FW > DC2 cEdge01.

توجيه جدار الحماية للشبكة الفرعية الداخلية.

الطرازdc1 cEdge01 > الخادم الفرعي cEdge01.

الطراز DC2 cEdge01 > الخادم الفرعي cEdge01.

تغليف Cisco SDWAN Routing من خلال بروتوكول إدارة التغشية (OMP).

الخادم الفرعي cEdge01 > الشبكة الفرعية للخادم 1.

الخادم الفرعي cEdge01 > الشبكة الفرعية للخادم 2.

توجيه موجه الفرع للشبكة الفرعية الداخلية.

الدخل إلى تدفق حركة المرور الخارجية

شبكة الخادم الفرعية 1 > Branch cEdge 01 > DC1 cEdge01 > DC1 FW (NAT) > مصدر الإنترنت (MS Teams).

شبكة الخادم الفرعية 2 > Branch cEdge 01 > DC2 cEdge01 > DC2 FW (NAT) > مصدر الإنترنت (MS Teams).

ويتم هذا التأثير على حركة المرور في نقطتي الأراضي على النحو التالي:

شبكة الخادم الفرعية 1 > الخادم الفرعي 01.

شبكة الخادم الفرعية 2 > الخادم الفرعي 01.

التوجيه الداخلي من جانب الخادم.

الخادم Branch cEdge 01 > DC1 cEdge01.

الخادم طرار cEdge 01 للفرع > الطرار dc2 cEdge01.

إستخدام سياسة البيانات المركزية (سلسلة الخدمات) للتأثير على مسار حركة المرور.

DC1 cEdge01 > DC1 FW.

DC2 cEdge01 > DC2 FW.

إستخدام تسميات الخدمات للتأثير على مسار حركة مرور البيانات من خادم SDWAN إلى وضع FW في الصلة في مراكز البيانات.

DC1 FW (NAT) > مصدر الإنترنت (MS Teams).

DC2 FW (NAT) > مصدر الإنترنت (MS Teams).

حركة مرور IP الخاصة المستمدة من الخادم NATed للخروج من FW للوصول إلى الإنترنت عبر CPE.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).