VMWARE NSX

LE SDN ADAPTÉ AUX ENVIRONNEMENTS VSPHERE

Julien CABESSUT (UT2J) pour Capitoul
12/2016

SOMMAIRE

- Pourquoi virtualiser les réseaux ?
- VXLANs et VTEPs : la magie de l'ethernet embarqué dans UDP
- Data plane, control plane, management plane
- Micro-segmentation et filtrage contextuel
- Edge Services Gateways : aux frontières du réel
- Ce qui est bien mais pas top

POURQUOI VIRTUALISER LES RÉSEAUX ?

PARCE QU'IL FAUT BIEN VENDRE, MAIS PAS QUE…

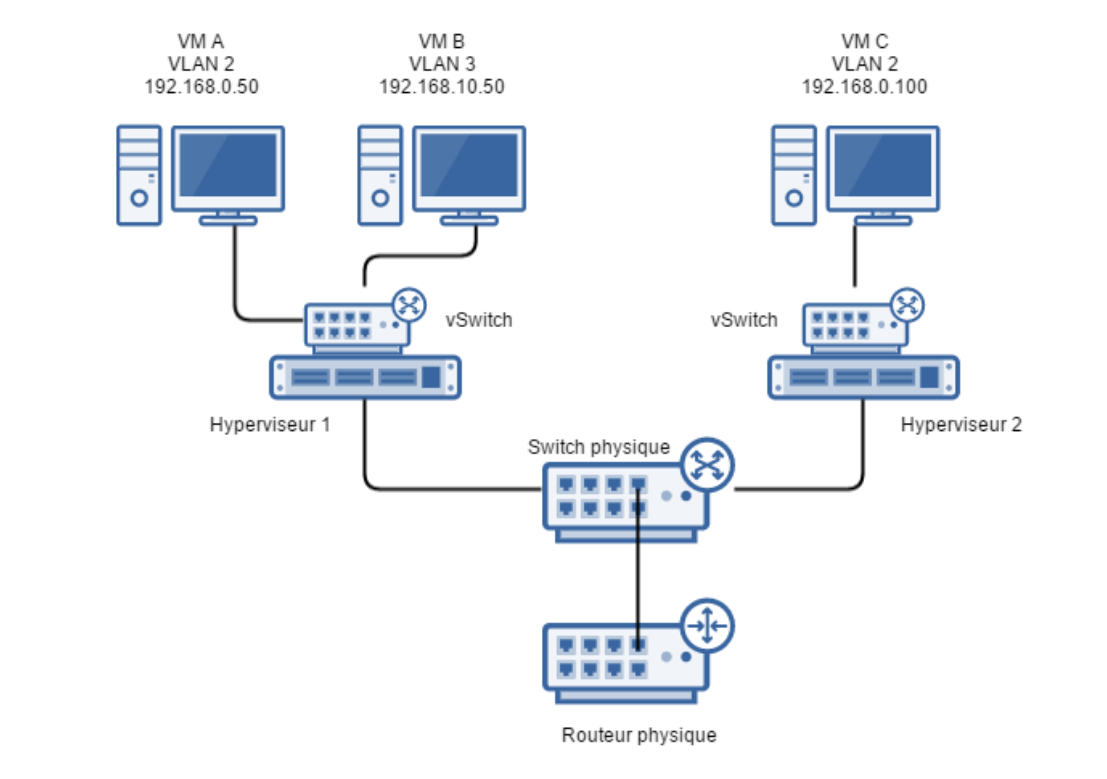
POURQUOI VIRTUALISER LES RÉSEAUX ?

- Limiter les interventions sur le hardware
- Migrer ou déployer facilement des architectures complexes
- Optimiser les performances
- Gagner en visibilité
- Automatiser

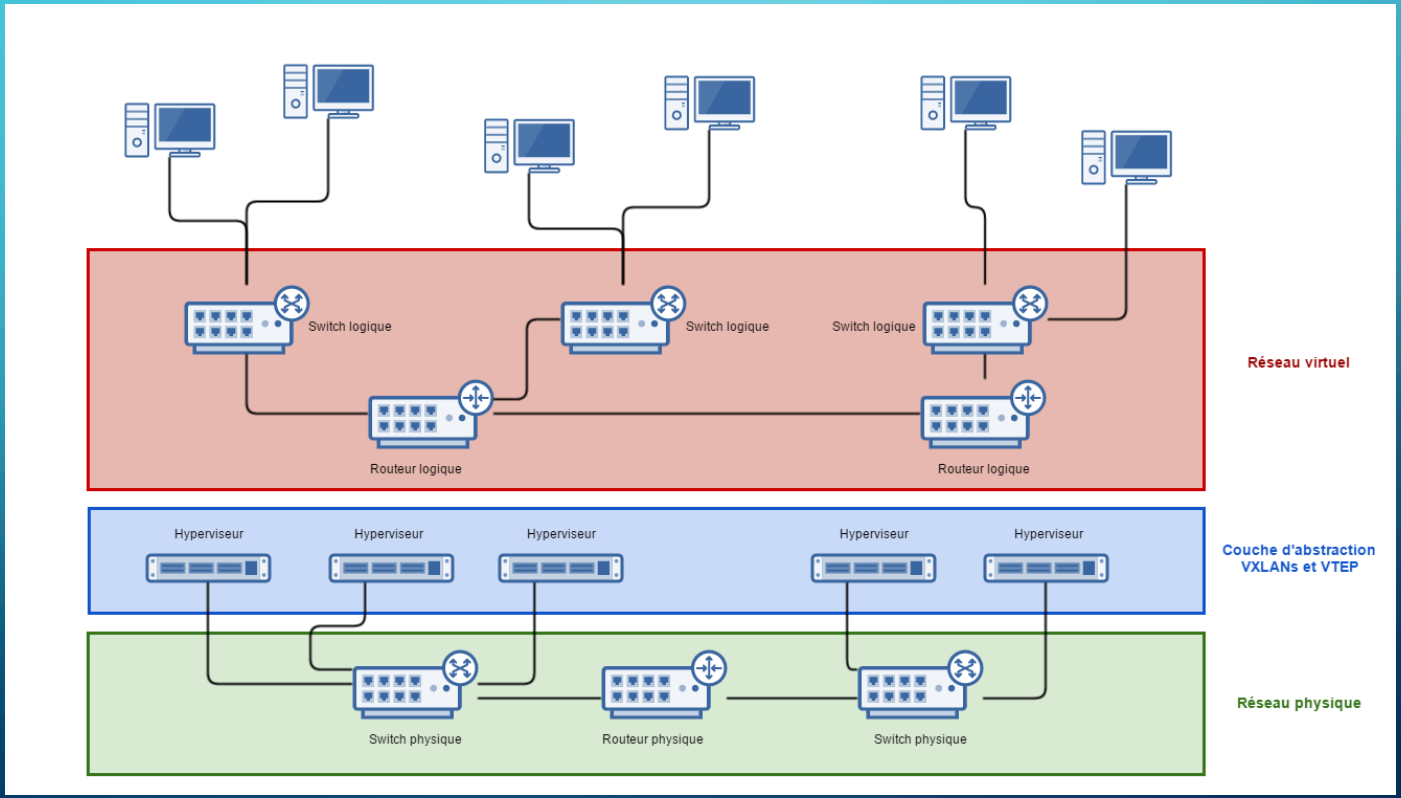
VXLANS ET VTEPS : LA MAGIE DE L'ETHERNET EMBARQUÉ DANS UDP

DU L2 DANS DU L3 DANS DU L2, LE KAMASUTRA DU MODELE OSI

VXLANS ET VTEPS : LA MAGIE DE L'ETHERNET EMBARQUÉ DANS UDP



VXLANS ET VTEPS : LA MAGIE DE L'ETHERNET EMBARQUÉ DANS UDP



VXLANS ET VTEPS : LA MAGIE DE L'ETHERNET EMBARQUÉ DANS UDP

- Tunnels entre les hyperviseurs
- Possibilité de « router » du L2
- Segmentation (presque) illimitée
- Le hardware ne connaît que les VTEPs
- Overhead : attention au MTU !

DATA PLANE, CONTROL PLANE, MANAGEMENT PLANE

(LE PREMIER QUI FAIT UNE BLAGUE SUR LE DELTAPLANE A PERDU)

Animated Slide

COMPOSANTS DE NSX

Management Plane

NSX Manager

- Point de configuration unique
- Présente l'API REST

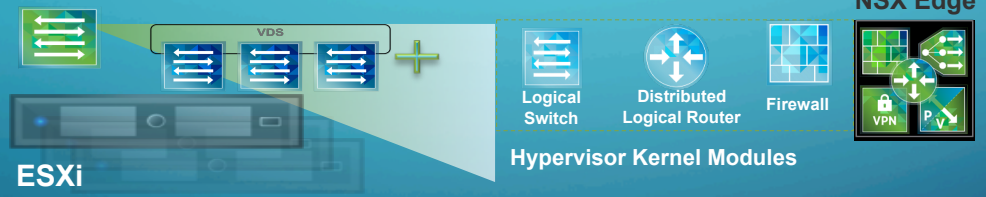
Control Plane

NSX Controller

- Manage les réseaux logiques
- VXLAN/Routage distribué
- Complétement séparé du Data Plane

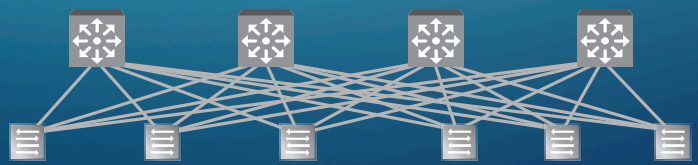
Data Plane

Distributed Services



- Distribution du data-plane dans les hyperviseurs
- Services hautes performances

Réseau physique



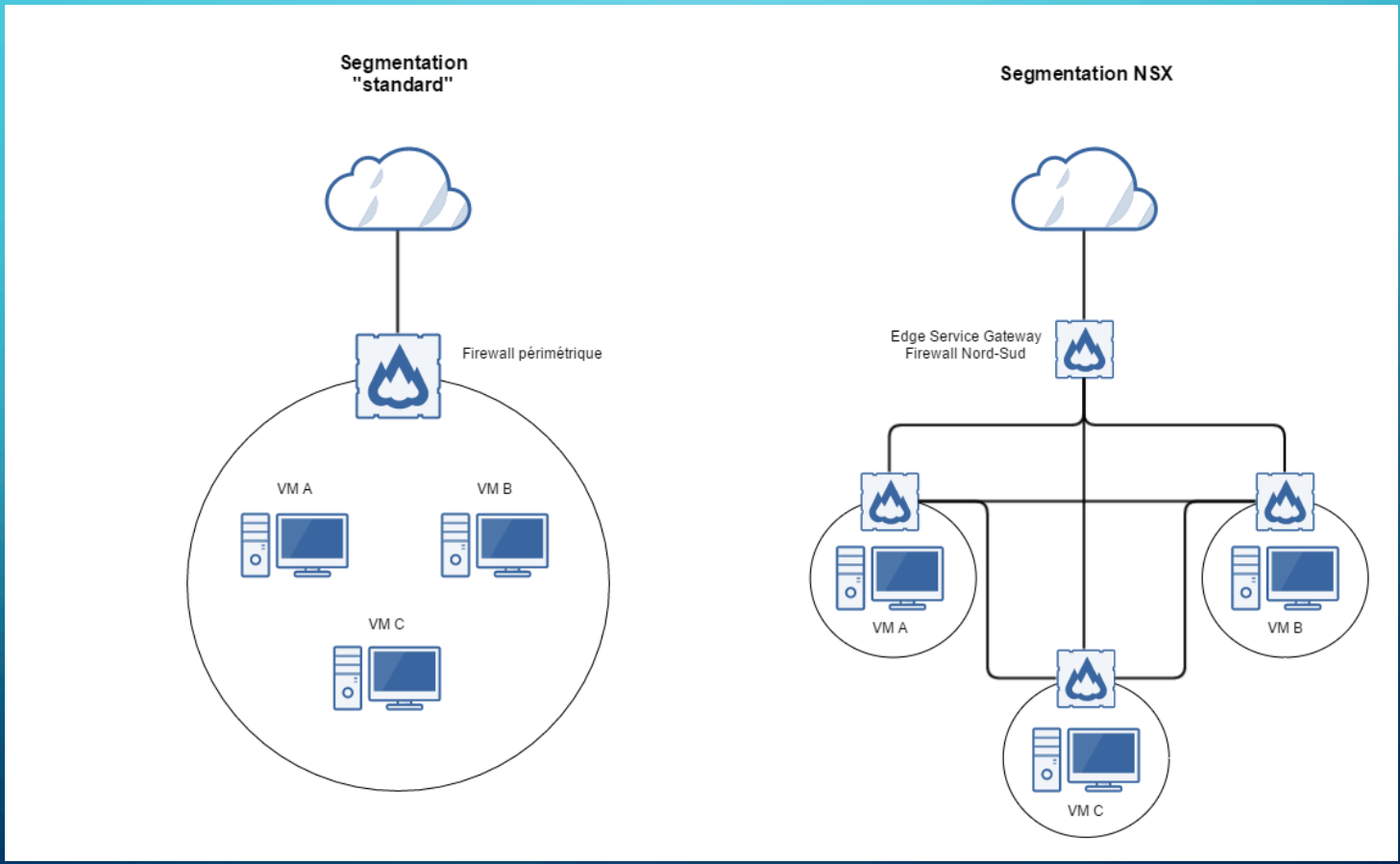
DATA PLANE, CONTROL PLANE, MANAGEMENT PLANE

- Data plane : géré par les hyperviseurs (modules VXLAN, DLR et DFW)
- Control plane : NSX controllers
- Control plane : Logical Control VMs
- Management plane : NSX Manager / NSX API
- Management plane : intégration vSphere
- Deltaplane : Le deltaplane est un appareil volant, adaptant l'aile Rogallo au concept inventé dans les années 1890 par Otto Lilienthal.

MICRO-SEGMENTATION ET FILTRAGE CONTEXTUEL

FILE DANS TA DMZ ET QUE JE T'ENTENDE PLUS !

MICRO-SEGMENTATION



MICRO-SEGMENTATION ET FILTRAGE CONTEXTUEL

- Filtrage EST-OUEST : un firewall derrière chaque VM
- Les hyperviseurs n'apprennent que les règles qui les concernent
- Le firewall connaît les objets vSphere
- Security groups et policies : appliquer les règles à des groupes dynamiques
- Intégration des outils tiers

EDGE SERVICES GATEWAYS : AUX FRONTIÈRES DU RÉEL

LA PORTE OUVERTE À TOUTES LES FENÊTRES

EDGE SERVICES GATEWAYS : AUX FRONTIÈRES DU RÉEL

- Routeurs périmétriques évolués
- Lien entre réseau virtualisé et réseau physique
- Filtrage NORD - SUD
- VPN SSL / IPsec / L2
- Load-balancing
- Routage dynamique IS-IS, OSPF, BGP
- NAT, DHCP, haute-disponibilité

CE QUI EST BIEN MAIS PAS TOP

PARCE QUE C'EST PAS NON PLUS LA FÊTE À NEUNEU

CE QUI EST BIEN MAIS PAS TOP

- Le modèle économique
- Le client vSphere
- La gestion des règles de filtrage
- L'acronyme que personne ne comprend