

BTS SIO

Situation professionnelle numéro 4

Elaboration d'une solution SDN avec VyOS

Description :

Le Software Defined Networking apporte des bénéfices inédits aux entreprises : agilité, flexibilité. La centralisation du réseau avec un découplage des éléments matériels du logiciel.

Mots-clés :

OVH VLANS
VRRP LAN-SIO Manager V6
VMware DHCP-RELAY
FIREWALL IP TOPOLOGIE
NAT SFLOW VyOS
WAN

Validation de la situation professionnelle

Nom	Date	Tampon
	26/05/2014	

Plan de la situation

Le cahier des charges.....	3
L'expression des besoins	3
La description de l'existant.....	3
L'analyse des choix.....	3
Mise en œuvre	4
Réalisation d'un projet SDN avec ovh.....	4
Le serveur EG-64	4
Installation de l'hyperviseur avec le manager V6.....	5
Première connexion à l'hyperviseur	6
Configurations des options louées chez ovh.....	6
Configuration de l'espace de stockage en NFS.....	7
Ajout de la technologie Vrack	8
Ajout de BLOC RIP	9
Configuration de notre SDN dans la ferme de serveurs :	10
La topologie de notre réseau informatique :	11
Solution SDN avec VyOS version "Hydrogen"	12
Configuration de la solution SDN	13
Conclusion de notre infrastructure SDN :	15

Le cahier des charges

L'expression des besoins

Notre société souhaite développer des services dans le cloud de type « privé ».

Deux serveurs d'infrastructure seront loués, avec des options spécifiques :Vrack,RIP,SAN.

Nous serons hébergés chez OVH, avec deux serveurs EG-64 infrastructure et différentes options.

Dans un future proche notre infrastructure sera full SDN afin d'avoir une scalabilité horizontale et un PRA.

L'ensemble de l'infrastructure reposera sur Vmware Vcenter !

Cependant, nous voulons dans un 1^{er} temps prendre conscience des possibilités offertes par un hebergeur, et surtout mettre en œuvre une solution SDN dans une infrastructure de test et découvrir les solutions qui s'offrent à nous avec le déploiement du SDN.

La description de l'existant

La gestion de notre réseau est directement gérée par l'hyperviseur lui-même avec la mise en réseau.

Les hôtes ont un pare-feux interne, la solution réseau est généralement avec une solution « ipcop » ou

« endian » mais elles ne sont plus du tout adaptées à la vision d'un réseau informatique d'aujourd'hui.

L'analyse des choix

Dans notre analyse, nous voulons centraliser nos flux réseaux pour fournir : élasticité et commande centralisée.

L'objectif premier est bien de réfléchir aux avantages d'une solution SDN pour permettre l'adéquation entre d'un côté les ressources (réseaux et IT) et de l'autre les besoins business.

Le SDN permet :

- La suppression des délais de provisioning réseau
- La modification des bandes passantes à la volée
- L'adaptation du paramétrage réseau aux besoins des applications (automatisation)
- L'élasticité des ressources (réseaux et IT)
- La réduction drastique de la complexité de gestion des réseaux

Nous utiliserons comme plateforme de test la ferme de serveur du GretaViva5.

Mise en œuvre

Réalisation d'un projet SDN avec ovh

Le serveur EG-64


Le serveur dédié EG-64 est présent dans la gamme infrastructure de l'hébergeur OVH. La gamme infrastructure permet de profiter de nombreuses options à un prix intéressant. Nous utiliserons deux serveurs dédiés EG-64 interconnectés avec le Vrack d'OVH. Notre but final est d'avoir un équilibrage de charge et une reprise d'activité réseau. Voici la description faite par OVH sur son site :

Serveur dédié EG-64



141,99€ HT* /Mois

Également disponible pour 1 semaine : 53,99€ HT

CPU :	Intel Xeon E5-1650v2 6c/12t 3,5 GHz+/3,9 GHz+
RAM :	64 Go DDR3 ECC 1600MHz
Disques :	2x 3 To SATA3
IP incluses	256 IP
Carte réseau publique :	1x 1 Gbps
Carte réseau vRack :	1x 1 Gbps
Disponibilité :	

Commander

* : Hors frais d'installation qui sont OFFERTS pour tout engagement de 12 mois.

Formules sans engagement : 99,99€ HT à la commande ou +20,00€ HT /Mois durant 6 mois

Pour déployer notre SDN, nous allons sélectionner les options suivantes lors de la commande:

- Une solution de Backup pour nos clients « backup storage » ovh.
- Une baie virtuelle et l'option professionnelle sur notre serveur dédié.
- Deux block RIP avec 8 IP FOx2 (failover).
- Une carte contrôleur: SI : 9271-4i (miroir HDD et SSD)

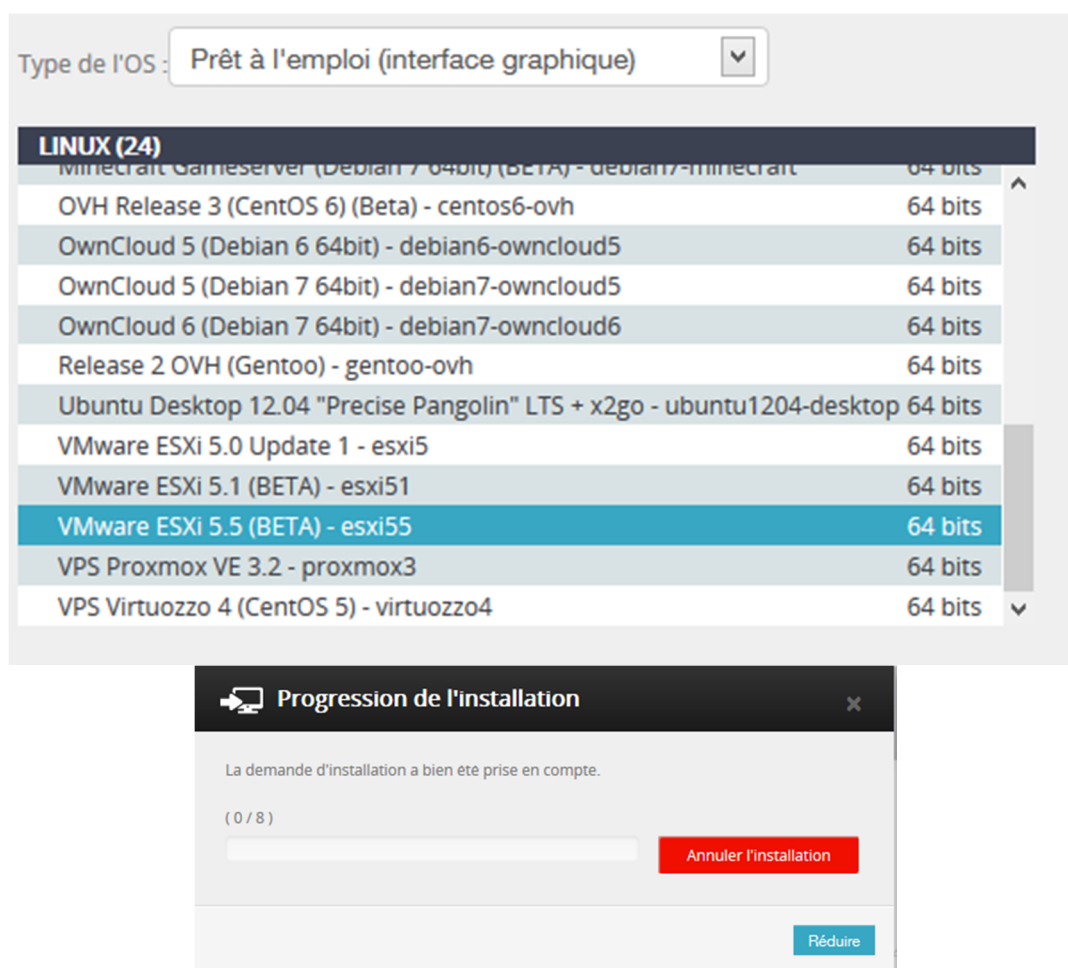
Installation de l'hyperviseur avec le manager V6

L'installation du serveur ESXi se fait via le manager en version 6 d'OVH.

Les étapes de l'installation sont différentes d'une installation standard, et aussi plus simple !

Voici les différentes étapes de l'installation :

1. Connexion à l'interface du manager sur le site d'ovh.
2. Sélectionner notre serveur dédié et choisir : « Installation du serveur dédié »
3. Nous devons sélectionner l'option : « installation à partir d'une template d'ovh »
4. La sélection d'un « système d'exploitation prêt à l'emploi » est validée.
5. Dans le menu déroulant , le choix de l'hyperviseur VMware est disponible.
6. Puis nous validons les changements, l'installation est en cours...



Le temps de l'installation est d'environ 10 minutes.

Un email de confirmation est ensuite reçu, il contient nos identifiants.

L'installation de L'ESXi via l'interface est terminée.

Première connexion à l'hyperviseur

Le premier contact avec l'hyperviseur se fait avec le logiciel : VMWare Vsphere.
Il nous faut télécharger le client VSphère correspondant à la version de notre hyperviseur.
Il existe deux méthodes pour récupérer le logiciel Vsphere :

1. En utilisant le site officiel de VMware avec un compte utilisateur.
2. En se connectant directement sur l'interface « https » du serveur.

Une fois installé, nous l'exécutons et nous nous identifions sur notre hyperviseur.

Configurations des options louées chez ovh

Par défaut notre système VMware est configuré comme ceci :

- Le système de l'hyperviseur est installé sur le disque SSD de 300Go (datastore1).
- Un datastore2 sur un volume de 3To.
- Les options ne sont pas « automatiquement » basculées vers notre serveur.

Pour profiter des options louées chez ovh nous devons configurer / ajouter :

1. Un système de fichier réseau (NFS) connecté sur la seconde carte réseau.
2. Un Vrack pour l'interconnexion de nos deux serveurs VMWare.
3. Deux blocs RIP (gestion des ip public) route vers l'un ou l'autre des serveurs.

Dans la continuité de mes études de cas, je ne développerai que les étapes 2 et 3.

Configuration de l'espace de stockage en NFS

Avec la gamme de serveurs dédiés, OVH nous offre un espace de sauvegarde de 500 Go par serveur (gratuitement). L'espace est entièrement gérée par OVH et mis à disposition au client final.

L'option "backup storage" est dans le manager : "commande de l'espace disque".

Nous avons commandé un espace de 500Go supplémentaire soit 1To à 12€ (ht) :

Capacité	Prix (par mois HT)
<input type="radio"/> 1000 Go	12.00 €
<input checked="" type="radio"/> 5000 Go	40.00 €
<input type="radio"/> 10000 Go	60.00 €

Ip	CIFS	FTP	NFS	Statut
/32	✓	✓	✓	Active

Les identifiants ne sont utilisables que sur notre serveur, par mesure de sécurité les IP/DNS sont masqués.

Ajoutons "le storage backup" en NFS :

Dans l'hyperviseur, il faut se rendre dans le menu : configuration et l'onglet : stockage.

Puis, il nous faut "ajouter un stockage" dans "système de fichiers réseaux" tel que :

Propriétés

Serveur: ovh.net
Exemples : nas, nas.it.com, 192.168.0.1 ou FE80:0:0:0:2AA:FF:FE9A:4CA2

Dossier: /export/ftpbackup/ovh.net/
Exemple : /vols/vol0/datastore-001

Montage NFS lecture seule

Nom banque de données: datastore_NFS

L'hyperviseur ajoute ensuite ce système de fichier en réseau (NFS), voici les tâches en cours :

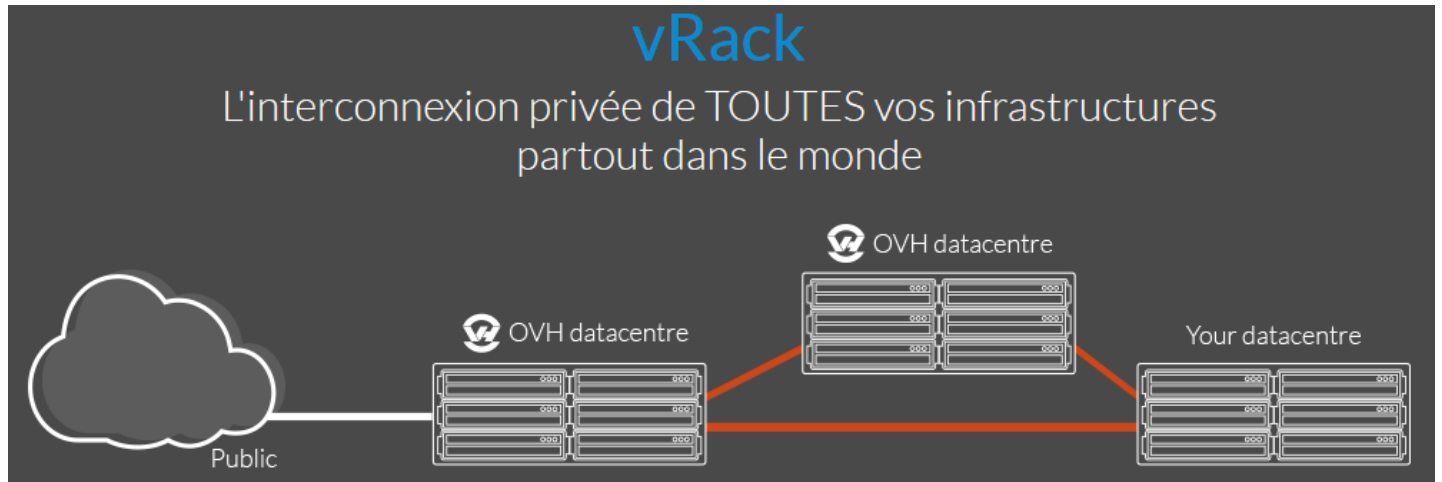
Nom	Cible
Créer une banque de données NAS	

La configuration de notre banque de données NFS est terminée :

Identification	Périphérique	Type de lecteur	Capacité	Libre	Type	Dernière mise à jour	Accélération matérielle
datastore_NFS	...	Inconnue	1 000,00 G	1 000,00 G	NFS	19/05/2014 13:53:29	Non pris en charge
datastore1	Local LSI Disk (n...	Non-SSD	271,50 Go	216,39 Go	VMFSS	25/04/2014 12:50:18	Non pris en charge
datastore2	Local LSI Disk (n...	Non-SSD	2,73 To	1,42 To	VMFSS	25/04/2014 12:50:18	Non pris en charge

Ajout de la technologie Vrack

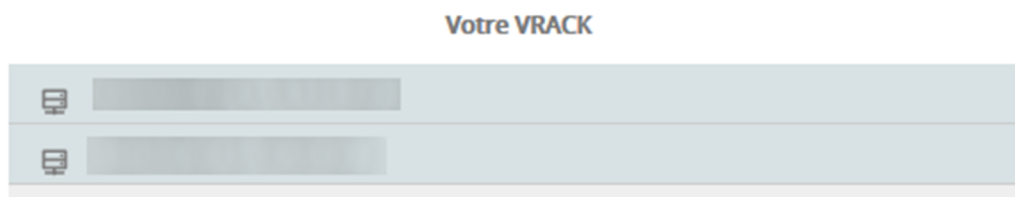
La technologie vRack (baie virtuelle) permet de connecter, isoler ou répartir les services OVH.com au sein d'un ou plusieurs réseaux privés et sécurisés. Nous pouvons bâtir des infrastructures privées complexes sur un périmètre multidatacentre mondial :



Source : <https://www.ovh.com/fr/solutions/vrack/>

L'option "Vrack" est disponible dans le manager version 6, comme pour le "backup storage" :
Il est fourni avec notre serveur mais nous devons passer une commande pour l'ajouter dans notre manager.
Une fois le Vrack disponible il nous suffit de les "Ajouter" dans la même infrastructure :

Après avoir cliqué sur le bouton "ajouter" ;voici nos deux serveurs listés qui n'appartiennent au mêmeVrack :



Nos deux serveurs peuvent désormais communiquer entre eux par la seconde carte réseau disponible.
On comprend qu'il appartient donc au même réseau privée, nous pouvons les joindre.

Ajout de BLOC RIP

Définir notre plan d'adressage, le router, le basculer jusqu'à 256 adresses IP publiques, nos deux serveurs EG-64 ont une capacité de gestion d'un réseau accru, et avec une Baie Virtuelle ,tout cela se fait en quelques secondes.

Ce service nous permet de renforcer la continuité de services de nos applications, et aussi d'optimiser notre référencement "international" et de personnaliser le whois Ripe !!

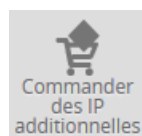
Source : https://www.ovh.com/fr/serveurs_dedies/blocs_ip_ripe_vrack.xml

Pour disposer de nos future Bloc RIP, rendons nous dans le manager V6 et créons une organisation :



Ensuite, nous pouvons organiser nos blocs RIPE :

Organisation	Type	Nom	Abuse
RIPE_	RIPE	Kevin	es2com.fr
Téléphone		Adresse	
00336			



Ensuite, il nous suffit de commander nos différents blocs ripe :

Voici un exemple d'utilisation de notre bloc RIP:

FO-1 : CloudStack pour Hébergement web mutualisé (http/https/ftp/Mysql/webmail)

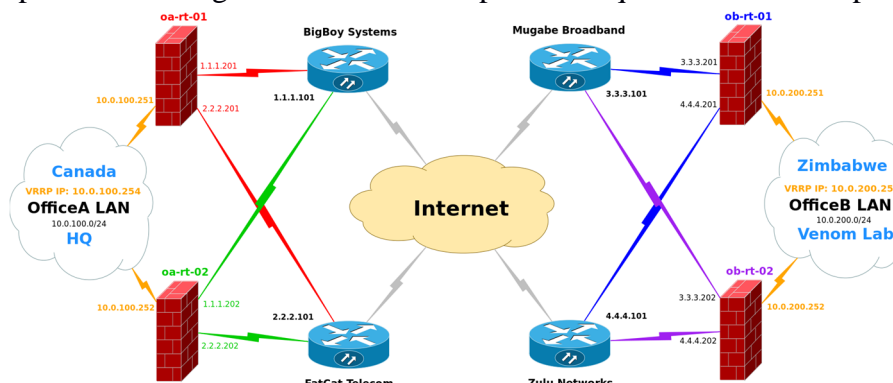
FO-2 : es2com (SCSM 2008, AD, Vcenter, Gestion licence RDP, WSUS, NAP)

FO-3 : Sett-interim (VPN, Progiciel compatibilité, RDP)

FO-4 : [client-autres] (VPN , Progiciel compatibilité, RDP)

Avec l'ensemble de nos options nous serons dans la capacité de pouvoir mettre en oeuvre des infrastructures complexes, cependant avec l'élément SDN la configuration et l'administration sont très aisées !

Exemple d'une configuration de haute disponibilité qui est maintenant possible :



source : <http://www.vyatta4people.org/highly-available-openvpn-connection-between-two-offices/>











Configuration de notre SDN dans la ferme de serveurs :

Le Software-Defined Networking (SDN) correspond à une mise en réseau basée sur logiciel.

Le SDN permet aux administrateurs du réseau de gérer aisément des services en ligne par la virtualisation de fonctionnalités de niveau inférieur. C'est une nouvelle architecture de réseau, dans laquelle le plan de contrôle est totalement découplé du plan de données.

Il permet de virtualiser le réseau de bout en bout et de déployer le plan de contrôle sur des plateformes aux capacités accrues. Couplé à une interface de programmation, le SDN permet de développer des services réseaux à forte valeur ajoutée.

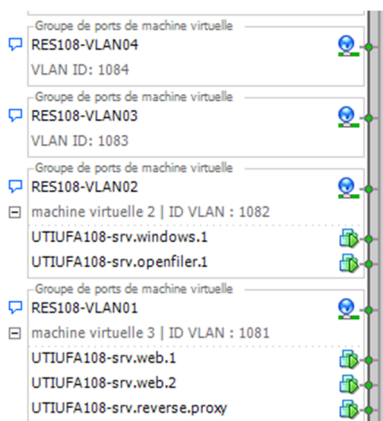
L'installation d'une machine sous VMware est très simple et pour cette raison je ne la détaillerai pas. Nous allons simplement spécifier la configuration matériel de notre machine VyOS :

Matériel	Résumé
 Mémoire	256 Mo
 CPU	1
 Carte vidéo	Carte vidéo
 Périphérique VMCI	Restreint
 Contrôleur SCSI 0	Parallèle logique de LSI
 Disque dur 1	Disque virtuel
 Lecteur CD/DVD 1	Périphérique client
 Adaptateur réseau 1	LAN SIO
 Adaptateur réseau 2	RES108
 Lecteur de disquettes 1	Périphérique client

Nous disposons donc de deux cartes réseau : LAN SIO (WAN) & RES108 (LAN)
Notre groupe de port "RES108" est directement relié à une DMZ-IPCOP (LAN-SIO) relié au VMkernel de notre hôte :



Remarquer que les deux SDN ont la possibilité de tagguer des trames dans toutes les VLANs.
En effet, l'administrateur de la ferme m'a configuré 4 autres VLANs :



L'optimisation du SDN avec uniquement deux cartes réseaux dans ma machine !

Dans le cadre de notre plateforme de tests, nous disposerons d'une ferme de serveurs sous Vcenter. Nous installerons une instance de notre routeur logiciel et nous le "clonerons" à la fin de l'installation. La disposition de notre architecture SDN comprendra alors deux VyOS :

- UTIUFA108-vyOS.1 et UTIUFA108-vyOS.2

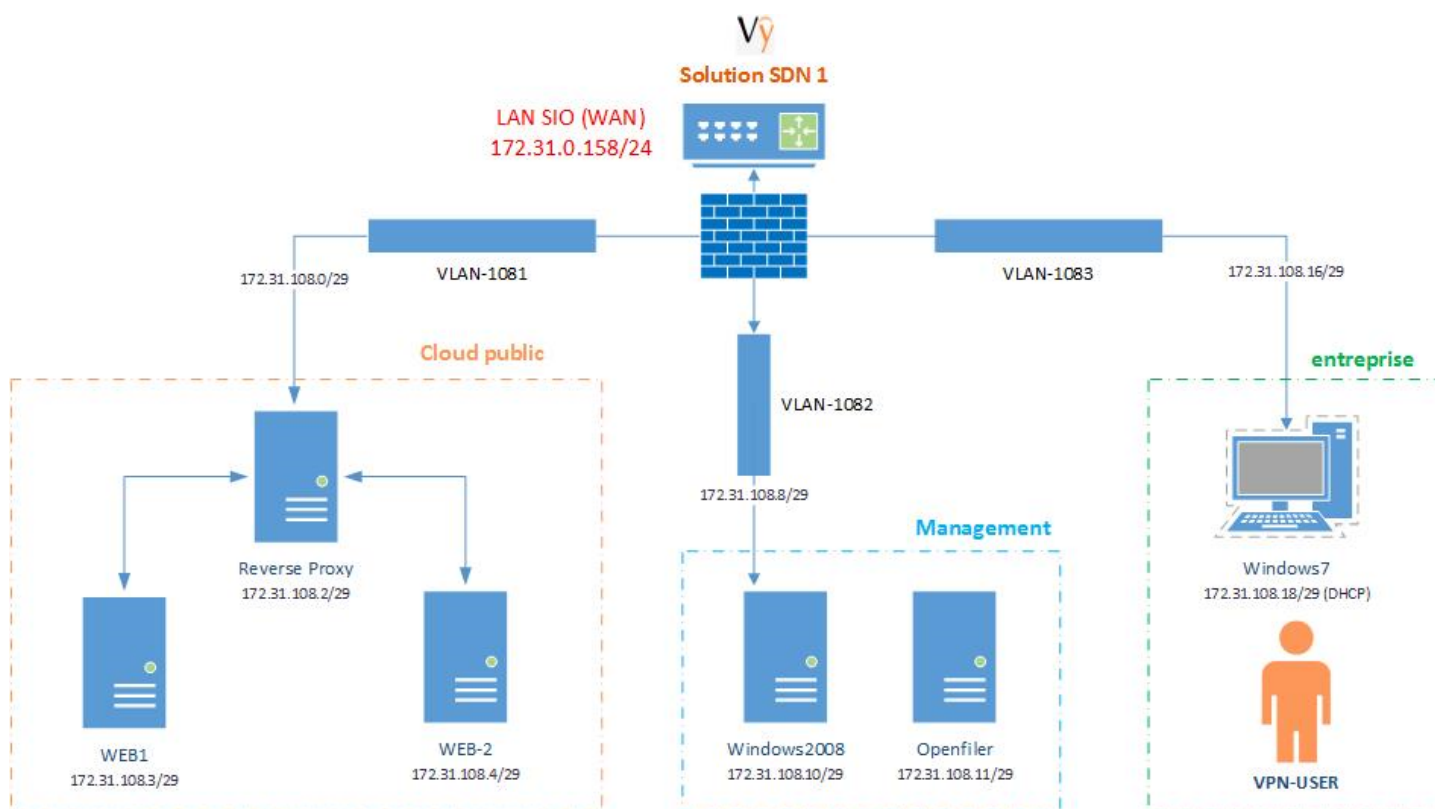
Le 1^{er} vyOS sera configuré de la façon suivante :

- LAN SIO : 172.31.0.158/24
- RES108-VLAN1 : 172.31.108.1/29
- RES108-VLAN2 : 172.31.108.9/29
- RES108-VLAN3 : 172.31.108.17/29

Le 2^{ème} vyOS sera configuré de la façon suivante :

- LAN SIO : DHCP
- RES108-VLAN1 : 172.31.108.5/29
- RES108-VLAN2 : 172.31.108.13/29
- RES108-VLAN3 : 172.31.108.21/29

La topologie de notre réseau informatique :



Nous allons maintenant passer à l'installation et la configuration de notre solution SDN-1 : Vyos-1

Solution SDN avec VyOS version “Hydrogen”

VyOS est un fork de la communauté de Vyatta, un système d'exploitation réseau basé sur Linux qui assure le routage lui-même basé sur un logiciel réseau, pare-feu, et VPN.

Vyatta est mort depuis que la société Brocade à racheté Vyatta en 2012, cependant la version open source était toujours mainten. Mais Brocade a annoncé l'arrêt du développement de Vyatta.... Heureusement VyOS est là !

VyOS étant un fork de la solution Vyatta open-source lancé en 2006 on comprend que :

Vyatta, Brocade V5400 et VyOS sont quasi identiques, cependant VyOS et Vyatta n'ont pas l'HTTPS et l'API.

Dans ma vision des choses, en tant qu'administrateur réseau & système, l'interface web n'est pas indispensable, l'API est par contre un énorme manque pour VyOS !

Elle devrait prochainement arriver tout comme l'interface WEB et d'autres développements en cours.

Je vais moi-même me lancer dans le développement du projet VyOS après mes études en Juillet 2014.

Téléchargement de l'ISO pour notre machine virtuelle :

Le site de la communauté de développeurs propose le téléchargement de la solution SDN :

Get the Software

Current stable release: VyOS 1.0.3. (Hydrogen)
Next release: Helium

Downloads: <http://mirror.vyos.net/iso/release/1.0.3>

- Physical and virtual 64-bit: [vyos-1.0.3-amd64.iso](#)
- Physical 32-bit: [vyos-1.0.3-i586.iso](#)
- Virtual 32-bit: [vyos-1.0.3-i586-virt.iso](#)

You can verify the build signature against our [Public key](#).

- [Mirrors](#)
- [View Git Repositories](#)
- Development Builds: <http://builds.vyos.net/>

Amazon Web Services (AWS)

- [VyOS on AWS Marketplace](#)

L'installation de VyOS

Nous lançons Vyos au démarrage (Il est identique à celui de Vyatta sans le logo), appuyons sur la touche :

Entrée

Par défaut le login et le mot de passe sont “vyos” et la configuration du clavier est en qwerty.



Pour lancer l'installation de VyOS : `install-system`

Ensuite il y'a 3 questions très simples et auxquelles il vous faut répondre par choix multiples.

Configuration de la solution SDN

Nous sommes fin prêt à déployer la solution étape par étape :

1. Configuration du système : route, dns, gateway, flow accounting/sflow :
2. Configuration des interfaces réseaux avec VLANS : eth1.1081, 1082, 1083
3. Configuration des services : dhcp-relais, vrrp
4. Configuration du VPN : pptp
5. Mise en place de règles de pare-feu sur les interfaces : eth0 (in) et eth1.1081 (in)
6. Configuration des NAT sources et destination

Nous aborderons les points numero 1 (route, flow accounting, sflow), 2, 3, 4, 5 et 6.

La configuration concerne par défaut le routeur VyOS-1, nous préciserons la configuration de VyOS-2.

La configuration du système : flow-accounting avec sflow

Le flow accounting et le sflow permettent de monitorer nos interfaces réseaux

```
set system flow-accounting interface eth0
set system flow-accounting interface eth1.1081
set system flow-accounting interface eth1.1082
set system flow-accounting interface eth1.1083
set system flow-accounting sflow server 172.31.108.10
```

La configuration des interfaces réseaux (vlans)

Les vlans permettent de séparer nos réseaux.

VyOS-1 :

```
set interfaces ethernet eth1 vif 1081 address 172.31.108.1/29
set interfaces ethernet eth1 description cloud-public

set interfaces ethernet eth1 vif 1082 address 172.31.108.9/29
set interfaces ethernet eth1 description management

set interfaces ethernet eth1 vif 1083 address 172.31.108.17/29
set interfaces ethernet eth1 description entreprise
```

VyOS-1 :

```
set interfaces ethernet eth1 vif 1081 address 172.31.108.5/29
set interfaces ethernet eth1 description cloud-public

set interfaces ethernet eth1 vif 1082 address 172.31.108.16/29
set interfaces ethernet eth1 description management

set interfaces ethernet eth1 vif 1083 address 172.31.108.21/29
set interfaces ethernet eth1 description entreprise
```

La configuration des services (dhcp-relais)

Le relai DHCP permet de laisser passer le dhcp de windows dans le vlan "entreprise".

```
set service dhcp-relay interface eth1.1082
set service dhcp-relay interface eth1.1083
set service dhcp-relay server 172.31.108.10
```

La configuration des services (vrrp)

Le service vrrp permet d'avoir une passerelle disponible si un routeur est down.

VyOS-1 :

```
set interfaces ethernet eth1 vif 1081 vrrp vrrp-group 1 virtual-address 172.31.108.6
set interfaces ethernet eth1 vif 1081 vrrp vrrp-group 1 priority 50
set interfaces ethernet eth1 vif 1081 vrrp vrrp-group 1 preempt true

set interfaces ethernet eth1 vif 1082 vrrp vrrp-group 1 virtual-address 172.31.108.14
set interfaces ethernet eth1 vif 1082 vrrp vrrp-group 1 priority 50
set interfaces ethernet eth1 vif 1082 vrrp vrrp-group 1 preempt true

set interfaces ethernet eth1 vif 1083 vrrp vrrp-group 1 virtual-address 172.31.108.22
set interfaces ethernet eth1 vif 1083 vrrp vrrp-group 1 priority 50
set interfaces ethernet eth1 vif 1083 vrrp vrrp-group 1 preempt true
```

VyOS-2 :

```
set interfaces ethernet eth1 vif 1081 vrrp vrrp-group 1 virtual-address 172.31.108.6
set interfaces ethernet eth1 vif 1081 vrrp vrrp-group 1 priority 10
set interfaces ethernet eth1 vif 1081 vrrp vrrp-group 1 preempt true

set interfaces ethernet eth1 vif 1082 vrrp vrrp-group 1 virtual-address 172.31.108.14
set interfaces ethernet eth1 vif 1082 vrrp vrrp-group 1 priority 10
set interfaces ethernet eth1 vif 1082 vrrp vrrp-group 1 preempt true

set interfaces ethernet eth1 vif 1083 vrrp vrrp-group 1 virtual-address 172.31.108.22
set interfaces ethernet eth1 vif 1083 vrrp vrrp-group 1 priority 10
set interfaces ethernet eth1 vif 1083 vrrp vrrp-group 1 preempt true
```

La configuration du VPN pptp

```
set vpn pptp remote-access authentication mode local
set vpn pptp remote-access dns-servers server-1 8.8.8.8
set vpn pptp remote-access client-ip-pool start 172.31.108.19
set vpn pptp remote-access client-ip-pool stop 172.31.108.21
set vpn pptp remote-access authentication local-users username jeremie password MyPwd@2
```

Configuration de deux règles pare-feu

```
set firewall name internet
set firewall name internet rule 1 default-action drop
set firewall name internet rule 1 action accept
set firewall name internet rule 1 destination address 0.0.0.0./0
set firewall name internet rule 1 destination port 80,1723
set firewall name internet rule 1 protocol tcp_udp

set firewall name cloud rule 1
set firewall name cloud rule 1 default-action drop
set firewall name cloud rule 1 action accept
set firewall name cloud rule 1 destination address 172.31.108.2/29
set firewall name cloud rule 1 destination port 443, 80
set firewall name cloud rule 1 source address 172.31.108.0/28
set firewall name cloud rule 1 protocol tcp_udp
```


Configuration des NAT :

```
source set nat source rule 1 source address 172.31.108.0/29
set nat source rule 1 inbound-interface eth0
set nat source rule 1 translation address masquerade

set nat source rule 2 source address 172.31.108.8/29
set nat source rule 2 inbound-interface eth0
set nat source rule 2 translation address masquerade
set nat source rule 3 source address 172.31.108.16/29
set nat source rule 3 inbound-interface eth0
set nat source rule 3 translation address masquerade

set nat destination rule 1 action accept
set nat destination rule 1 destination address 172.31.0.158/24
set nat destination rule 1 destination port 80
set nat destination rule 1 protocol tcp_udp
set nat destination rule 1 translation adresse 172.31.108.2/29
```

Configuration du firewall internet sur eth0 :

```
set interfaces ethernet eth0 firewall in name internet
```

Conclusion de notre infrastructure SDN :

Dans la topologie de notre réseau nous avons configuré différents protocoles.

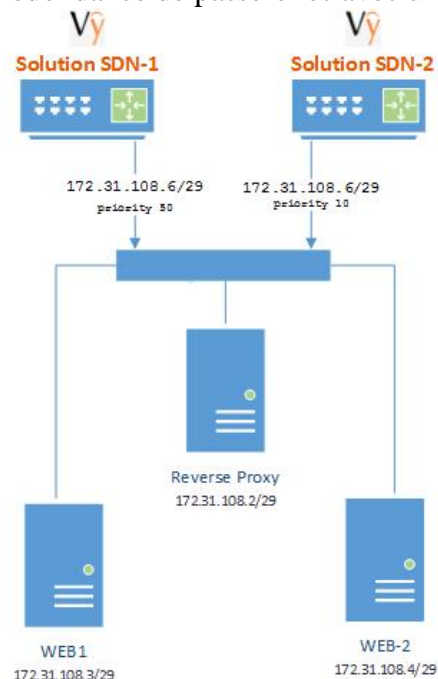
Voici les possibilités qu'offrent notre réseau SDN :

- Le monitoring de nos interfaces réseaux sur VyOS-1
- La séparation des réseaux dans plusieurs vlan logiques (vlans) adresse CIDR.
- Un relais DHCP entre deux VLANS (routage de niveau 3)
- Une continuité de services pour la redondance de passerelles par défaut.
- Une solution d'accès distant simple et peu sécurisée mais sécurisée quand même !
- Des règles pare-feu sur deux interfaces (eth0 et eth1.1082)
- Possibilité de fournir le web à différents réseaux et un NAT destination vers un cloud.

D'autres possibilités peuvent être déployées telle que du Loadbalancing WAN par exemple.

On retiendra de notre architecture deux schémas :

La solution de continuité de services, redondance de passerelles avec un exemple dans le vlan-1 :



Le fonctionnement global de notre solution SDN :

