Direct Internet Access (DIA) providing internet access to guest users

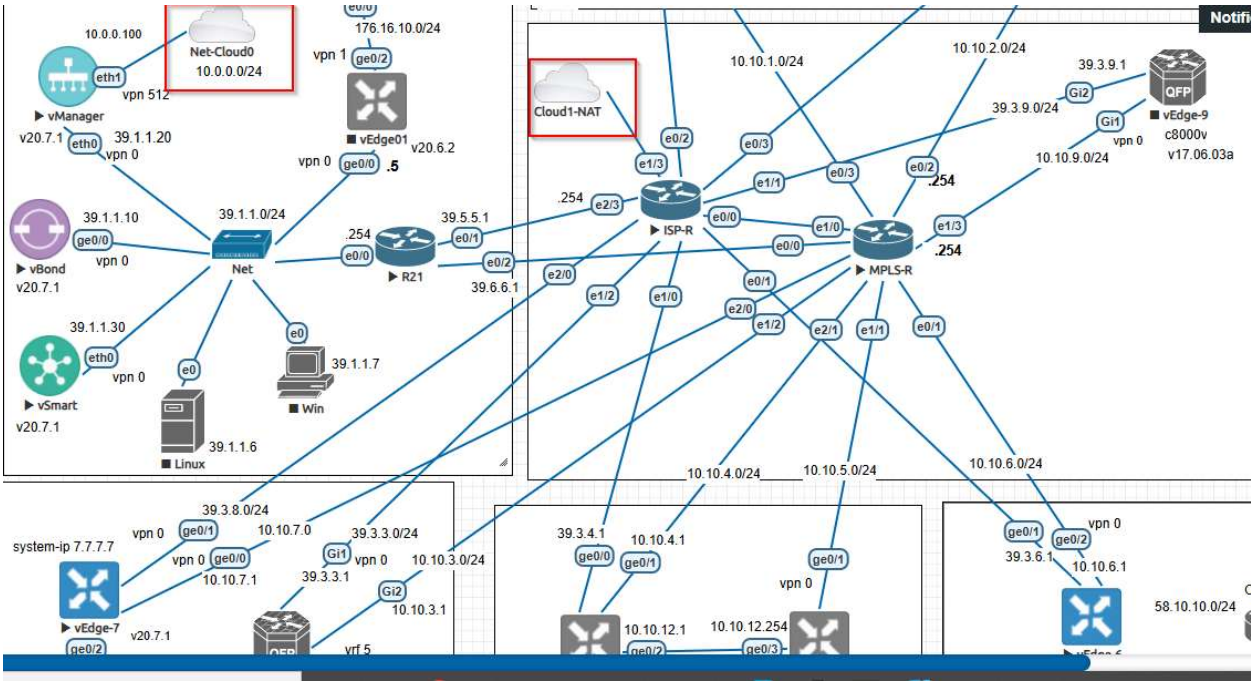
Simulation of SD-WAN on Eve-NG platform

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)

Le labo est basée sur un mélange de Vedges et de Cedges (Cisco). Les Cedges , notamment les c8000v de Cisco ont un un jeux de commande différend des Vedges et donc nécessitent une autre approche.

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

Il faut noter aussi, qu'une autre méthode existe pour faire du DIA avec les Cedges, en utilisant des''data policies '' au niveau de Vsmart. Ce qui pourrait faire l'objet d'un autre lab.



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

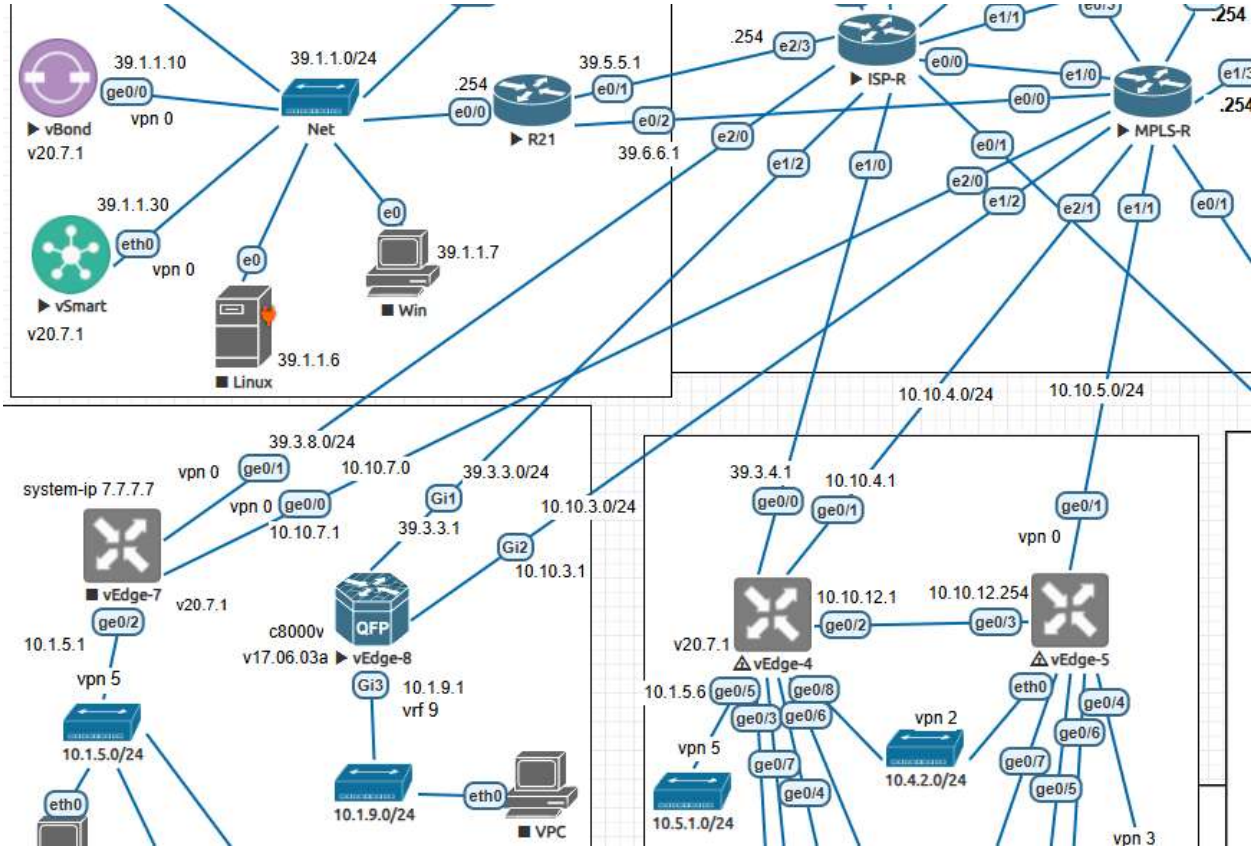
Le routeur ISP-R permet l'accès à internet via l'interface e1/3 . Il est connecté au nuage WAN (cloud1-NAT).

```
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 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 raccordements 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 permets de voir le vrf 9 , 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 :
sur l'interface gi/1 , qui est connectée à un provider ISP (internet) via le routeur ISP-R, taper la commande :
Au niveau de l'interface gi1 , 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
!
```

taper ensuite la commande :
ip nat route vrf 9 0.0.0.0 0.0.0.0 global

```
ip nat settings central-policy
ip nat settings gatekeeper-size 1024
ip nat route vrf 65528 0.0.0.0 0.0.0.0 global
ip nat route vrf 9 0.0.0.0 0.0.0.0 global
no ip nat service h225
no ip nat service ras
no ip nat service rtsp udp
no ip nat service rtsp tcp
no ip nat service netbios-ns tcp
no ip nat service netbios-ns udp
```

taper la commande :
ip name-server vrf 9 8.8.8.8

taper la commande qui définis une access-list :

```
vEdge-8#
vEdge-8#show access-list
Standard IP access list NAT_DIA
    10 permit 0.0.0.0
Extended IP access list meraki-fqdn-dns
vEdge-8#
```

taper la commande :
ip nat inside source list NAT_DIA interface GigabitEthernet1 overload

la commande suivante montre les 3 commandes NAT qui ont été utilisées
show run | include nat

```
vEdge-8# sh run | include nat
 ip nat outside
ip nat settings central-policy
ip nat settings gatekeeper-size 1024
ip nat route vrf 65528 0.0.0.0 0.0.0.0 global
ip nat route vrf 9 0.0.0.0 0.0.0.0 global
no ip nat service H225
no ip nat service ras
no ip nat service rtsp udp
no ip nat service rtsp tcp
no ip nat service netbios-ns tcp
no ip nat service netbios-ns udp
no ip nat service netbios-ssn
no ip nat service netbios-dgm
no ip nat service ldap
no ip nat service sunrpc udp
no ip nat service sunrpc tcp
no ip nat service msrpc tcp
no ip nat service tftp
no ip nat service rcmd
no ip nat service pptp
ip nat inside source list NAT_DIA interface GigabitEthernet1 overload
  destination transport-method http
vEdge-8#
```

Vérifications et tests :

taper la commande : ip route vrf 9 0.0.0.0 0.0.0.0
on vois que le type de la route est de type : NAT DIA

Ensuite , faire une commande : ping vrf 9 google.com
Le résultat montre que le site google.com est atteint.

un ping vers par exemple 8.8.8.8 dans le vrf 9, montre que les utilisateurs du vrf 9 ont accès à internet
La route statique NAT DIA fonctionne.

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.

```
vEdge-8#
vEdge-8#sh ip route vrf 9 0.0.0.0 0.0.0.0

Routing Table: 9
Routing entry for 0.0.0.0/0, supernet
  Known via "nat-route", distance 6, metric 0, candidate default path, type NAT DIA
  Redistributing via omp
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 0, traffic share count is 1
vEdge-8#
vEdge-8#ping vrf 9 google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.250.69.142, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/16/20 ms
```

Configuration de l'interface gi3 :

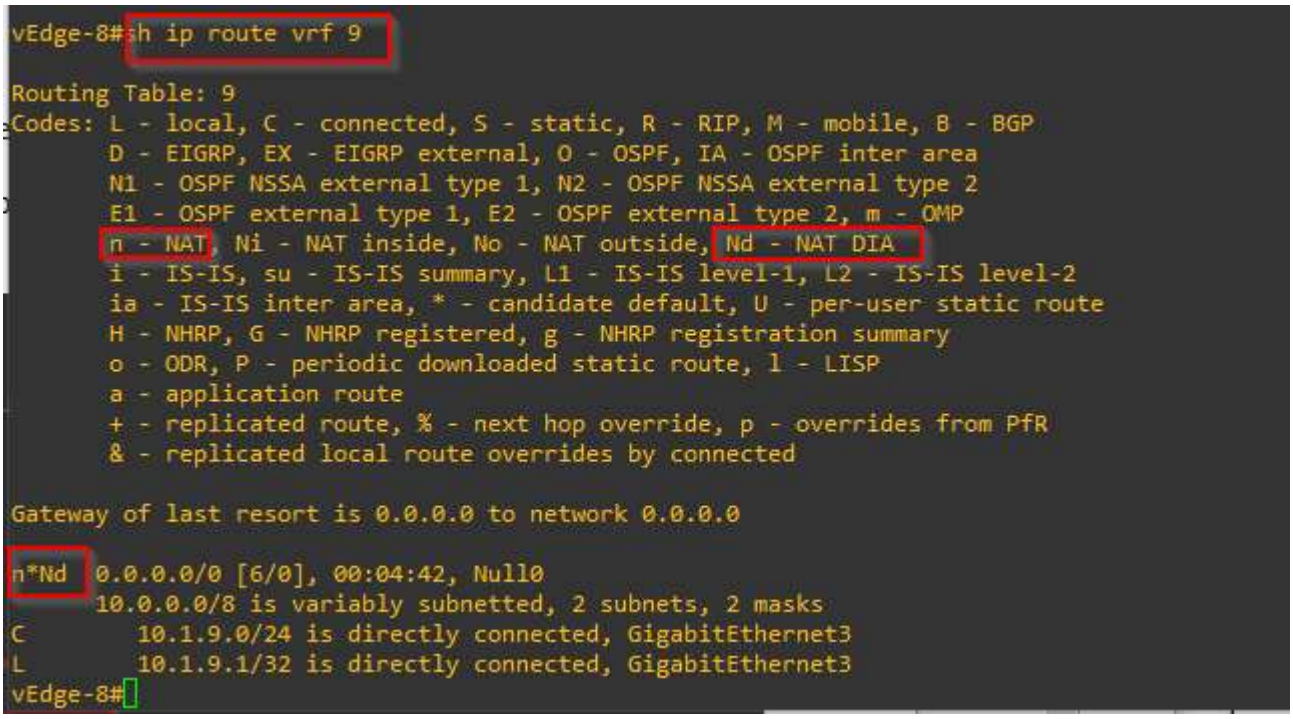
```
vEdge-8#
vEdge-8#sh run int gi3
Building configuration...

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 . La route indique : ‘’n*Nd’’

Nd pour NAT DIA

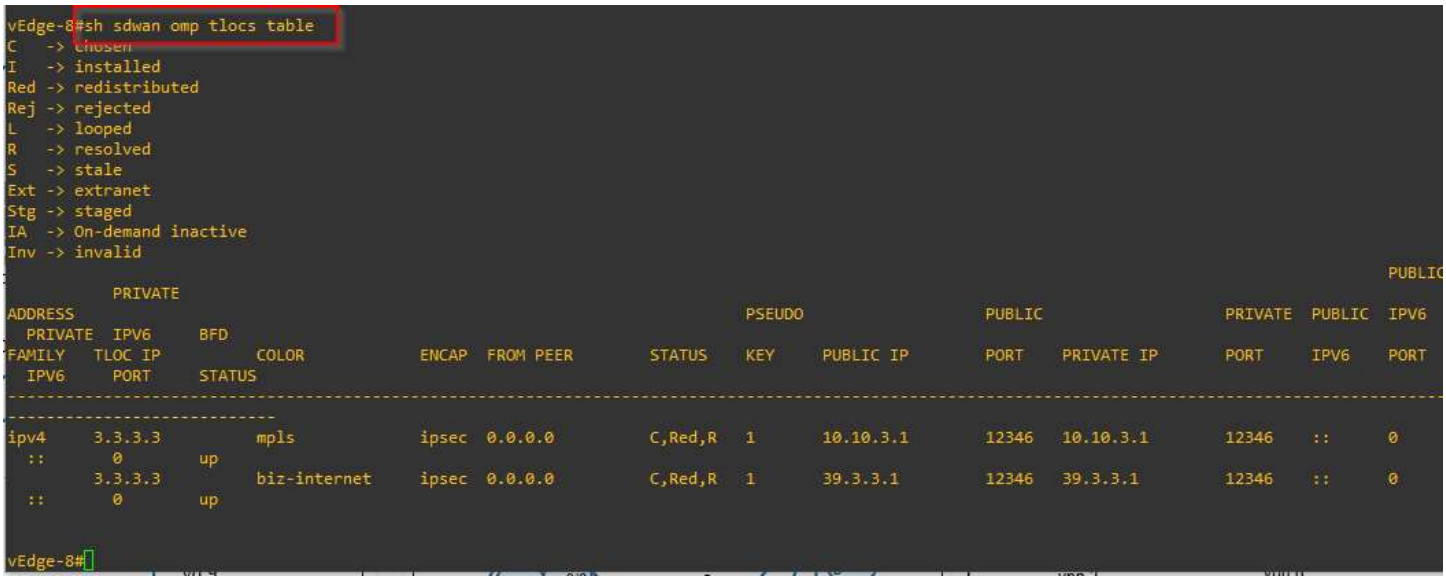
n pour NAT



commandes complémentaires :

show sdwan omp tlocs

Montre sur vedge-8 , les deux TLOCs : 3.3.3.3 mpls ipsec et 3.3.3.3 biz-internet ipsec



Show sdwan bfd sessions
il n'y a pas de sessions bfd, car les autres routeurs Vedges n'ont pas été activées, dans le cadre de ce lab.

```
vEdge-8#show sdwan bfd sessions table
% No entries found.

vEdge-8#
```

Au niveau de Vsmart :
Show omp tlocs | tab

```
vSmart# sh omp tlocs | tab
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Stg -> staged
IA  -> On-demand inactive
Inv -> invalid

                                                                                                                                              PUBLIC           PRIVATE
ADDRESS                                                                          PSEUDO                   PUBLIC                   PRIVATE  PUBLIC  IPV6    PRIVATE  IPV6     BF
D
FAMILY   TLOC IP          COLOR            ENCAP  FROM PEER         STATUS     KEY     PUBLIC IP        PORT    PRIVATE IP       PORT     IPV6    PORT    IPV6     PORT     ST
ATUS  REGION ID   TO PEER
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-----------------------------------
ipv4     3.3.3.3          mpls             ipsec  3.3.3.3           C,I,R      1       10.10.3.1        12346   10.10.3.1        12346    ::      0       ::       0        -
      None
         3.3.3.3          biz-internet     ipsec  3.3.3.3           C,I,R      1       39.3.3.1         12346   39.3.3.1         12346    ::      0       ::       0        -
      None

vSmart#
```