

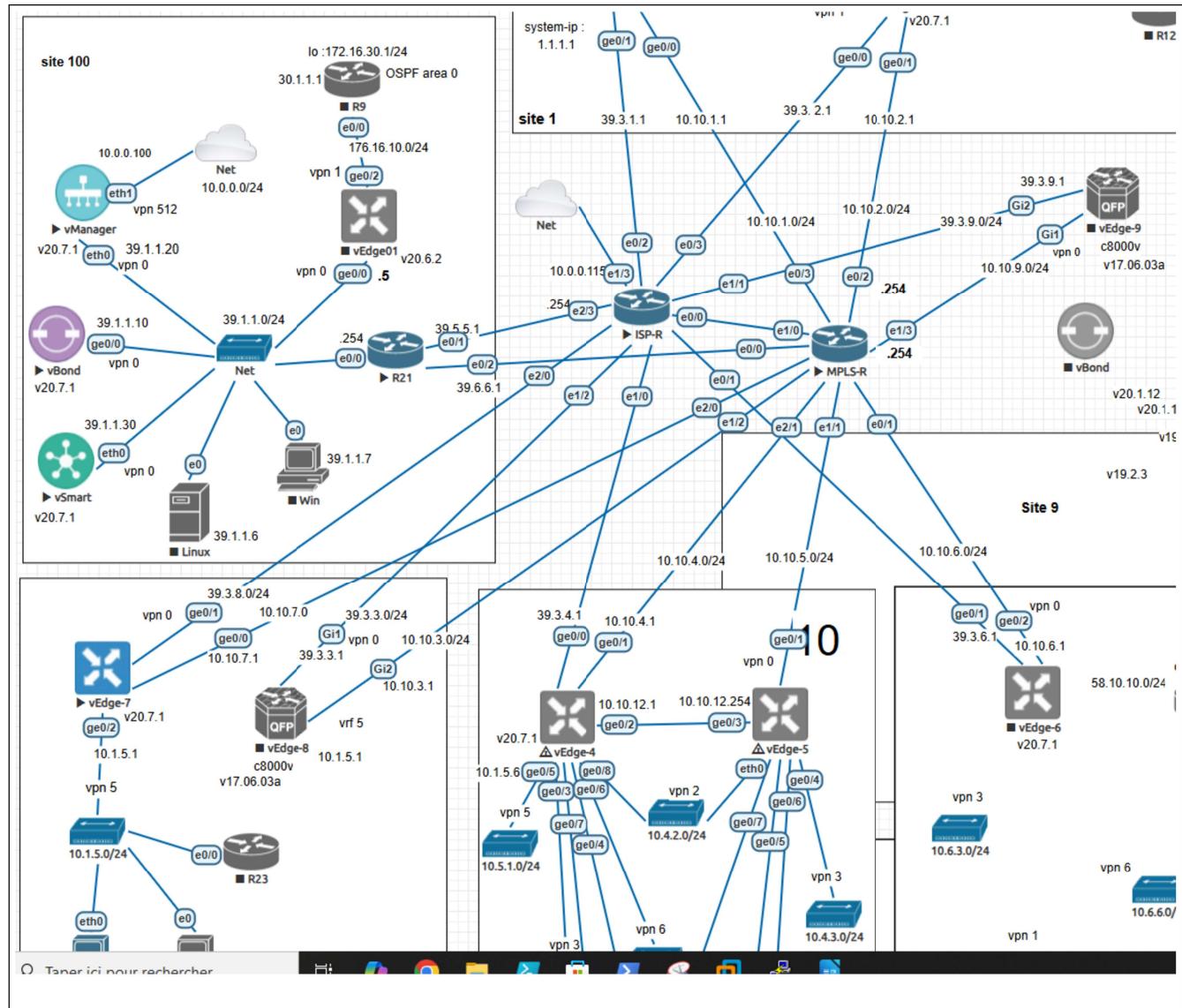
Voici un exemple simple d'application de QOS et de central policy

environnement : labo SD-WAN sur plateforme Eve-NG

vManage v20.7.1, vSmart v20.7.1, vBond v20.7.1, vEdges v20.7.1

schémas du labo sur Eve-NG :

Tous les vEdges n'ont pas été démarrés pour cet exemple :



### Préambule :

Pour que cela fonctionne j'ai mis vManage et vSmart en mode vManage

Les deux devices ne sont plus en mode CLI , mais en mode de gestion via les templates ( j'ai créé deux templates à base de CLI ).

Cisco vManage Select Resource Group Configuration

WAN Edge List Controllers

Search

Add Controller Change Mode

Controller Type	Hostname	System-ip	Site ID	Region ID	Mode	Assigned Template	Draft Mode
vManage	vManage	1.1.1.20	100	--	vManage	vManage-CLI-v1	Disabled
vSmart	vSmart	1.1.1.30	100	--	vManage	vsmart	Disabled
vBond	vBond	1.1.1.10	100	--	CLI	--	Disabled

### Étape 1 :

police centrale , définie sur vManage :

elle s'applique sur tous les vEdges qui sont sur le site 3 et s'applique sur le VPN5 (VPN5 à l'intérieur du périmètre du site numéro 3).

Cisco vManage Select Resource Group Configuration

Centralized Policy Localized Policy

Search

Add Policy Add Default AAR & QoS

Policy Configuration Preview

Name	Description
CLASSIFY-INCOMING-TRAFFIC1	CLASSIFY-INCOMING
site-3-qos-v3	v3
site-3-qos-v4	ewe

```

viptela-policy:policy
  data-policy _VPN-5_QOS-v3
    vpn-list VPN-5
      sequence 1
        match
          protocol 1
          source-ip 0.0.0.0/0
        !
        action accept
        set
          dscp 10
        !
        !
        default-action accept
      !
      lists
        site-list SITE-3
        site-id 3
      !
      vpn-list VPN-5
      vpn 5
    !
  
```

## Étape 2 :

On active la police  
une fois activée , elle est poussée sur vSmart

-----  
ci joint la configuration de la police sur vSmart :

```
vSmart# sh run policy
policy
  data-policy _VPN-5_QOS-v3
    vpn-list VPN-5
      sequence 1
        match
          source-ip 0.0.0.0/0
          protocol 1
        !
        action accept
          set
            dscp 10
        !
        !
        default-action accept
      !
    !
lists
  vpn-list VPN-5
    vpn 5
  !
  site-list SITE-3
    site-id 3
  !
vSmart#
```

## Étape 3 :

vSmart l'applique (pousse la police) sur les vEdges qui sont sur le site 3 et sur le VPN 5 :

sur vEdge-7 (qui est sur le site 3) on peut voir la police qui a été appliquée par vSmart :

```

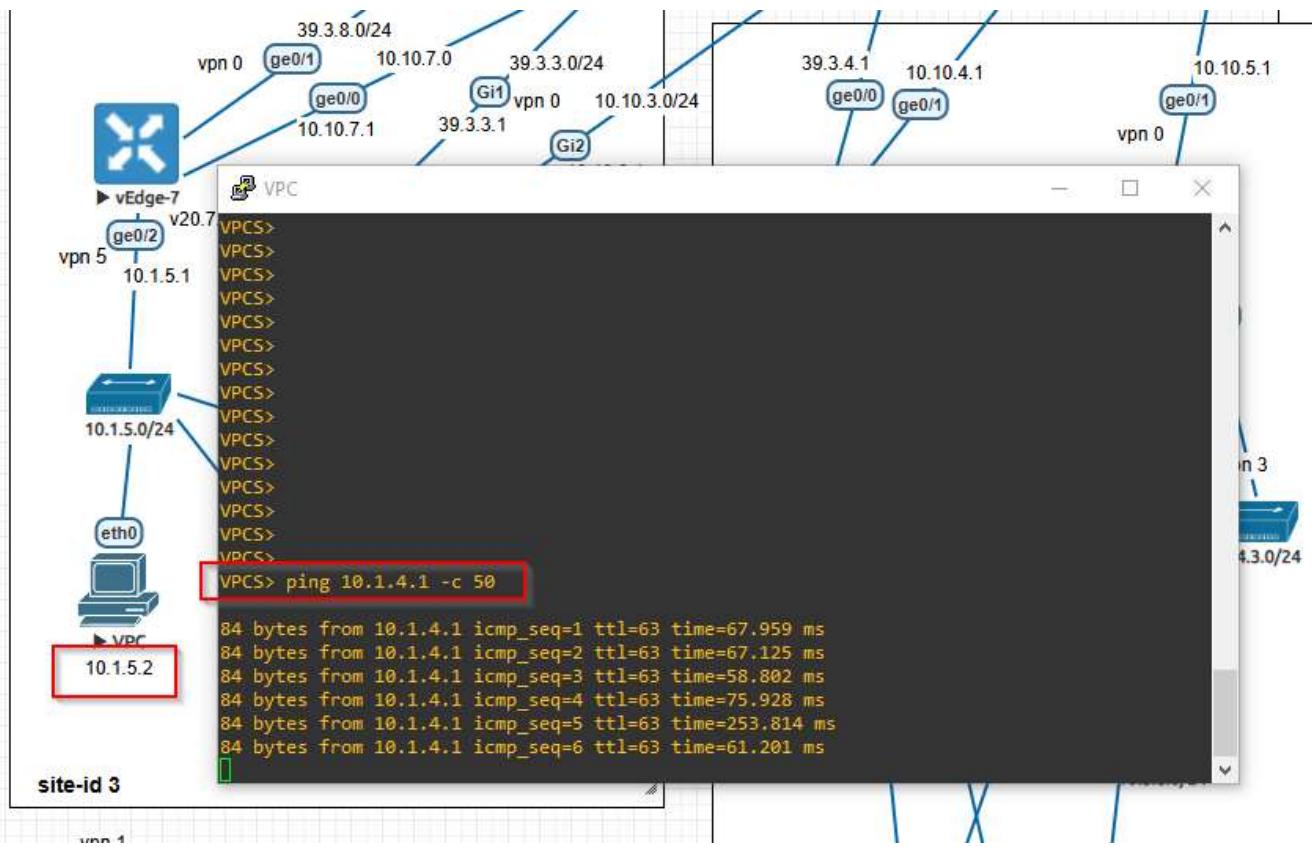
vEdge-7#
vEdge-7# sh policy from-vsmart
from-vsmart data-policy _VPN-5_QOS-v3
direction from-service
vpn-list VPN-5
sequence 1
match
source-ip 0.0.0.0/0
protocol 1
action accept
set
dscp 10
default-action accept
from-vsmart lists vpn-list VPN-5
vpn 5
vEdge-7#

```

#### Étape 4-1 : Tests

ping à partir du vpn 5 : device VPC

On ping le 10.1.4.1



#### Étape 4-2

capture par wireshark sur ge0/2 de vEdge-7

Le device en 10.1.4.1 répond au ping et  
tout le trafic au niveau (entrant) du VPN 5 est marqué avec la valeur DSCP 10  
DSCP 10 correspond à DSP AF11

Pour toutes les occurrences de trafic de l'adresse source 10.1.4.1 vers la destination 10.1.5.2 (10.1.5.2 est dans le vpn 5) , on constate que le paquet IP est marqué avec une valeur DSP = 10 (AF11).

