Comment sélectionner un site particulier pour être une session Internet séparée régionale préférée ?

Contenu

Introduction

Ce document décrit comment configurer le fabric SD-WAN afin de configurer un vEdge de filiale en tant que découpage Internet régional préféré à l'aide de l'accès direct à Internet (DIA) et de la politique de données centralisée. Cette solution pourrait être utile, par exemple, lorsqu'un site régional utilise un service centralisé tel que Zscaler® et devrait être utilisé comme point de sortie Internet préféré. Ce déploiement nécessite la configuration de tunnels GRE (Generic Routing Encapsulation) ou IPSec (Internet Protocol Security) à partir d'un VPN de transport et le flux de données est différent de la solution DIA classique, où le trafic atteint directement Internet.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez une connaissance de ce sujet :

- Compréhension de base du cadre stratégique SD-WAN.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

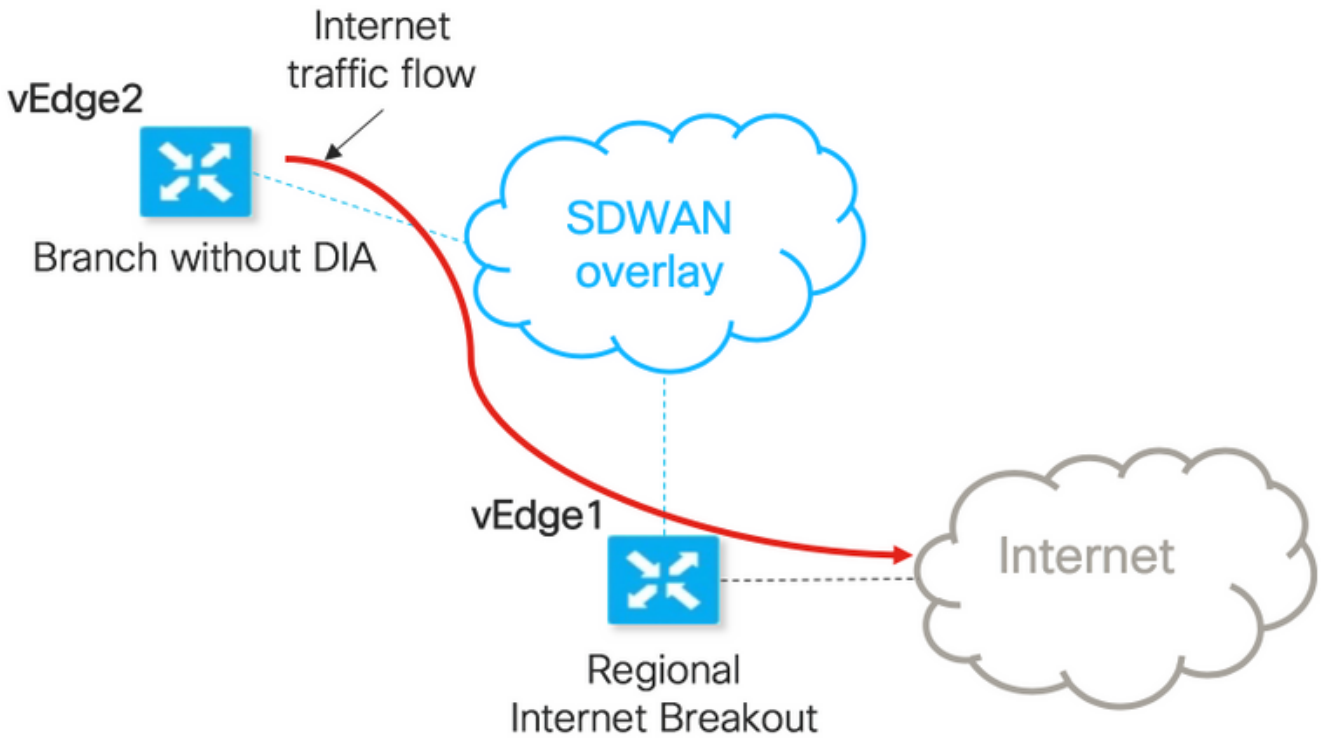
- Routeurs vEdge

- vSmart Controller avec la version 18.3.5 du logiciel.

Informations générales

Le trafic VPN de service de vEdge2, qui doit atteindre Internet, est transféré vers une autre succursale vEdge1, à l'aide de tunnels de plan de données. vEdge1 est le routeur sur lequel DIA est configuré pour le découpage Internet local.

Diagramme du réseau



Nom de l´hôte	vEdge1	vEdge2
Rôle hôte	Périphérique de filiale doté de la DIA (division Internet régionale)	Périphérique de filiale sans DIA configuré
VPN 0		
Emplacements de transport (TLOC) 1	biz-internet, ip : 192.168.110.6/24	biz-internet, ip : 192.168.110.5/2
Emplacements de transport (TLOC) 2	public-internet, ip : 192.168.109.4/24	public-internet, ip : 192.168.109.
VPN de service 40	Interface ge0/1, ip : 192.168.40.4/24	Interface ge0/2, ip : 192.168.50.5

Configurations

Solution 1 : Utilisation centralisée des politiques de données pour modifier le saut suivant.

vEdge2 dispose d'un tunnel de plan de données établi avec vEdge1 et d'autres sites (connectivité de type maillage global)

vEdge1 a DIA configuré avec **ip route 0.0.0.0/0 vpn 0**.

Configuration de la politique de données centralisée vSmart :

```
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 - ne nécessite aucune configuration spéciale.

Vous trouverez ici les étapes permettant d'effectuer une vérification si une stratégie a été appliquée correctement.

1. Vérifiez que la stratégie est absente de vEdge2 :

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

2. Vérifiez la programmation FIB (Forwarding Information Base). Il doit afficher l'absence de route (Blackhole) pour la destination sur Internet :

```
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. Appliquez la stratégie de données vSmart dans la section **appliquer la stratégie** de configuration vSmart ou activez-la dans l'interface utilisateur graphique vManage.

4. Vérifiez que vEdge2 a bien reçu la stratégie de données de vSmart :

```
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. Vérifiez la programmation de la Base d'informations de transfert (FIB), qui affiche les routes possibles pour la destination sur Internet :

```
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. Confirmer l'accessibilité à la destination sur Internet :

```
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
```

Vous trouverez ici les étapes de configuration de vEdge1.

1. Activez la traduction d'adresses de réseau (NAT) sur l'interface de transport, où DIA doit être utilisé :

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

2. Ajoutez la route statique **ip route 0.0.0.0/0 vpn 0** dans un VPN de service pour activer DIA :

```
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. Vérifiez si RIB contient la route NAT :

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

4. Confirmez que DIA fonctionne et que nous pouvons voir la session ICMP (Internet Control Message Protocol) vers 173.37.145.84 depuis vEdge2 dans les traductions NAT

```
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 -
```

Note: Cette solution ne nous permet pas d'organiser la redondance ou le partage de charge avec différentes utilisations de sorties régionales.

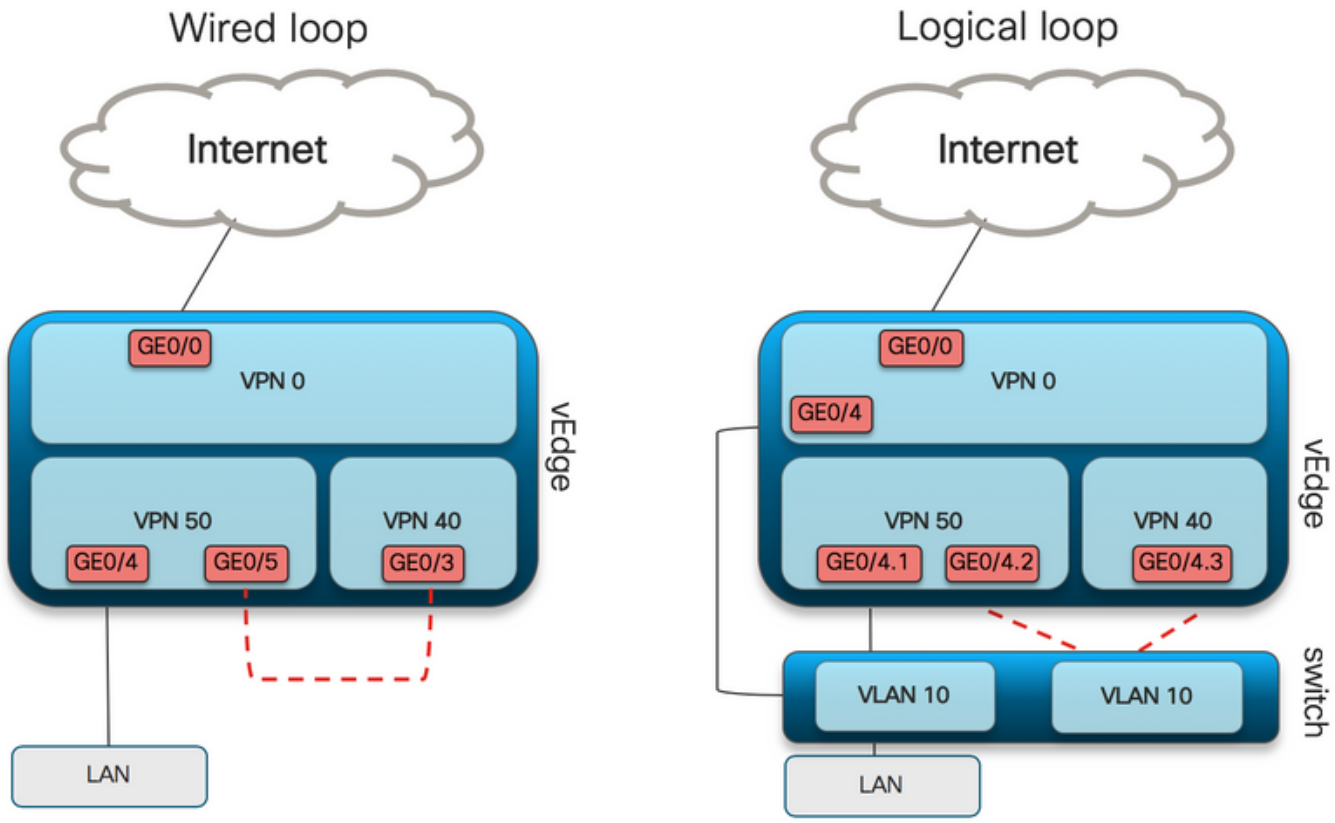
Ne fonctionne pas avec les routeurs IOS-XE

Solution 2 : Injection requise GRE\IPSec\NAT Default Route to OMP.

Àce jour, il n'est pas possible d'obtenir que la route par défaut, pointant vers le tunnel GRE\IPSec sur vEdge1, soit annoncée via OMP vers vEdge2 (redistribuez le protocole Nat route OMP). Veuillez noter que le comportement peut changer dans les versions futures du logiciel.

Notre objectif est de créer une route statique par défaut régulière (**route IP 0.0.0.0/0 <adresse IP de tronçon suivant>**) qui pourrait être créée par vEdge2 (périphérique préféré pour DIA) et propagée via OMP.

Pour ce faire, un VPN factice est créé sur vEdge1 et une boucle de port physique est exécutée avec un câble. La boucle est créée entre les ports affectés au VPN factice et les ports du VPN souhaité qui nécessitent une route statique par défaut. Vous pouvez également créer une boucle avec une seule interface physique connectée au commutateur avec un VLAN factice et deux sous-interfaces affectées aux VPN correspondants sur l'image ci-dessous :



Vous trouverez ici un exemple de configuration de vEdge1.

1. Créer un VPN factice :

```
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. Vérifiez que la route DIA, pointant vers l'interface NAT, a été correctement ajoutée à la table de routage :

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

3. VPN de service utilisé à des fins de production, où une route par défaut régulière est configurée (quel OMP pourra annoncer) :

```
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. Vérifiez la présence d'une route par défaut pointant vers l'interface de boucle :

```
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. Vérifiez que vEdge1 a annoncé la route par défaut via OMP :

```
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 ne nécessite aucune configuration, la route par défaut est reçue via OMP, qui pointe vers vEdge1

```
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. Confirmer l'accessibilité à 173.37.145.84 :

```
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
```

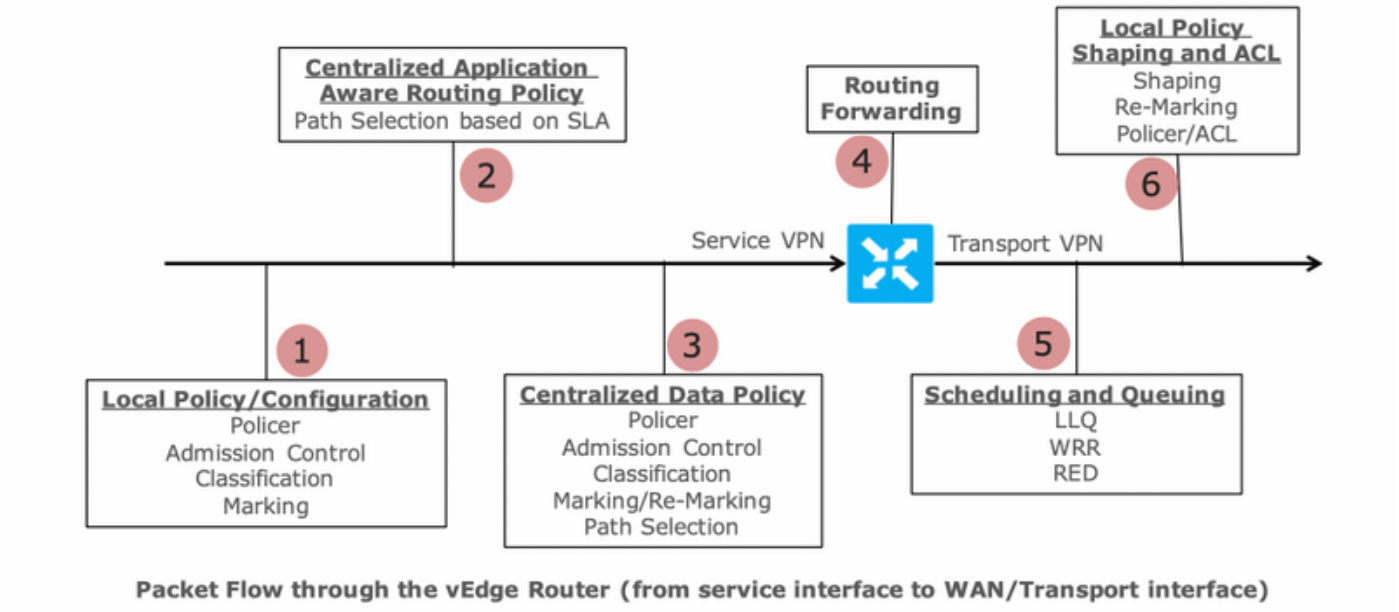
Note: Cette solution vous permet d'organiser la redondance ou le partage de charge avec différentes utilisations de sorties régionales.

Ne fonctionne pas avec les routeurs IOS-XE

Solution 3 : Injecter la route par défaut vers OMP lorsque la stratégie de données centralisée est utilisée pour DIA.

Lorsque la politique de données centralisée est utilisée pour le DIA local, la façon possible d'injecter la route par défaut, elle pointe vers un périphérique régional avec DIA qui est l'utilisation de cette route statique par défaut : **ip route 0.0.0.0/0 Null0**.

En raison du flux de paquets interne, le trafic qui arrive des filiales atteint DIA grâce à la politique de données et n'atteint jamais la route vers Null0. Comme vous pouvez le voir ici, la recherche de tronçon suivant n'a lieu qu'après un déploiement de stratégie.



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

vEdge2 dispose d'un tunnel de plan de données établi avec vEdge1 et d'autres sites (connectivité de type maillage global). Il ne nécessite aucune configuration spéciale.

Le protocole DIA de vEdge1 est configuré avec une politique de données centralisée.

Vous trouverez ici les étapes de configuration de vEdge1.

1. Activez la traduction d'adresses de réseau (NAT) sur l'interface de transport, où DIA doit être utilisé :

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

2. Ajoutez la route statique **ip route 0.0.0.0/0 null0** dans un VPN de service pour annoncer la valeur par défaut aux filiales :

```
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. Vérifiez si RIB contient la route par défaut :

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

4. Vérifiez que vEdge1 a annoncé la route par défaut via OMP :

```
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. Vérifiez que la stratégie est absente sur vEdge1 et que DIA n'est pas activé :

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

6. Vérifiez la programmation FIB (Forwarding Information Base). Il doit afficher l'absence de route (Blackhole) pour la destination sur Internet, car DIA n'est pas activé :

```
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
```

Configuration de stratégie de données centralisée vSmart pour 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
```

Appliquez la stratégie de données vSmart dans la section **appliquer la stratégie** de configuration vSmart ou activez-la dans l'interface utilisateur graphique vManage.

7. Vérifiez que vEdge1 a bien reçu la stratégie de données de vSmart :

```
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. Vérifiez la programmation de la Base d'informations de transfert (FIB), qui affiche les routes

possibles pour la destination sur Internet :

```
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. Confirmer l'accessibilité à la destination sur Internet :

```
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
```

Étapes de vérification vEdge2 :

1. Confirmez que la route par défaut a bien été reçue et installée dans RIB :

```
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. Vérifiez la programmation de la Base d'informations de transfert (FIB), qui affiche les routes possibles pour la destination sur Internet :

```
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. Confirmer l'accessibilité à la destination sur Internet :

```
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. Confirmez que DIA fonctionne et que nous pouvons voir la session ICMP (Internet Control Message Protocol) vers 173.37.145.84 depuis vEdge2 dans les traductions NAT

```
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 -
```

Note: Cette solution permet d'organiser la redondance ou le partage de charge avec différentes utilisations de sorties régionales.

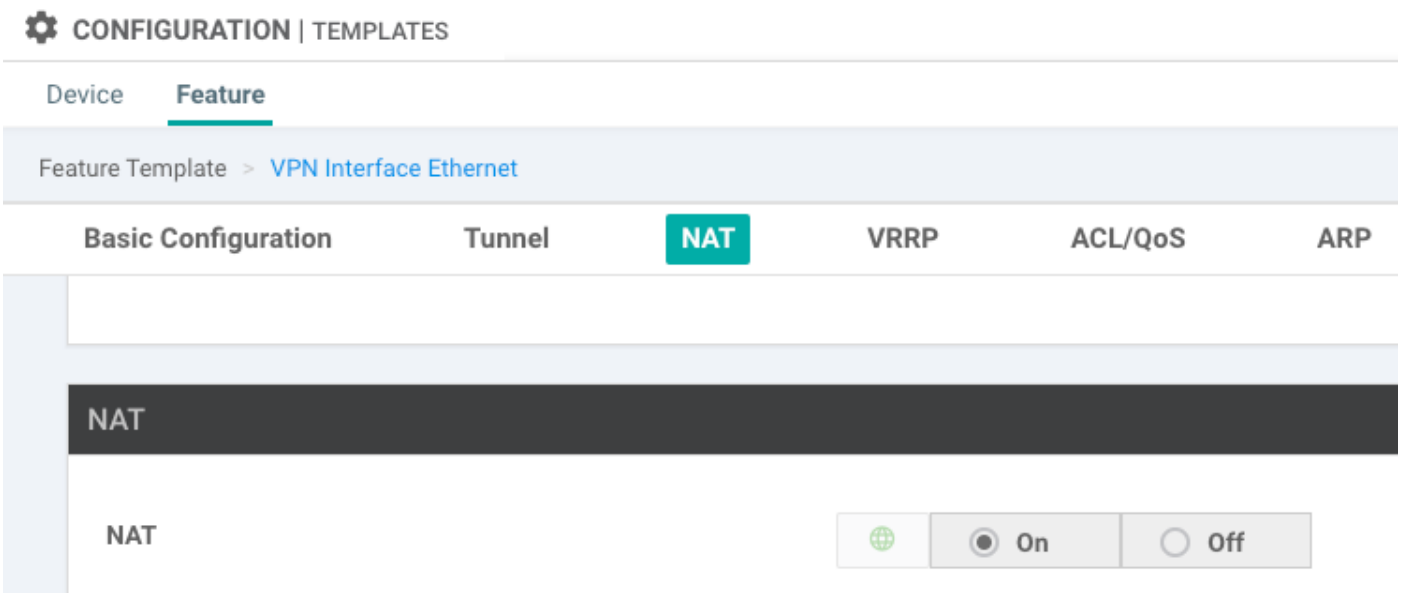
Ne fonctionne pas avec les routeurs IOS-XE

Solution 4 : Injecter le routage par défaut vers OMP lorsque le DIA local est utilisé.

Cette solution peut être utilisée pour les routeurs SD-WAN IOS-XE et Viptela OS.

En bref, dans cette solution, une route par défaut pour DIA (0.0.0.0/0 Null0) est divisée en deux sous-réseaux 0.0.0.0/1 et 128.0.0.0/1 pointant vers Null0. Cette étape est effectuée pour éviter le chevauchement d'une route par défaut qui doit être annoncée aux filiales et d'une route par défaut, utilisée pour le DIA local. Dans les routes IOS-XE utilisées pour DIA, la distance administrative (AD) est égale à 6, tandis que la distance administrative par défaut statique est 1. L'avantage de la solution est la possibilité d'utiliser un schéma de redondance lorsque le DIA régional est configuré dans deux emplacements différents.

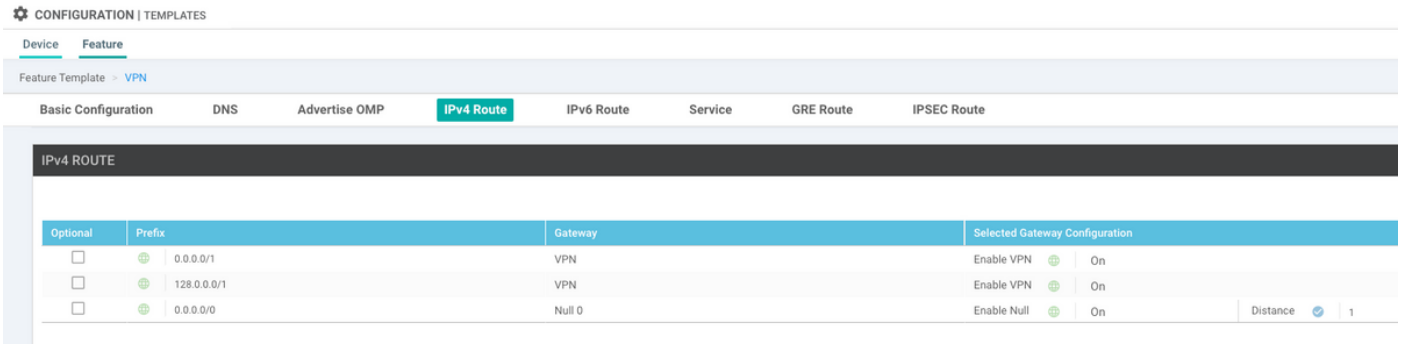
1. Activer la NAT sur une interface de transport



2. Dans un modèle de fonction pour un VPN de service, où DIA doit être utilisé, ajoutez les routes IPv4 statiques suivantes :

- 0.0.0.0/1 et 128.0.0.0/1 pointant vers VPN. Ces routes sont utilisées pour DIA

- 0.0.0.0/0 pointant vers Null 0. Cette route est utilisée pour la publicité via OMP vers les filiales (comme dans la solution 3)



3. Vérifiez que les routes ont été correctement ajoutées à RIB :

```
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. Vérifiez que DIA fonctionne bien localement :

```
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. Vérifiez que la route par défaut a été correctement annoncée à une succursale et installée dans RIB

```
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. Vérifiez que DIA fonctionne bien localement :

```
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. Vérifiez la traduction NAT réussie du routeur DIA régional.

```
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
```

Note: Cette solution permet d'organiser la redondance ou le partage de charge avec différentes utilisations de sorties régionales.

Note: CSCvr72329 - requête d'amélioration « redistribution de route NAT vers OMP »

Informations connexes

- Politique de données centralisée
- Configuration de la politique de données centralisée
- Exemples de configuration de la stratégie de données centralisée
- Protocole de routage OMP
- Configuration du protocole OMP