Direct Internet Access (DIA) providing internet access to guest users – Méthode Vsmart policy

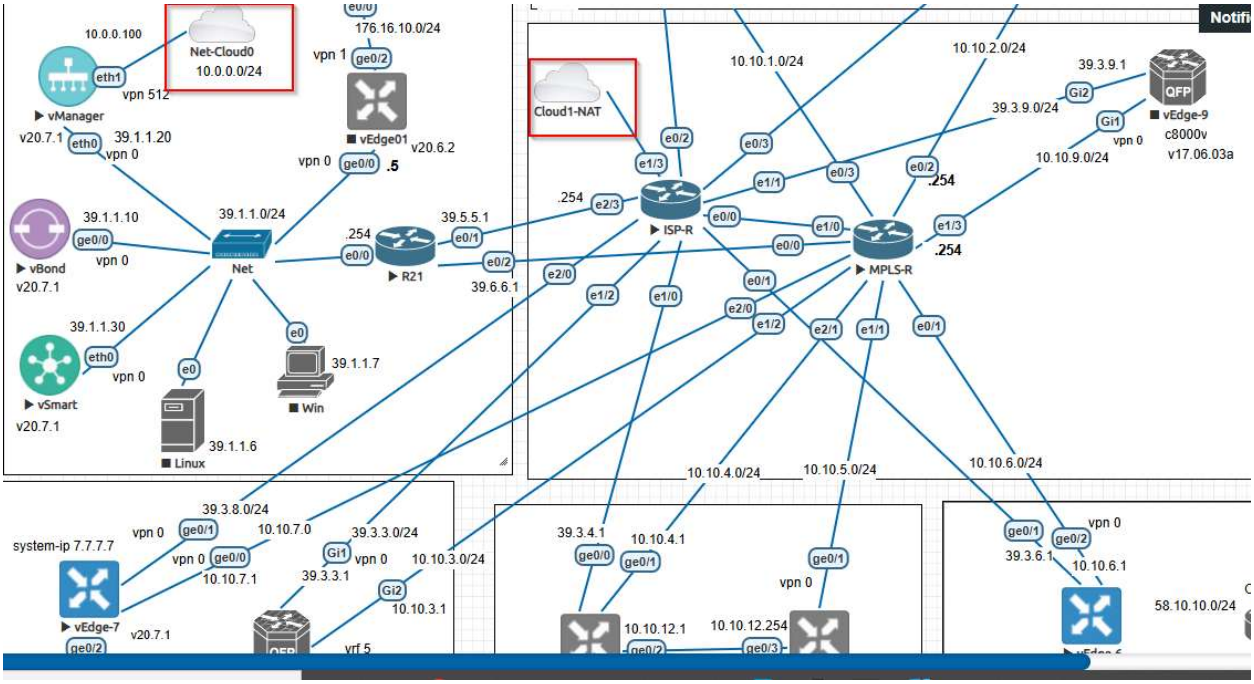
Simulation of SD-WAN on Eve-NG platform

Environnement : labo SD-WAN sur plateforme Eve-NG

vManage v20.7.1 (24 Go) , vSmart v20.7.1 (2 G0) , vBond v20.7.1 (1Go), vEdges v20.7.1 (1 Go), Cedges v17.06 (2 Go)

Ici le labo est réalisé sur un Cedge Cisco c8000v, de version : v17.06.03.a. Le Cedge est intitulé dans ce labo : Vedge-8

La méthode, ici utilisée, est l'utilisation de police (Data-policy), définies sur Vsmart qui seront ensuite poussées par Vsmart vers le Vedge 8.



Ce schéma représente seulement une partie haute du plan et est indiquée pour des raisons de visibilité.

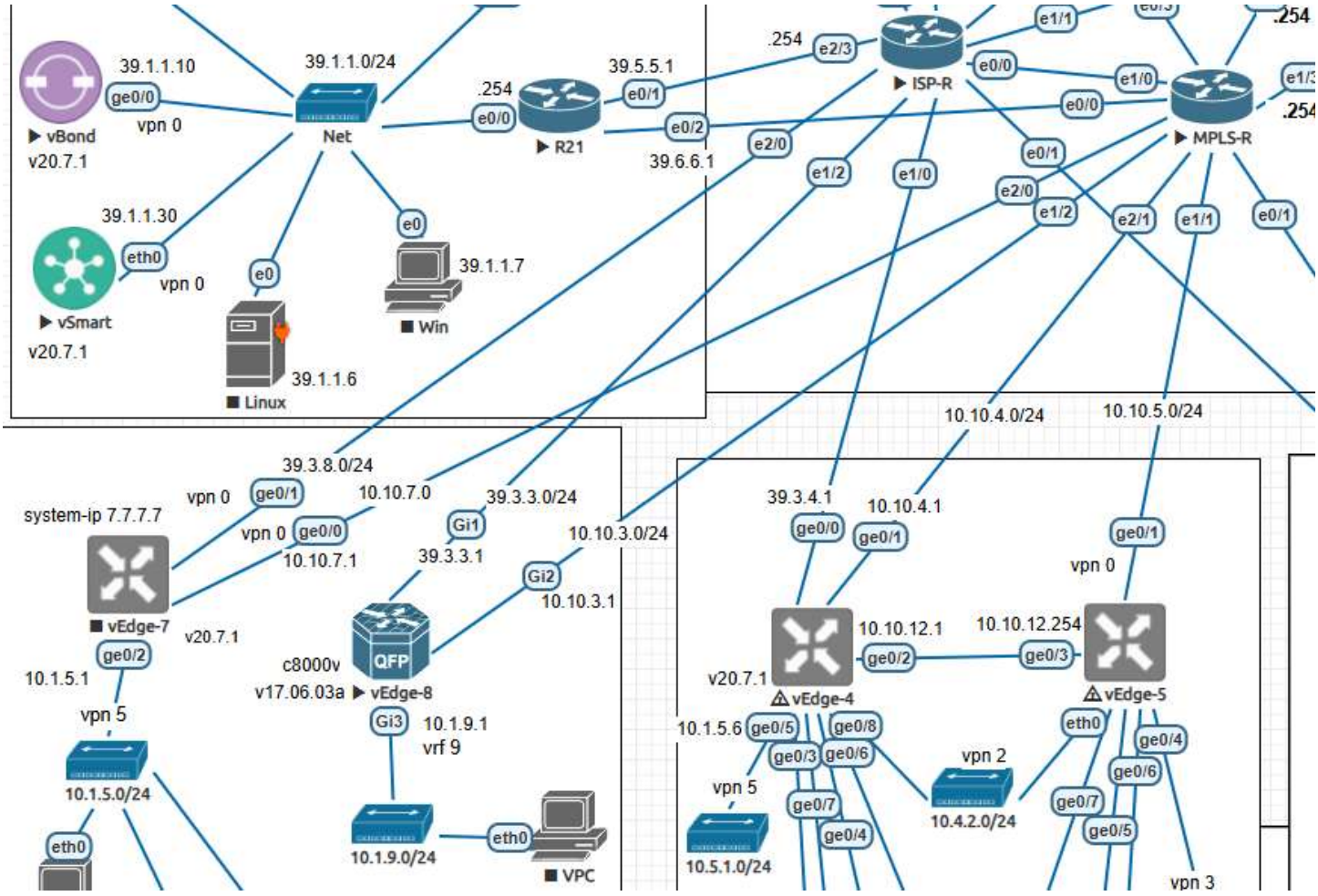
Le routeur ISP-R permet l'accès à internet via l'interface e1/3 :

```
ISP-R#      sh run inte e1/3
Building configuration...

Current configuration : 77 bytes
!
interface Ethernet1/3
 no switchport
 ip address dhcp
 ip nat outside
end

ISP-R#
```

Topologie :

Le plan montre une partie du plan global. La partie basse de la topologie ci-dessous, montre, notamment, le routeur Cisco c8000v, ainsi que d'autres routeurs Vedges. Pour des raisons de simplification, pour ce lab, seul le c8000v a été activé, ainsi que les autres routeurs IPS-R et MPLS pour la partie du haut. Et également sont activés, les équipements Vmanage, Vbond, Vsmart.

Les deux routeurs ISP-R et MPLS-R peuvent être représentés ou symbolisés par des nuages internet ou MPLS, et synthétisent les raccordement au WAN. En réalité, sur un réseau véritable. Il s'agirait d'un ensemble de routeurs et de divers équipements réseaux, représentant le cloud.



Au niveau de Vedge-8 :

```
vEdge-8#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       39.3.3.1        YES other  up                    up
GigabitEthernet2       10.10.3.1       YES other  up                    up
GigabitEthernet3       10.1.9.1        YES other  up                    up
GigabitEthernet4       unassigned      YES unset  up                    up
Sdwan-system-intf      3.3.3.3         YES unset  up                    up
Loopback65528          192.168.1.1     YES other  up                    up
Tunnel1                39.3.3.1        YES TFTP   up                    up
Tunnel2                10.10.3.1       YES TFTP   up                    up
vEdge-8#
```

Définition du vrf :

Le ou les VRF utilisateurs doivent avoir préalablement été configurés au niveau global

```
!
vrf definition 9
 rd 1:9
 !
 address-family ipv4
  route-target export 1:9
  route-target import 1:9
 exit-address-family
!
```

show vrf.

Cette commande permet de voir les vrf configurés sur le vedge-8. Seul le vrf 9 est configuré , dans lequel l'interface gi/3 est situé.

```
vEdge-8#
vEdge-8#sh vrf
  Name                            Default RD            Protocols   Interfaces
  65528                           <not set>             ipv4        Lo65528
  9                               1:9                   ipv4        Gi3
vEdge-8#
```

Configuration DIA NAT :

1 Étape 1 :

sur l'interface gi/1 , qui est connectée à un provider ISP (internet) via le routeur ISP-R, taper la commande : ip nat outside

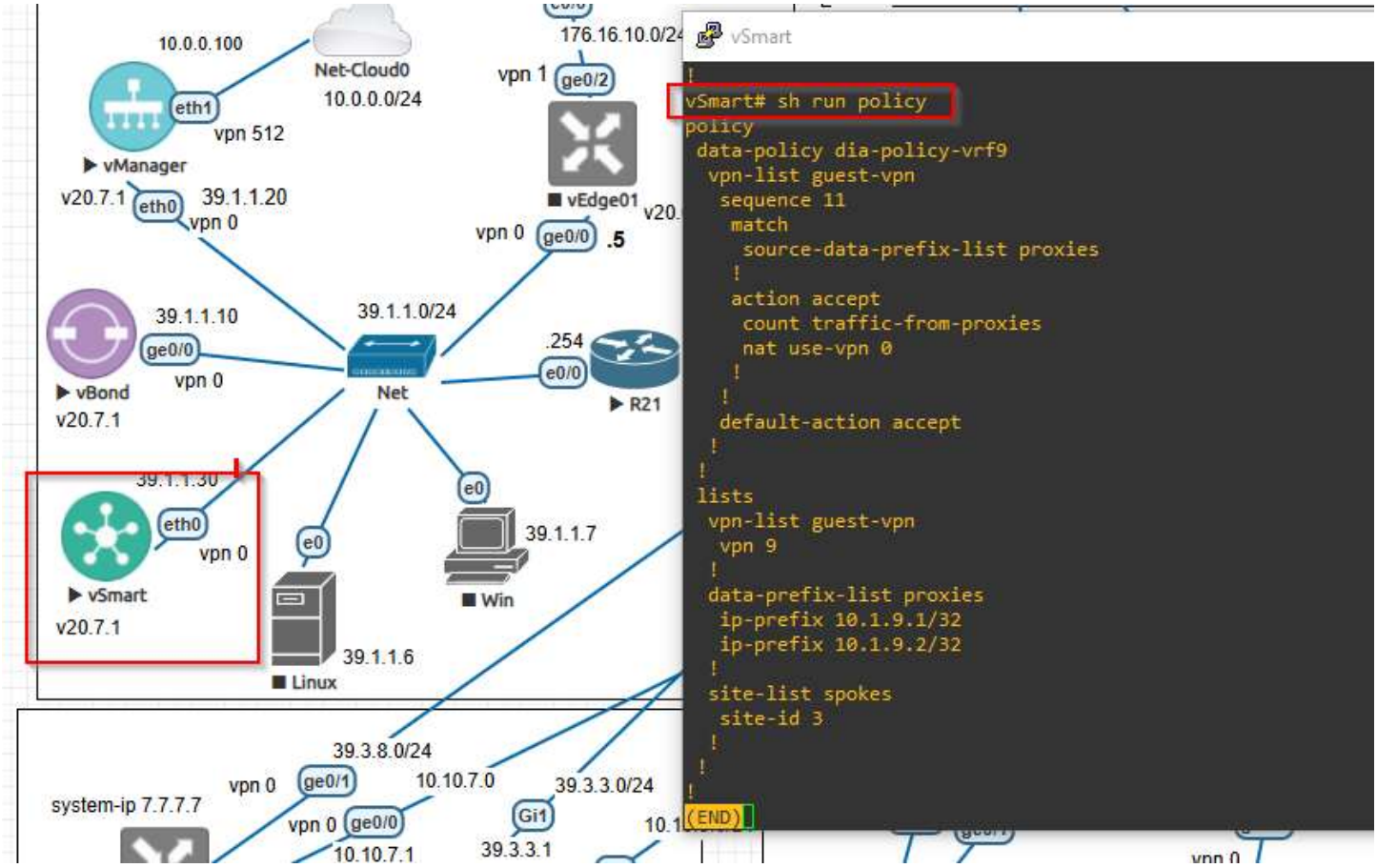
```
interface GigabitEthernet1
 ip address 39.3.3.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
!
```

Configuration sur vsmart :

2 Étape 2 :

on définit la police suivante sur vsmart :

vSmart# sh run policy
policy
data-policy dia-policy-vrf9
vpn-list guest-vpn
sequence 11
match
source-data-prefix-list proxies
action accept
count traffic-from-proxies
nat use-vpn 0
default-action accept
lists
vpn-list guest-vpn
vpn 9
data-prefix-list proxies
ip-prefix 10.1.9.1/32
ip-prefix 10.1.9.2/32
site-list spokes
site-id 3



Configuration sur vsmart :

3 Étape 3 :

on applique (active) ensuite la police

LA police est pousse ensuite sur l'équipement vedge-8 (qui est sur le site 3, site-di : 3) et pour le vrf 9 , ce uniquement pour les adresses ip : 10.1.9.1 et 10.1.9.2

sur vsmart : show run apply-policy

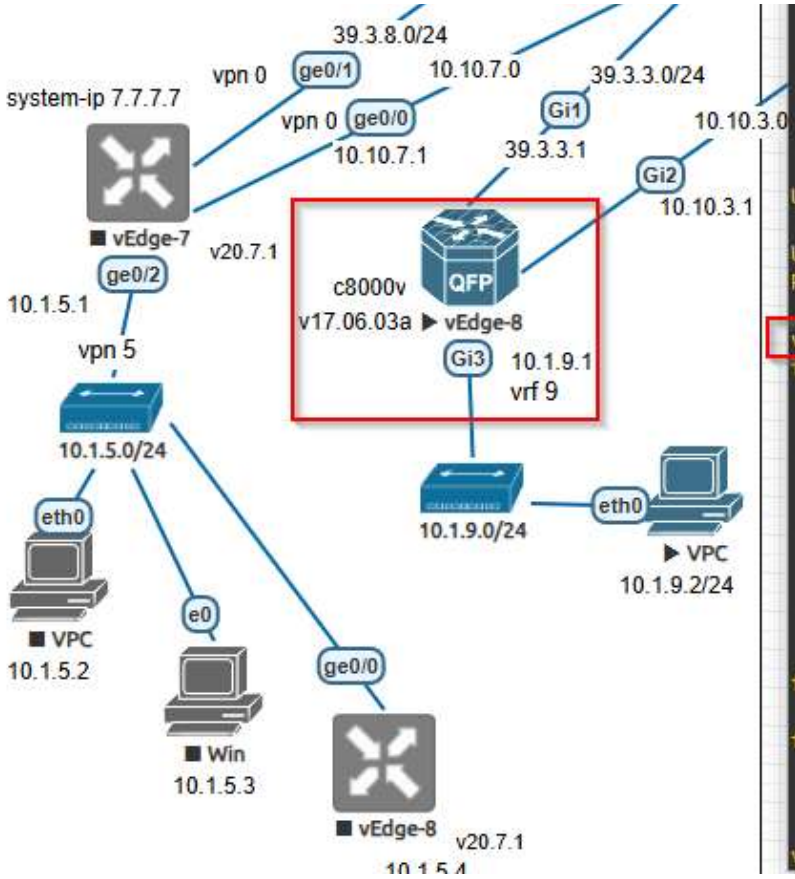
```
vSmart#
vSmart# sh run apply-policy
apply-policy
 site-list spokes
  data-policy dia-policy-vrf9 from-service
 !
!
vSmart#
```

Vérification sur vedge-8 :

4 Étape 4

Maintenant, on vérifie que la police a bien été poussée sur vedge-8 :

sur vedge-8 : show sdwan policy from-vsmart

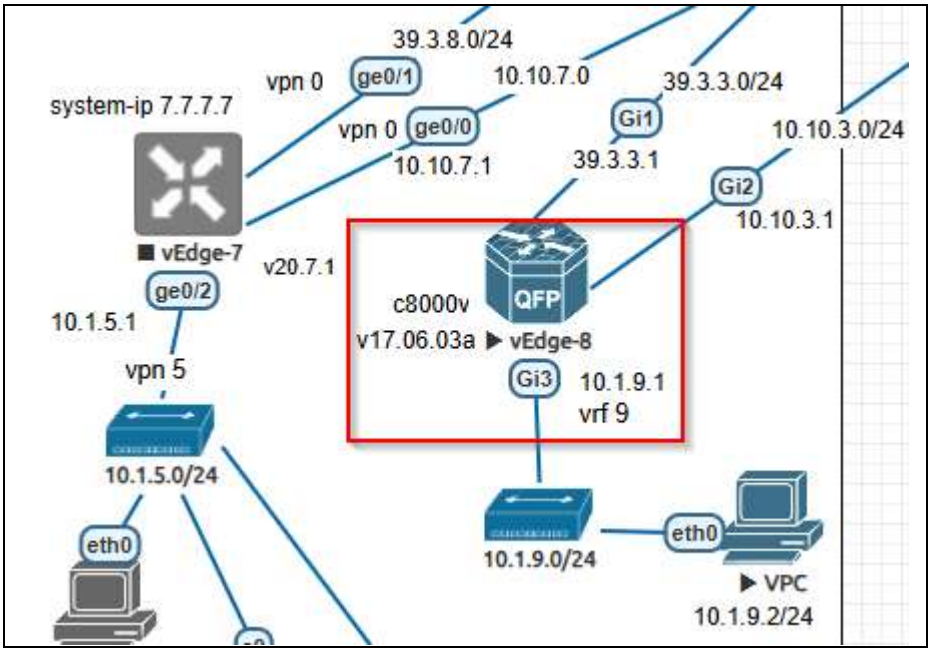



```
User Access Verification

Username: admin
Password:

vEdge-8#sh sdwan policy from-vsmart
from-vsmart data-policy dia-policy-vrf9
 direction from-service
 vpn-list guest-vpn
  sequence 11
   match
    source-data-prefix-list proxies
   action accept
    count traffic-from-proxies
    nat use-vpn 0
    no nat fallback
  default-action accept
from-vsmart lists vpn-list guest-vpn
 vpn 9
from-vsmart lists data-prefix-list proxies
 ip-prefix 10.1.9.1/32
 ip-prefix 10.1.9.2/32

vEdge-8#
```

Vérifications et tests :

Test 1 :

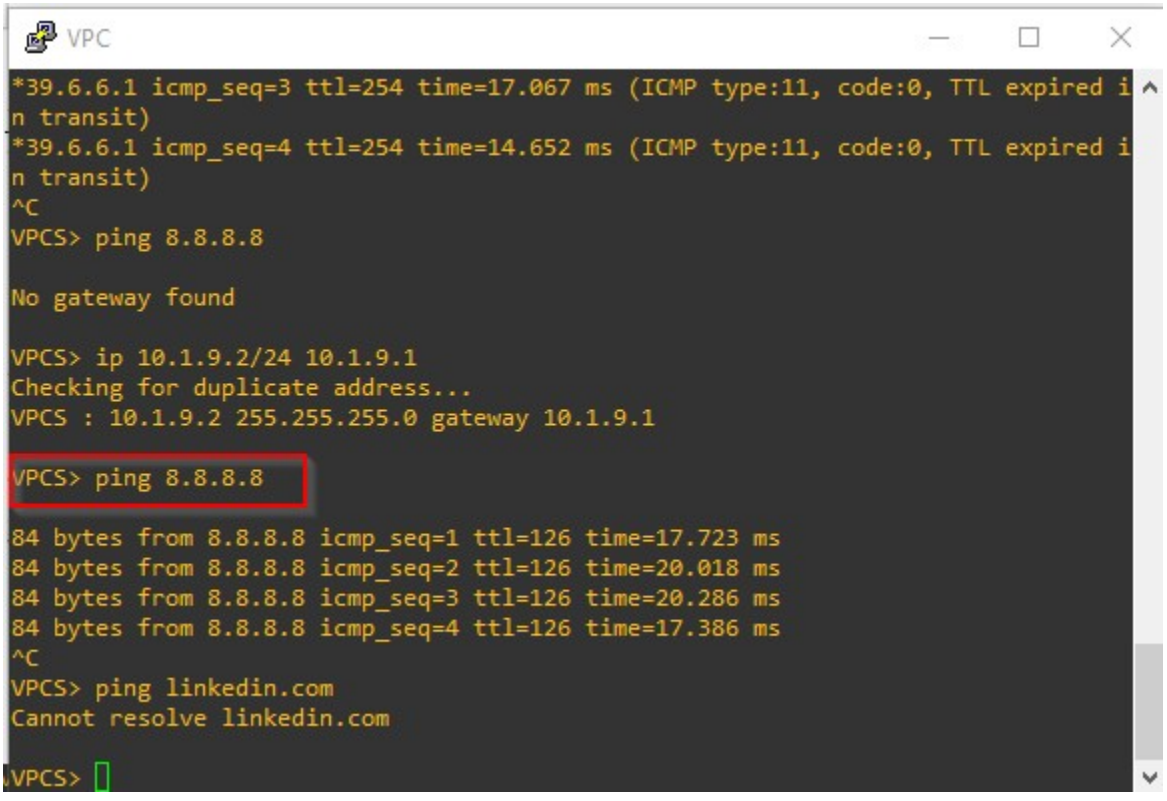
Tous les paquets provenant du vrf 9 passent à travers l'interface gi3 et sont redirigés vers l'interface gi1 naté (gi1 NAT-enabled). Ce suivant les configurations indiquées plus haut dans cet article.



Ping a partir d'instances à l'intérieur du vrf 9

Seules les instances (devices) du vrf 9 , qui sont incluses dans la liste autorisée (via la prefix-list 10.1.91 et 10.1.9.2) sont autorisés à communiquer vers internet

Ici en pratique, seul l'ordinateur VPC interne au vrf 9, d'adresse ip 10.1.9.2 peut communiquer avec internet



Test 2 :

Par contre ,a partir du vedge-8 , on ne peut pas communiquer sur internet .

Ce qui est normal, Car DIA est configuré seulement pour les adresses ip des équipements internes au vrf 9 (pour certaines adresses IP).

On aurait pu aussi permettre à toute la plage ip, interne au vrf 9 , la communication vers internet. Mais pour des raisons pratiques, nous nous sommes limité à quelques adresses IP.

```
vEdge-8#ping vrf 9 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
vEdge-8#
vEdge-8#
```

Test 3 :

sur vedge-8 : Vérification des compteurs.

On voit que les ping effectués a partir de l'ordinateur VPC ont généré du trafic, filtré par la police en place sur vedge-8, pour le site 3 . vrf 9 :

Le nom du compteur, qui a été précédemment défini dans la police, est : traffic-from-proxies

```
vEdge-8#
vEdge-8#sh sdwan policy data-policy-filter
data-policy-filter dia-policy-vrf9
 data-policy-vpnlist guest-vpn
  data-policy-counter default_action_count
   packets 0
   bytes   0
  data-policy-counter traffic-from-proxies
   packets 38
   bytes   3764

vEdge-8#
```

Test 4 :

LA commande suivante permet de voir que le trafic à destination d'internet venant de l'adresse ip : 10.1.9.2 passe par l'interface gi3 de vedge-8 , puis est redirigé vers l'interface Gi1 de vegde-8 puis vers le next hop : qui est 39.3.3.254 . l'adresse ip du next-hop correspond à l'adresse du provider (ISP) internet

```
vEdge-8#
vEdge-8#$vpn 9 interface gi3 source-ip 10.1.9.2 dest-ip 8.8.8.8 protocol 1
Next Hop: Remote
  Remote IP: 39.3.3.254, Interface GigabitEthernet1 Index: 7


vEdge-8#$vpn 9 interface gi3 source-ip 10.1.9.1 dest-ip 8.8.8.8 protocol 1
Next Hop: Remote
  Remote IP: 39.3.3.254, Interface GigabitEthernet1 Index: 7


vEdge-8#
```

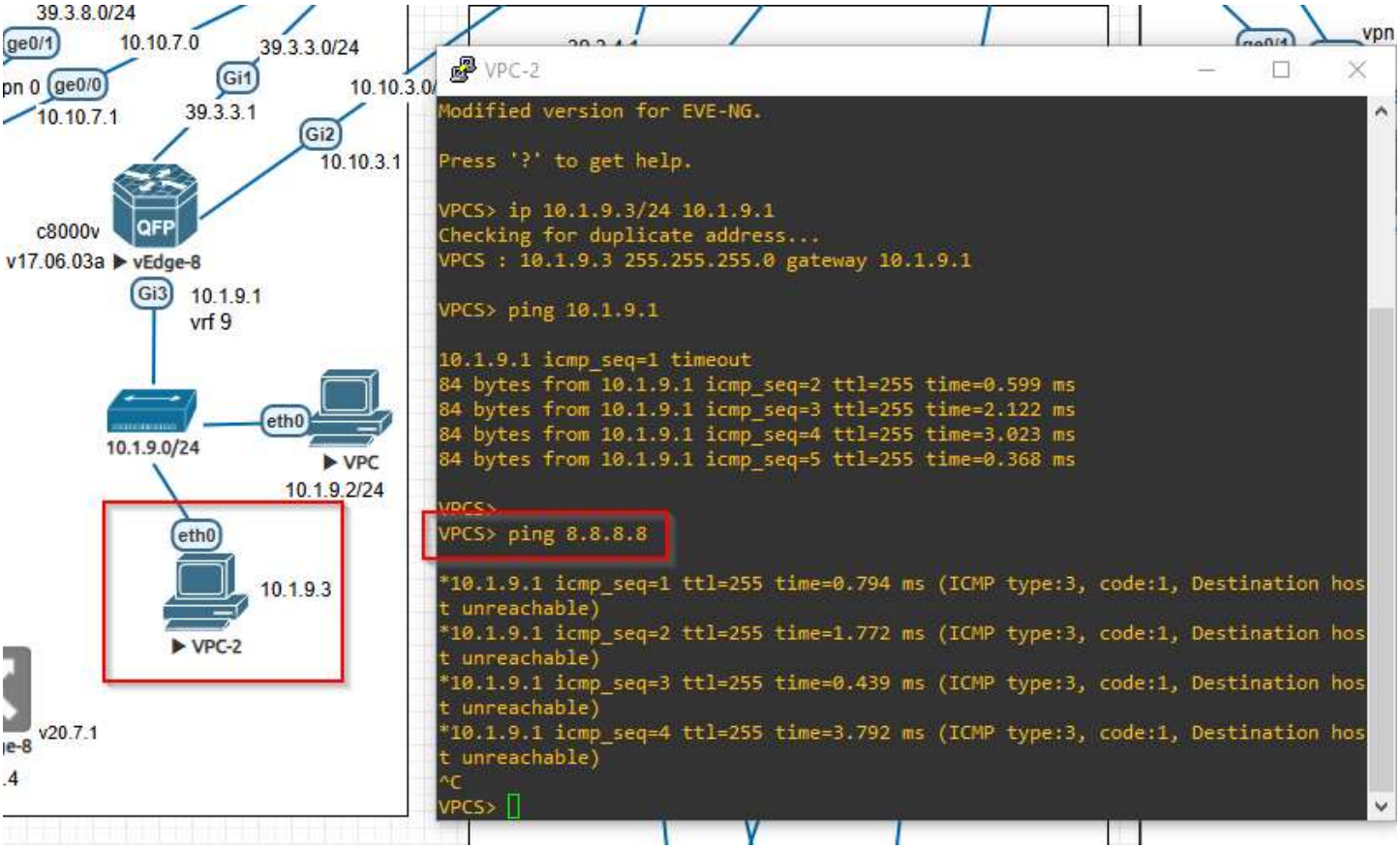
Test 5 :
Cas de Devices qui sont dans le vrf 9 , mais non configurés pour DIA

On ajoute un ordinateur (intitulé : VPC-2) dans le vrf 9, tel qu'indiqué dans le schéma, plus bas.
Dans cet exemple, on voit un autre ordinateur dans le vrf 9 , VPC-2 qui n'est pas configuré pour DIA
son adresse ip fait partie du subnet du vrf 9 : 10.1.9.3 , mais son adresse ip n'a pas été ajouté dans la liste des préfixes de la police.
Dans ce cas, il ne pourra pas communiquer sur internet. C'est le cas dit du 'black- hole

LA commande suivante montre le chemin du trafic de 10.1.9.3 vers 8.8.8.8 via l'interface gi3 , pour le vrf 9 . et on voit que le next hop est indiqué comme 'blackhole'.
Autrement dit , le trafic ne passe pas vers internet.

```
vEdge-8#
vEdge-8#$vpn 9 interface gi3 source-ip 10.1.9.3 dest-ip 8.8.8.8 protocol 1
Next Hop: Blackhole


vEdge-8#
```

On constate, aussi sur le VPC-2, qu'un ping vers 8.8.8.8 n'atteint pas internet. Ce qui est normal.



Informations complémentaires :

Configuration de l'interface gi3 :

```
vEdge-8#
vEdge-8#sh run int gi3
Building configuration...

Current configuration : 135 bytes
!
interface GigabitEthernet3
 vrf forwarding 9
 ip address 10.1.9.1 255.255.255.0
 negotiation auto
 no mop enabled
 no mop sysid
end

vEdge-8#
```

taper la commande : show ip route vrf 9
On vois la route 0.0.0.0/0 dans la table de routage du vrf 9 .

```
vEdge-8#h ip route vrf 9
help ip route vrf 9
     ^
% Invalid input detected at '^' marker.

vEdge-8#
vEdge-8#
vEdge-8#show ip route vrf 9

Routing Table: 9
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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.9.0/24 is directly connected, GigabitEthernet3
L        10.1.9.1/32 is directly connected, GigabitEthernet3
vEdge-8#
```