So wählen Sie eine bestimmte Website als bevorzugte regionale Internet-Breakout aus:

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die SD-WAN-Fabric so konfiguriert wird, dass der vEdge in einer bestimmten Zweigstelle mithilfe von Direct Internet Access (DIA) und einer zentralen Datenrichtlinie als bevorzugtes regionales Internet-Breakout konfiguriert wird. Diese Lösung könnte beispielsweise dann nützlich sein, wenn ein regionaler Standort einen zentralisierten Service wie Zscaler® nutzt und als bevorzugter Internet-Ausgangspunkt verwendet werden sollte. Für eine solche Bereitstellung müssen Generic Routing Encapsulation (GRE) oder Internet Protocol Security (IPSec)-Tunnel von einem Transport-VPN konfiguriert werden, und der Datenfluss unterscheidet sich von der normalen DIA-Lösung, bei der der Datenverkehr direkt ins Internet gelangt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in diesem Bereich zu verfügen:

- Grundlegende Kenntnisse des SD-WAN-Richtlinien-Framework

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

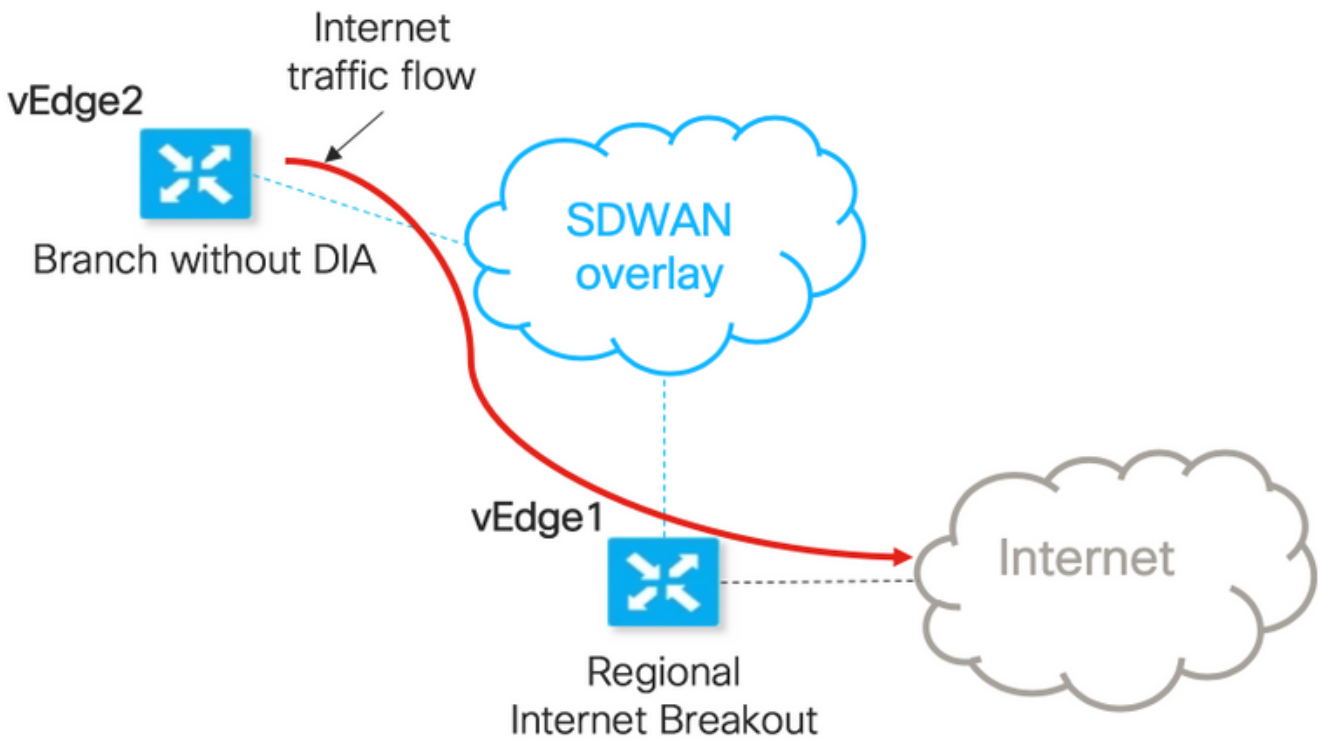
- vEdge-Router

- vSmart Controller mit Softwareversion 18.3.5

Hintergrundinformationen

Service-VPN-Datenverkehr vom vEdge2, der ins Internet gelangen sollte, wird mithilfe von Datenebenentunneln an einen anderen vEdge1 der Außenstelle weitergeleitet. vEdge1 ist der Router, auf dem die DIA für das lokale Internet-Breakout konfiguriert ist.

Netzwerkdiagramm



Hostname	vEdge1	vEdge2
Hostrolle	Zweigstellengerät mit DIA (Regional Internet Breakout)	Zweigstellengerät ohne konfiguri DIA
VPN 0		
Transportstandorte (TLOC) 1	biz-internet, ip: 192.168.110.6/24	biz-internet, ip: 192.168.110.5/24
Transportstandorte (TLOC) 2	public-internet, ip: 192.168.109.4/24	public-internet, ip: 192.168.109.5
Service-VPN 40	Schnittstelle ge0/1, ip: 192.168.40.4/24	Schnittstelle ge0/2, ip: 192.168.50.5/24

Konfigurationen

Lösung 1: Zentralisierte Nutzung von Datenrichtlinien für Next-Hop-Änderungen

vEdge2 verfügt über einen Datenebenentunnel, der mit vEdge1 und anderen Standorten eingerichtet wurde (Full-Mesh-Konnektivität).

Für vEdge1 ist DIA mit **ip route 0.0.0.0/0 vpn 0** konfiguriert.

vSmart zentralisierte Datenrichtlinienkonfiguration:

```
policy
 data-policy DIA_vE1
  vpn-list VPN_40
   sequence 5
    match
     destination-data-prefix-list ENTERPRISE_IPs
    !
    action accept
    !
   !
   sequence 10
    action accept
     set
      next-hop 192.168.40.4
     !
    !
   !
   default-action accept
  !
 !
!
lists
  vpn-list VPN_40
   vpn 40
  !
  data-prefix-list ENTERPRISE_IPs
   ip-prefix 10.0.0.0/8
   ip-prefix 172.16.0.0/12    ip-prefix 192.168.0.0/16 ! apply-policy site-list SITE2 data-
policy DIA_vE1 from-service
```

vEdge2 - Keine spezielle Konfiguration erforderlich.

Hier finden Sie die Schritte zur Überprüfung, ob eine Richtlinie ordnungsgemäß angewendet wurde.

1. Überprüfen Sie, ob die Richtlinie vom vEdge2 fehlt:

```
vedge2# show policy from-vsmart
% No entries found.
```

2. Überprüfen Sie die Programmierung der Forwarding Information Base (FIB). Es sollte die Route Abwesenheitsmeldung (Blackhole) für das Ziel im Internet anzeigen:

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole
```

3. Anwendung von vSmart-Datenrichtlinien im Abschnitt "**Anwendungs-Richtlinien**" der vSmart-Konfiguration oder Aktivierung in der vManage-GUI

4. Überprüfen Sie, ob vEdge2 erfolgreich Datenrichtlinien von vSmart erhalten hat:

```
vedge2# show policy from-vsmart
from-vsmart data-policy DIA_vE1
 direction from-service
 vpn-list VPN_40
  sequence 5
```

```
   match
    destination-data-prefix-list ENTERPRISE_IPs
   action accept
  sequence 10
   action accept
    set
     next-hop 192.168.40.4
  default-action accept
from-vsmart lists vpn-list VPN_40
 vpn 40
from-vsmart lists data-prefix-list ENTERPRISE_IPs
 ip-prefix 10.0.0.0/8
 ip-prefix 172.16.0.0/12
 ip-prefix 192.168.0.0/16
```

5. Überprüfen Sie die FIB-Programmierung (Forwarding Information Base), die mögliche Routen für das Ziel im Internet anzeigt:

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 4
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.110.6 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.110.6 12346 Color: public-internet
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.109.4 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.109.4 12346 Color: public-internet
```

6. Erreichbarkeit zum Ziel im Internet bestätigen:

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.392 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.346 ms
^C
--- 173.37.145.84 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.345/0.361/0.392/0.021 ms
```

Hier finden Sie die vEdge1-Konfigurationsschritte.

1. Aktivieren Sie Network Address Translation (NAT) auf der Transportschnittstelle, wobei DIA verwendet werden sollte:

```
vpn 0
 !
 interface ge0/0
  description "DIA interface"
  ip address 192.168.109.4/24
 nat <<<<==== NAT activated for a local DIA !
```

2. Hinzufügen der statischen Route **ip route 0.0.0.0/0 vpn 0** in einem Service-VPN, um die DIA zu aktivieren:

```
vpn 40
```

```
 interface ge0/4
  ip address 192.168.40.4/24
  no shutdown
 !
 ip route 0.0.0.0/0 vpn 0     <<<<==== Static route for DIA !
```

3. Überprüfen Sie, ob RIB eine NAT-Route enthält:

```
vedge1# show ip route vpn 40 | include nat
40 0.0.0.0/0 nat - ge0/0 - 0 - - - F,S
```

4. Bestätigen Sie, dass DIA funktioniert und die Sitzung Internet Control Message Protocol (ICMP) vom vEdge2 zum 173.37.145.84 in NAT-Übersetzungen angezeigt wird.

```
vedge1# show ip nat filter | tab

                              PRIVATE                         PRIVATE  PRIVATE
PUBLIC  PUBLIC
NAT  NAT                      SOURCE          PRIVATE DEST    SOURCE   DEST     PUBLIC SOURCE
PUBLIC DEST    SOURCE  DEST    FILTER        IDLE          OUTBOUND  OUTBOUND   INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS         ADDRESS         PORT     PORT     ADDRESS
ADDRESS        PORT    PORT    STATE         TIMEOUT      PACKETS   OCTETS     PACKETS  OCTETS
DIRECTION
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
------
0 ge0/0 40 icmp 192.168.50.5 173.37.145.84 9269 9269 192.168.109.4 173.37.145.84 9269 9269
established 0:00:00:02 10 840 10 980 -
```

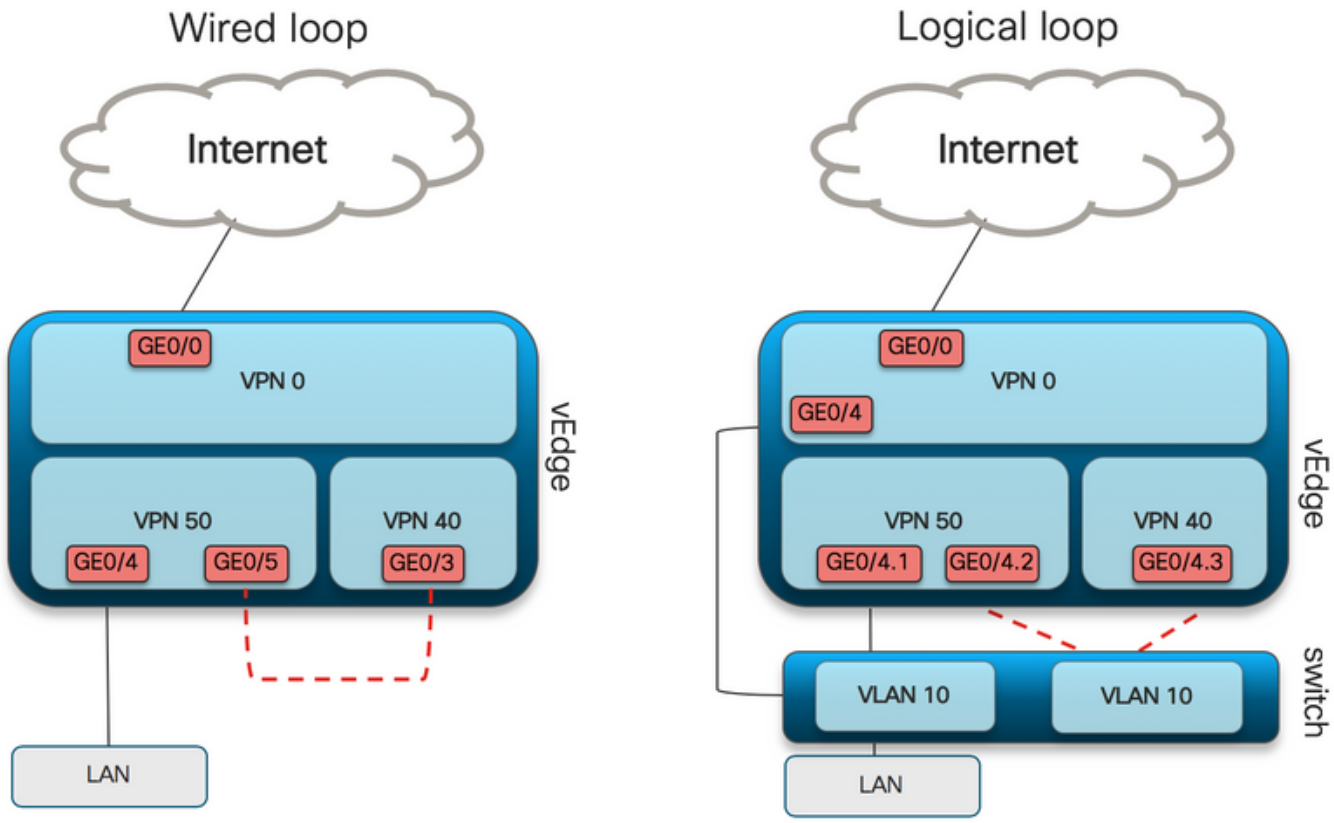
> **Hinweis:** Diese Lösung ermöglicht es uns nicht, Redundanz oder Lastverteilung mit verschiedenen regionalen Ausgängen zu organisieren.
>
> Funktioniert nicht mit IOS-XE-Routern

Lösung 2: Injizieren erforderlich GRE\IPSec\NAT Default Route to OMP.

Derzeit besteht keine Möglichkeit, das Standard-Routing, das auf GRE\IPSec-Tunnel auf vEdge1 verweist, über OMP an vEdge2 anzukündigen (nat route OMP-Protokoll neu zu verteilen). Bitte beachten Sie, dass sich das Verhalten bei zukünftigen Softwareversionen ändern kann.

Unser Ziel ist es, eine reguläre statische Standardroute (**IP-Route 0.0.0.0/0 <Next-Hop-IP-Adresse>**) zu erstellen, die von vEdge2 (Gerät bevorzugt für DIA) ausgehen und über OMP weiter verbreitet werden kann.

Zu diesem Zweck wird auf dem vEdge1 ein Dummy-VPN erstellt, und es wird eine physische Portschleife mit Kabel durchgeführt. Zwischen den Ports, die einem Dummy-VPN zugewiesen sind, und dem Port im gewünschten VPN wird eine Schleife erstellt, die eine statische Standardroute erfordert. Sie können auch eine Schleife mit nur einer physischen Schnittstelle erstellen, die mit einem Dummy-VLAN verbunden ist, und zwei Subschnittstellen, die entsprechenden VPNs auf der Abbildung unten zugeordnet sind:



Hier finden Sie ein vEdge1-Konfigurationsbeispiel.

1. Erstellen eines Dummy-VPNs:

```
vpn 50
 interface ge0/3
description DIA_for_region ip address 192.168.111.2/30 no shutdown ! ip route 0.0.0.0/0 vpn 0
<<<<==== NAT activated for a local DIA
 ip route 10.0.0.0/8 192.168.111.1 <<<<==== Reverse routes, pointing to loop interface GE0/3
ip route 172.16.0.0/12 192.168.111.1
ip route 192.168.0.0/16 192.168.111.1 !
```

2. Überprüfen Sie, ob die DIA-Route, die auf die NAT-Schnittstelle verweist, der Routing-Tabelle erfolgreich hinzugefügt wurde:

```
vedge1# show ip route vpn 50 | i nat
50     0.0.0.0/0 nat - ge0/0 - 0 - - - F,S
```

3. Service-VPN, das für Produktionszwecke verwendet wird und für das eine normale Standardroute konfiguriert wird (die OMP ankündigen kann):

```
vpn 40
 interface ge0/4
  description CORPORATE_LAN
  ip address 192.168.40.4/24
  no shutdown
 !
 interface ge0/5
description LOOP_for_DIA ip address 192.168.111.1/30 no shutdown ! ip route 0.0.0.0/0
192.168.111.2 <<<<==== Default route, pointing to loop interface GE0/5 omp advertise connected
advertise static ! !
```

4. Überprüfen Sie die RIB auf das Vorhandensein einer Standardroute, die auf die

Schleifenschnittstelle verweist:

```
vedge1# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 static - ge0/5 192.168.111.2 - - - - F,S
```

5. Überprüfen Sie, ob vEdge1 das Standard-Routing über OMP angekündigt hat:

```
vedge1# show omp routes detail | exclude not\ set

-------------------------------------------------
omp route entries for vpn 40 route 0.0.0.0/0 <<<<==== Default route OMP entry ------------------
-------------------------------- RECEIVED FROM: peer 0.0.0.0 <<<<==== OMP route is locally
originated path-id 37 label 1002 status C,Red,R Attributes: originator 192.168.30.4 type
installed tloc 192.168.30.4, public-internet, ipsec overlay-id 1 site-id 13 origin-proto static
origin-metric 0 ADVERTISED TO: peer 192.168.30.3 Attributes: originator 192.168.30.4 label 1002
path-id 37 tloc 192.168.30.4, public-internet, ipsec site-id 13 overlay-id 1 origin-proto static
origin-metric 0
```

6. vEdge2 erfordert keine Konfiguration, die Standardroute wird über OMP empfangen, was auf vEdge1 zeigt.

```
vedge2# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 omp - - - - 192.168.30.4 public-internet ipsec F,S
```

7. Erreichbarkeit bis 173.37.145.84 bestätigen:

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=2 ttl=62 time=0.518 ms
64 bytes from 173.37.145.84: icmp_seq=5 ttl=62 time=0.604 ms
^C
--- 192.168.109.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.518/0.563/0.604/0.032 ms
```

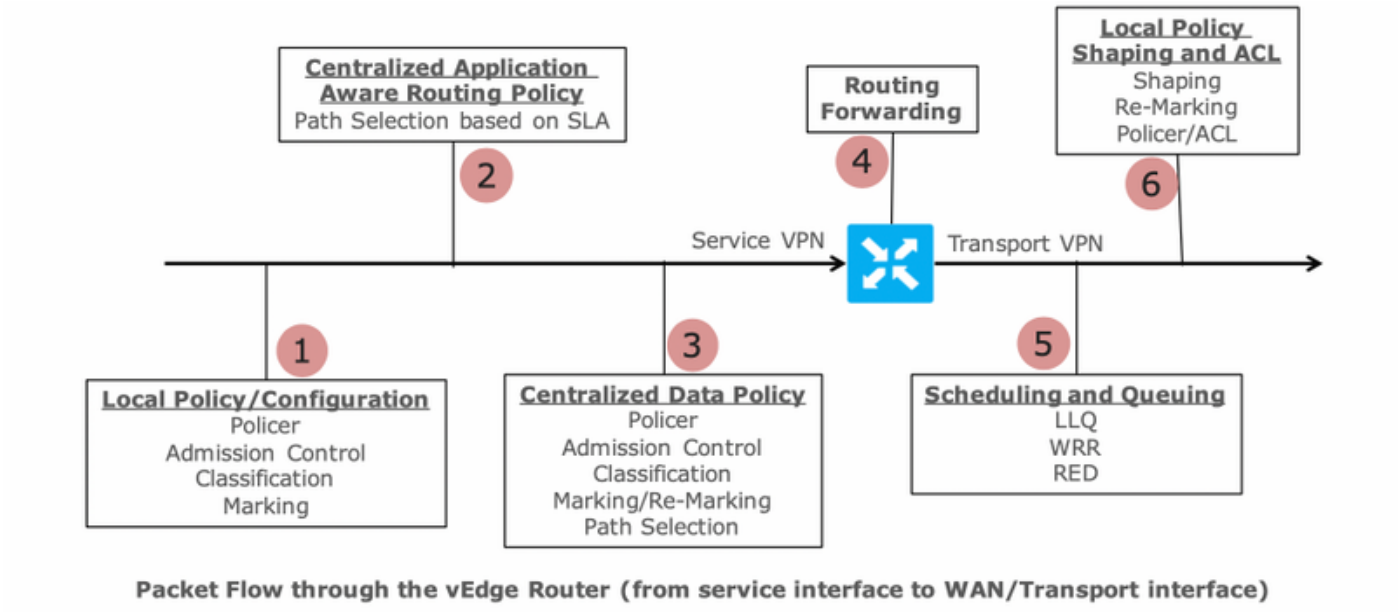
Hinweis: Mit dieser Lösung können Sie Redundanz oder Lastverteilung mit verschiedenen regionalen Ausgängen organisieren.

Funktioniert nicht mit IOS-XE-Routern

Lösung 3: Bei Verwendung einer zentralen Datenrichtlinie für DIA wird die Standardroute zum OMP injiziert.

Wenn für die lokale DIA eine zentrale Datenrichtlinie verwendet wird, um die Standardroute einzufügen, verweist sie auf ein regionales Gerät mit DIA, das die Verwendung dieser statischen Standardroute darstellt: **ip route 0.0.0.0/0 Null0**.

Aufgrund des internen Paketflusses erreicht Datenverkehr, der von Zweigstellen ankommt, die DIA mithilfe der Datenrichtlinie und erreicht niemals die Route zu Null0. Wie Sie hier sehen können, erfolgt die Next-Hop-Suche nur nach einer Richtlinienbereitstellung.



Packet Flow through the vEdge Router (from service interface to WAN/Transport interface)

vEdge2 verfügt über einen Datenebenentunnel, der mit vEdge1 und anderen Standorten eingerichtet wurde (Full-Mesh-Konnektivität). Es ist keine spezielle Konfiguration erforderlich.

Für vEdge1 ist DIA mit einer zentralisierten Datenrichtlinie konfiguriert.

Hier finden Sie die vEdge1-Konfigurationsschritte.

1. Aktivieren Sie Network Address Translation (NAT) auf der Transportschnittstelle, wobei DIA verwendet werden sollte:

```
vpn 0
 !
 interface ge0/0
  description "DIA interface"
  ip address 192.168.109.4/24
 nat <<<<==== NAT activated for a local DIA !
```

2. Fügen Sie in einem Service-VPN statische Route **ip route 0.0.0.0/0 null0 hinzu**, um Verzweigungen Standardangaben anzukündigen:

```
vpn 40
 interface ge0/4
  ip address 192.168.40.4/24
  no shutdown
 !
 ip route 0.0.0.0/0 null0     <<<<==== Static route to null0 that will be advertised to branches
via OMP !
```

3. Überprüfen Sie, ob RIB Standardroute enthält:

```
vedge1# show ip route vpn 40 | include 0.0.0.0
40 0.0.0.0/0 static - - - 0 - - - B,F,S
```

4. Überprüfen Sie, ob vEdge1 das Standard-Routing über OMP angekündigt hat:

```
vedge1# show omp routes detail | exclude not\ set
```

```
-------------------------------------------------
omp route entries for vpn 40 route 0.0.0.0/0 <<<<==== Default route OMP entry ------------------
-------------------------------- RECEIVED FROM: peer 0.0.0.0 <<<<==== OMP route is locally
originated path-id 37 label 1002 status C,Red,R Attributes: originator 192.168.30.4 type
installed tloc 192.168.30.4, public-internet, ipsec overlay-id 1 site-id 13 origin-proto static
origin-metric 0 ADVERTISED TO: peer 192.168.30.3 Attributes: originator 192.168.30.4 label 1002
path-id 37 tloc 192.168.30.4, public-internet, ipsec site-id 13 overlay-id 1 origin-proto static
origin-metric 0
```

5. Stellen Sie sicher, dass die Richtlinie auf vEdge1 nicht vorhanden ist und dass DIA nicht aktiviert ist:

```
vedge1# show policy from-vsmart
% No entries found.
```

6. Überprüfen Sie die Programmierung der Forwarding Information Base (FIB). Es sollte Route Abwesenheitsmeldungen (Blackhole) für das Ziel im Internet anzeigen, da DIA nicht aktiviert ist:

```
vedge1# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Blackhole
```

vSmart zentralisierte Datenrichtlinienkonfiguration für DIA:

```
policy
 data-policy DIA_vE1
  vpn-list VPN_40
   sequence 5
    match
     destination-data-prefix-list ENTERPRISE_IPs
    action accept
   sequence 10
    action accept
     nat-use vpn0             <<<<==== NAT reference for a DIA default-action accept lists
vpn-list VPN_40    vpn 40   data-prefix-list ENTERPRISE_IPs    ip-prefix 10.0.0.0/8    ip-prefix
172.16.0.0/12    ip-prefix 192.168.0.0/16
site-list SITE1
site-id 1001 apply-policy site-list SITE1 <<<<==== policy applied to vEdge1 data-policy DIA_vE1
from-service
```

Anwendung von vSmart-Datenrichtlinien im Abschnitt "**Anwendungs-Richtlinien**" der vSmart-Konfiguration oder Aktivierung in der vManage-GUI

7. Überprüfen Sie, ob vEdge1 erfolgreich Datenrichtlinien von vSmart erhalten hat:

```
vedge1# show policy from-vsmart
from-vsmart data-policy DIA_vE1
 direction from-service
 vpn-list VPN_40
  sequence 5
   match
    destination-data-prefix-list ENTERPRISE_IPs
   action accept
  sequence 10
   action accept
nat-use vpn0 default-action accept from-vsmart lists vpn-list VPN_40 vpn 40 from-vsmart lists
data-prefix-list ENTERPRISE_IPs ip-prefix 10.0.0.0/8 ip-prefix 172.16.0.0/12    ip-prefix
192.168.0.0/16
```

8. Überprüfen Sie die FIB-Programmierung (Forwarding Information Base), die mögliche Routen für das Ziel im Internet anzeigt:

```
vedge1# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.40.4 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 1
Next Hop: Remote
Remote IP:173.37.145.84, Interface ge0/0 Index: 4
```

9. Erreichbarkeit zum Ziel im Internet bestätigen:

```
vedge1# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.192 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.246 ms
64 bytes from 173.37.145.84: icmp_seq=3 ttl=63 time=0.236 ms ^C --- 173.37.145.84 ping
statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt
min/avg/max/mdev = 0.245/0.221/0.192/0.021 ms
```

vEdge2-Verifizierungsschritte:

1. Bestätigen Sie, dass die Standardroute erfolgreich empfangen und in RIB installiert wurde:

```
vEdge2# sh ip route vpn 40 | include 0.0.0.0
40     0.0.0.0/0           omp              -         -           -                -
192.168.30.4   biz-internet     ipsec  F,S
40 0.0.0.0/0 omp - - - - 192.168.30.4 public-internet ipsec F,S
```

2. Überprüfen Sie die FIB-Programmierung (Forwarding Information Base), die mögliche Routen für das Ziel im Internet anzeigt:

```
vedge2# show policy service-path vpn 40 interface ge0/2 source-ip 192.168.50.5 dest-ip
173.37.145.84 protocol 1 all
Number of possible next hops: 4
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.110.6 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.110.6 12346 Color: public-internet
Next Hop: IPsec
  Source: 192.168.110.5 12366 Destination: 192.168.109.4 12346 Color: biz-internet
Next Hop: IPsec
  Source: 192.168.109.5 12366 Destination: 192.168.109.4 12346 Color: public-internet
```

3. Erreichbarkeit zum Ziel im Internet bestätigen:

```
vedge2# ping vpn 40 173.37.145.84
Ping in VPN 40
PING 173.37.145.84 (173.37.145.84) 56(84) bytes of data.
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.382 ms
64 bytes from 173.37.145.84: icmp_seq=1 ttl=63 time=0.392 ms 64 bytes from 173.37.145.84:
icmp_seq=3 ttl=63 time=0.346 ms ^C --- 173.37.145.84 ping statistics --- 3 packets transmitted,
3 received, 0% packet loss, time 2000ms rtt min/avg/max/mdev = 0.392/0.361/0.346/0.023 ms
```

4. Bestätigen Sie, dass DIA funktioniert und die Sitzung Internet Control Message Protocol (ICMP) vom vEdge2 zum 173.37.145.84 in NAT-Übersetzungen angezeigt wird.

```
vedge1# show ip nat filter | tab

                          PRIVATE                       PRIVATE  PRIVATE
PUBLIC  PUBLIC
NAT  NAT                  SOURCE         PRIVATE DEST   SOURCE   DEST     PUBLIC SOURCE
PUBLIC DEST    SOURCE  DEST    FILTER       IDLE        OUTBOUND  OUTBOUND   INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS        ADDRESS       PORT     PORT     ADDRESS
ADDRESS        PORT    PORT    STATE        TIMEOUT     PACKETS   OCTETS     PACKETS  OCTETS
DIRECTION
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
------
0 ge0/0 40 icmp 192.168.50.5 173.37.145.84 9175 9175 192.168.109.4 173.37.145.84 9175 9175
established 0:00:00:04 18 1440 18 1580 -
```

Hinweis: Diese Lösung ermöglicht die Organisation von Redundanz oder Lastverteilung mit unterschiedlichen regionalen Ausgängen.

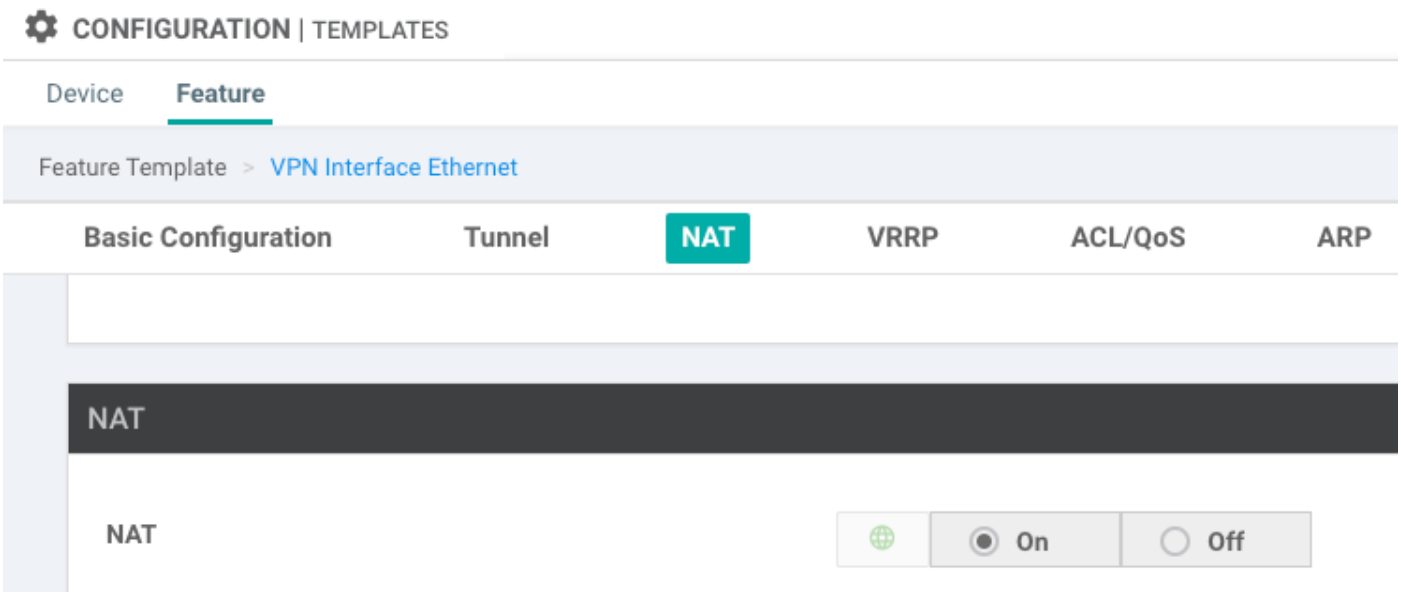
Funktioniert nicht mit IOS-XE-Routern

Lösung 4: Injizieren Sie die Standardroute zum OMP, wenn die lokale DIA verwendet wird.

Diese Lösung kann für IOS-XE- und Viptela OS-basierte SD-WAN-Router verwendet werden.

Kurz gesagt, in dieser Lösung wird eine Standardroute für DIA (0.0.0.0/0 Null0) in zwei Subnetzwerke 0.0.0.0/1 und 128.0.0.0/1 aufgeteilt, die auf Null0 zeigen. Mit diesem Schritt wird vermieden, dass sich eine Standardroute überschneidet, die Zweigstellen und Standardrouten für lokale DIAs mitgeteilt werden sollte. In IOS-XE haben für DIA verwendete Routen eine administrative Distanz (AD) gleich 6, während AD mit dem statischen Standardwert 1 ist. Der Vorteil der Lösung besteht in der Möglichkeit, ein Redundanzschema zu verwenden, wenn regionale DIA an zwei verschiedenen Standorten konfiguriert wird.

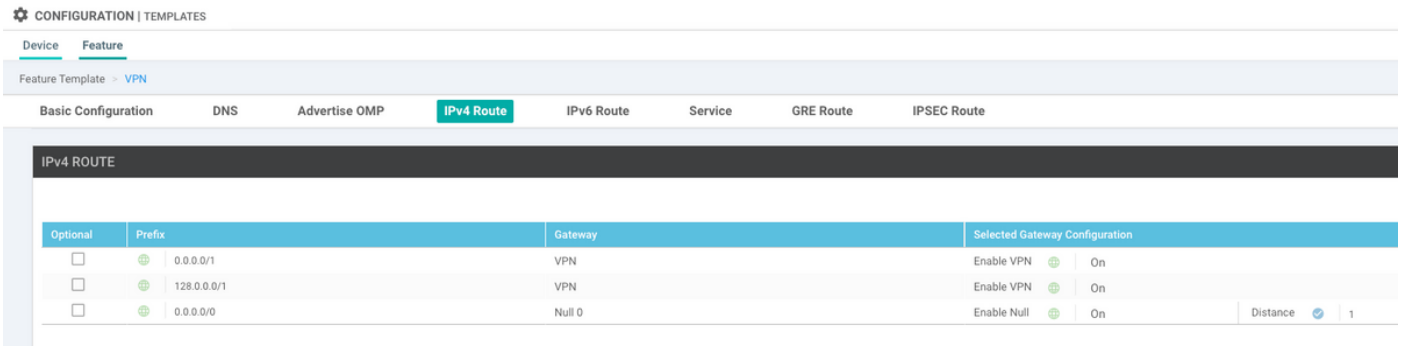
1. Aktivieren von NAT auf einer Transportschnittstelle



2. Fügen Sie in einer Funktionsvorlage für ein Service-VPN, in dem die DIA verwendet werden soll, die folgenden statischen IPv4-Routen hinzu:

- 0.0.0.0/1 und 128.0.0.0/1 auf VPN verweisen. Diese Routen werden für DIA verwendet

- 0.0.0.0/0 zeigen auf Null 0. Diese Route wird für die Werbung über OMP in Zweigstellen verwendet (ähnlich wie in Lösung 3).



3. Überprüfen Sie, ob Routen erfolgreich zu RIB hinzugefügt wurden:

```
cedge1#show ip route vrf 40

Routing Table: 40
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP,  D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary,
L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P -
periodic downloaded static route, H - NHRP, l - LISP
       a - application route, + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Null0                    <<<<==== Static route to null0
that will be advertised to branches via OMP n Nd 0.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA
route n Nd 128.0.0.0/1 [6/0], 00:08:23, Null0 <<<<==== DIA route 192.40.1.0/32 is subnetted, 1
subnets m 192.40.1.1 [251/0] via 192.168.30.207, 3d01h 192.40.2.0/32 is subnetted, 1 subnets m
192.40.2.1 [251/0] via 192.168.30.208, 3d01h
```

4. Stellen Sie sicher, dass die DIA lokal gut funktioniert:

```
cedge1#ping vrf 40 173.37.145.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

5. Überprüfen Sie, ob die Standardroute erfolgreich an eine Außenstelle weitergeleitet und in RIB installiert wurde.

```
cedge3#show ip route vrf 40

Routing Table: 40
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP
external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA, i - IS-IS, su - IS-IS summary,
L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route, o - ODR, P -
```

```
periodic downloaded static route, H - NHRP, l - LISP
       a - application route, + - replicated route, % - next hop override, p - overrides from
PfR

Gateway of last resort is 192.168.30.204 to network 0.0.0.0

m*    0.0.0.0/0 [251/0] via 192.168.30.204, 00:02:45    <<<<==== Default route that advertised
via OMP 192.40.1.0/32 is subnetted, 1 subnets m 192.40.11.1 [251/0] via 192.168.30.204, 00:02:45
192.40.13.0/32 is subnetted, 1 subnets C 192.40.13.1 is directly connected, Loopback40
```

6. Stellen Sie sicher, dass die DIA lokal gut funktioniert:

```
cedge3#ping vrf 40 173.37.145.84
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.84, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

7. Prüfen Sie, ob der regionale DIA-Router die NAT-Übersetzung erfolgreich war.

```
cedge1#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 192.168.109.204:1     192.40.13.1:1         173.37.145.84:1       173.37.145.84:1
Total number of translations: 1
```

Hinweis: Diese Lösung ermöglicht die Organisation von Redundanz oder Lastverteilung mit unterschiedlichen regionalen Ausgängen.

Hinweis: CSCvr72329 - Erweiterungsanforderung "NAT route redistribution to OMP"

Zugehörige Informationen

- Zentrale Datenrichtlinie
- Konfigurieren einer zentralen Datenrichtlinie
- Konfigurationsbeispiele für zentrale Datenrichtlinien
- OMP Routing Protocol
- Konfigurieren von OMP