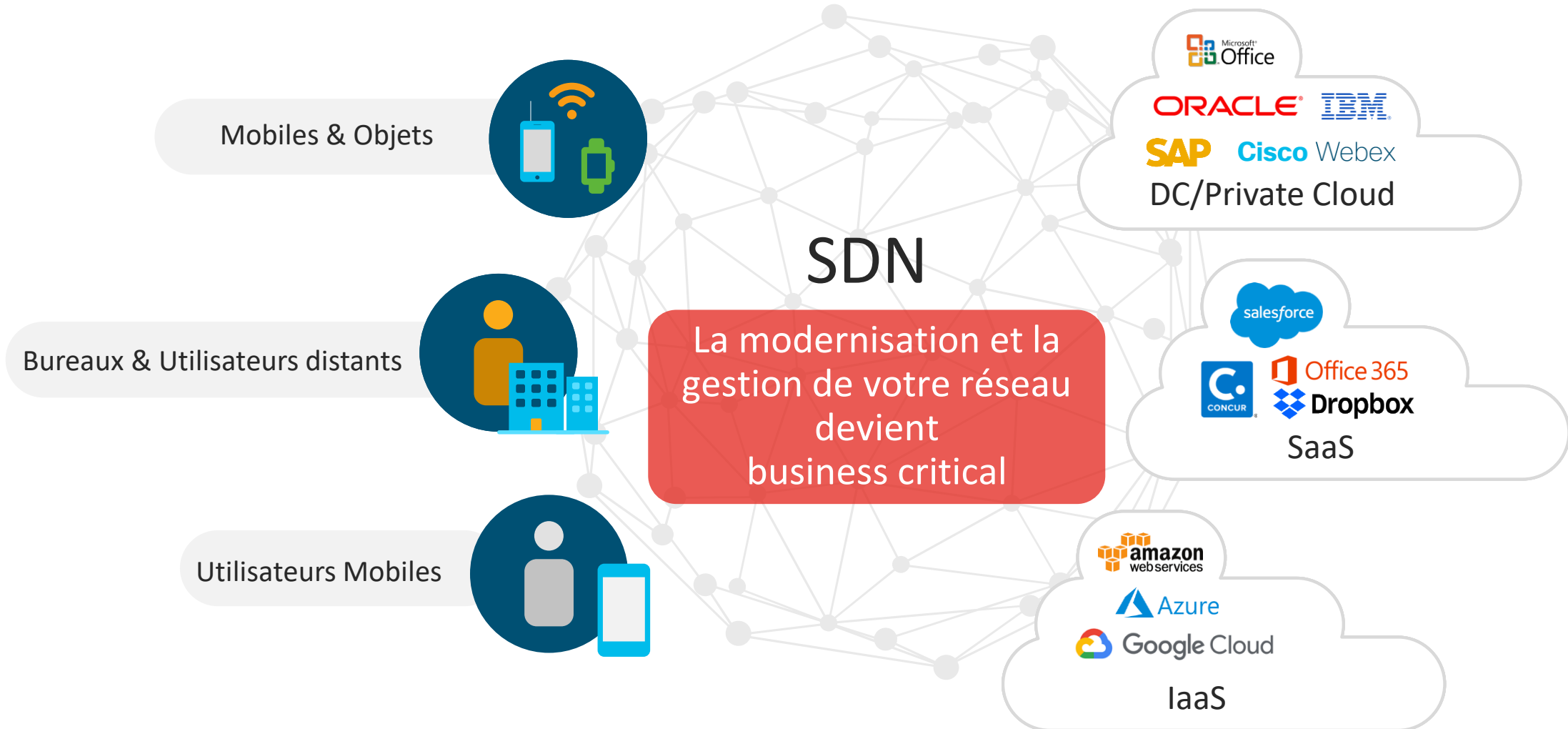


A hand is shown reaching out from the left side of the frame. In the background, there is a soft-focus image of a white cloud against a blue sky. Overlaid on the scene is a network diagram consisting of several blue dots connected by thin lines, representing a network topology. The background transitions from a light blue gradient on the left to a solid blue on the right.

Sécurisez votre réseau Datacenter avec le SDN en intégrant les services L4-L7 Software Defined Network (SDN)



Les applications sont partout.



Plus d'utilisateurs, d'objets et d'applications partout

Simplified Network
Management



Simplified L2/L3
Extension



Security & Visibility



Private Cloud / SDDC



Multi-Tenancy

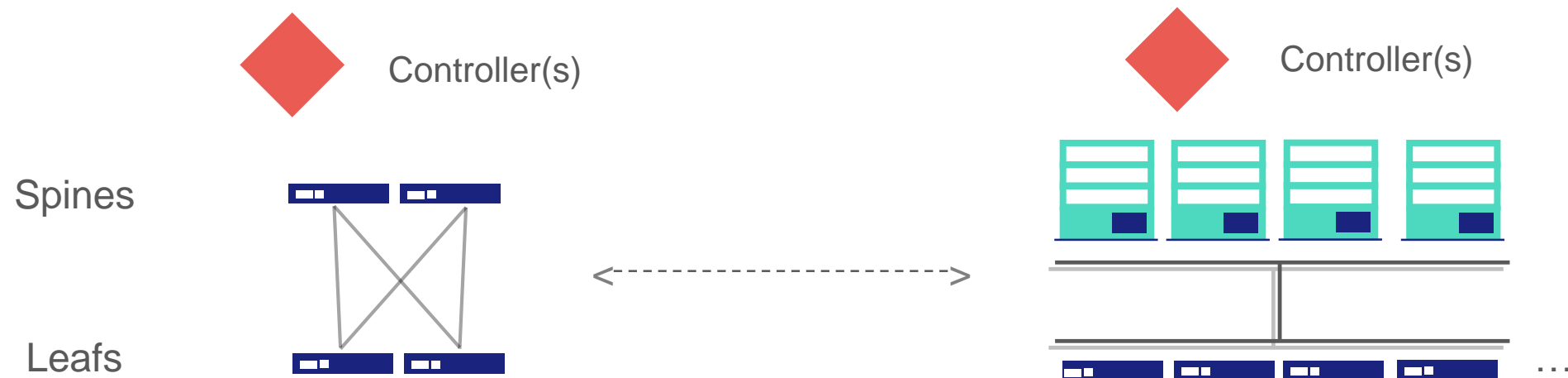


Multiple DCs and
Mobility



SDN - Software Defined Network

**Gérer, configurer et mettre à jour
comme un seul système**
2 à 200 leafs



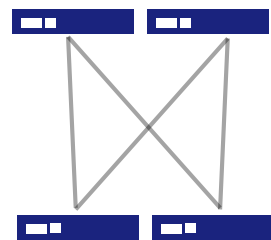
○ SDN - Software Defined Network

Vous pouvez tout intégrer

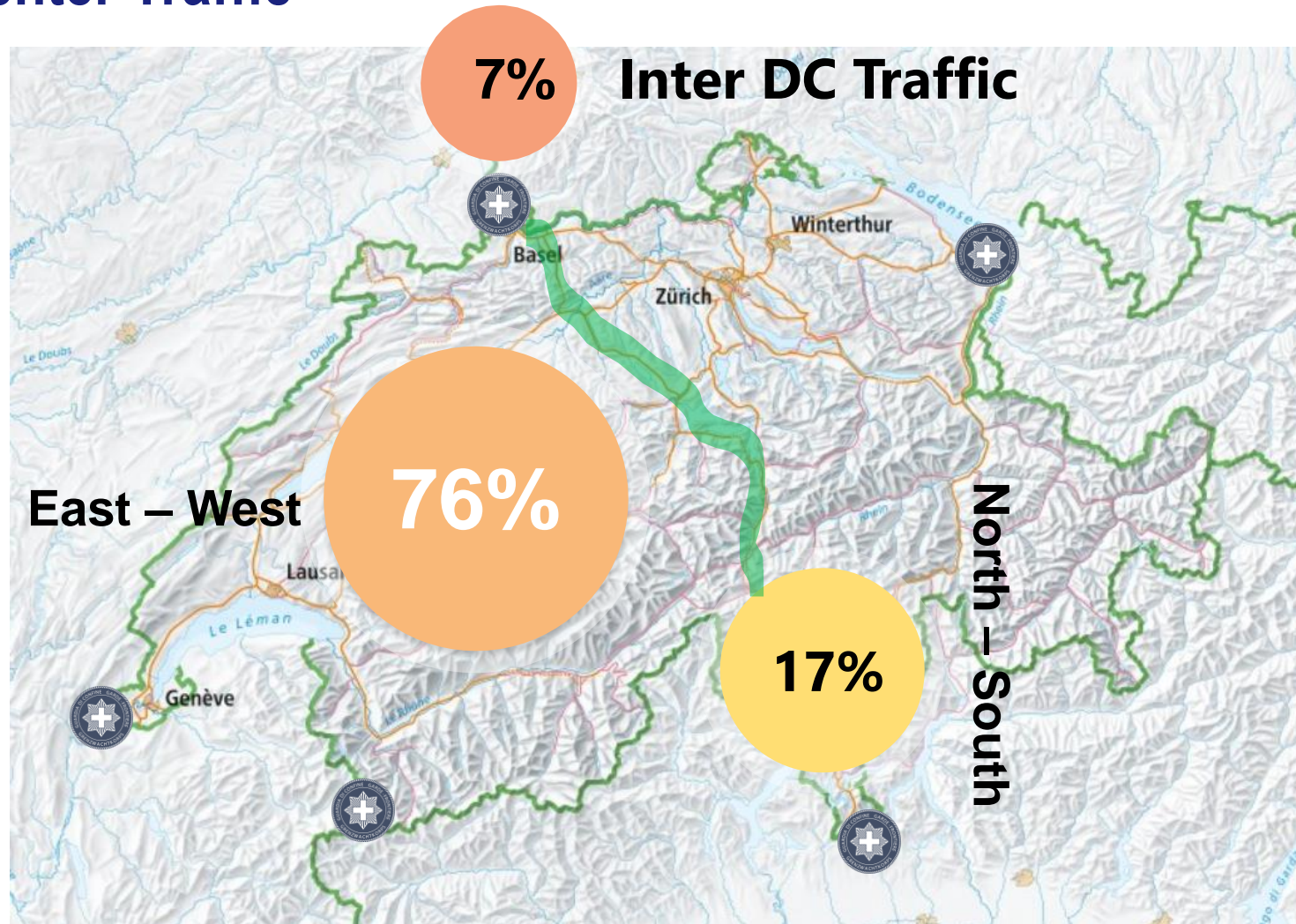


Spines

Leafs



○ Datacenter Traffic

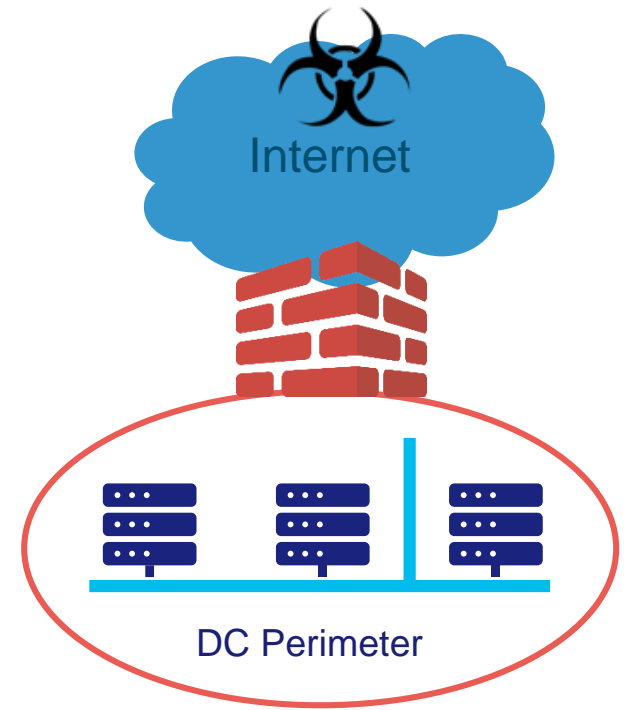


Source: Cisco Global Cloud Index 2012 by destination

Pourquoi segmenter ?



*La sécurité périmétrique n'est pas suffisante.
Dès que la faille est créée, les mouvements latéraux, permettent
aux attaquants de compromettre d'autres équipements*

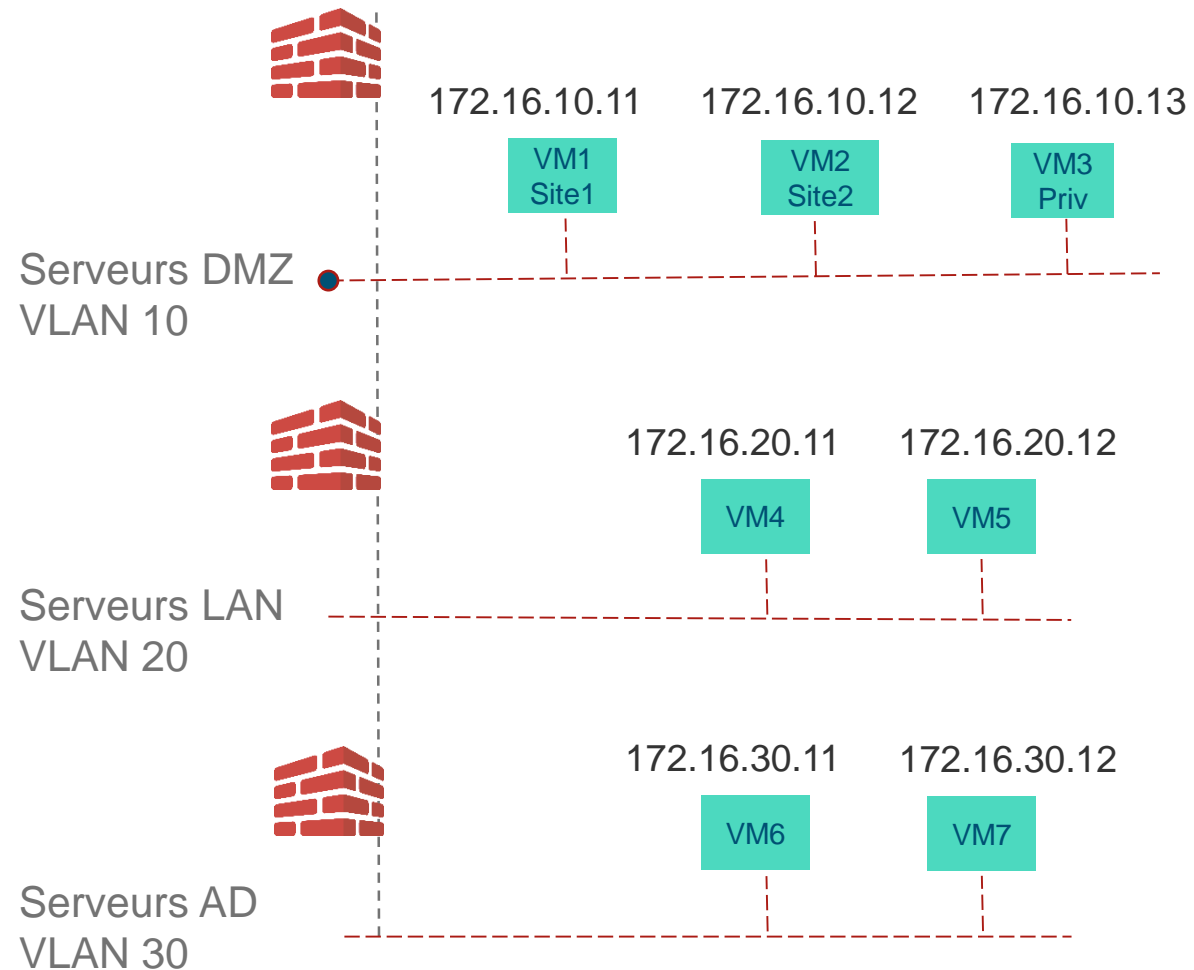


BÉNÉFICES DE LA MICRO-SEGMENTATION

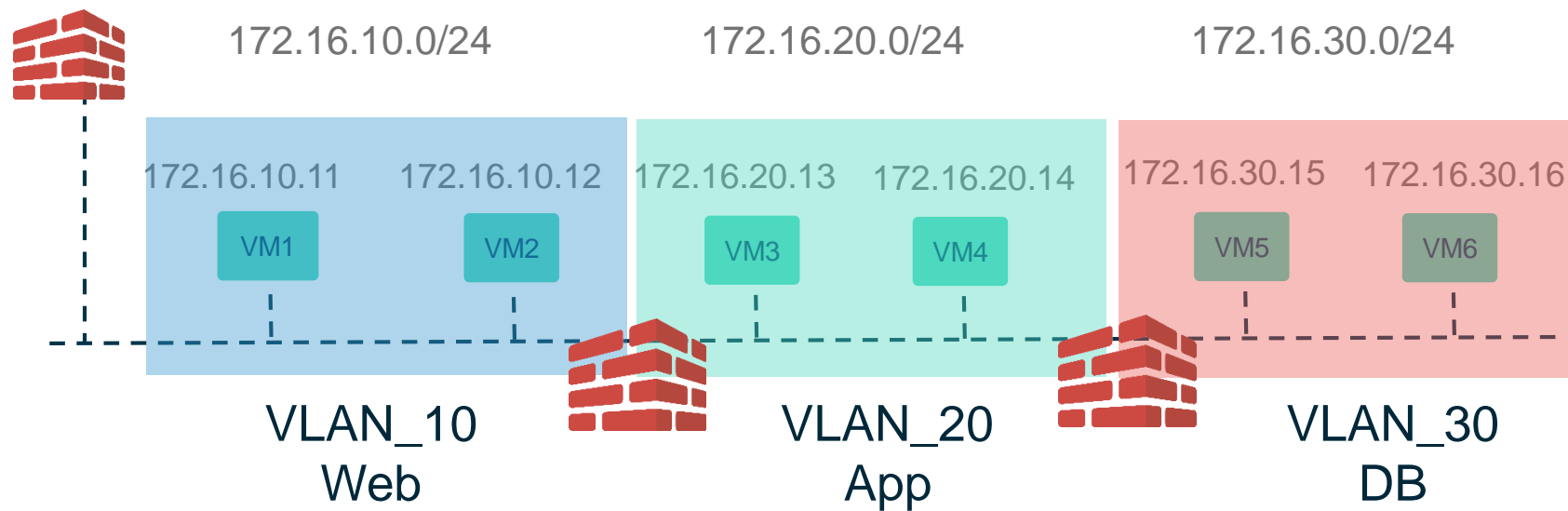
Amélioration de la sécurité au sein du datacenter

Diminution de la taille des segments induisant une réduction de l'exposition aux mouvements latéraux

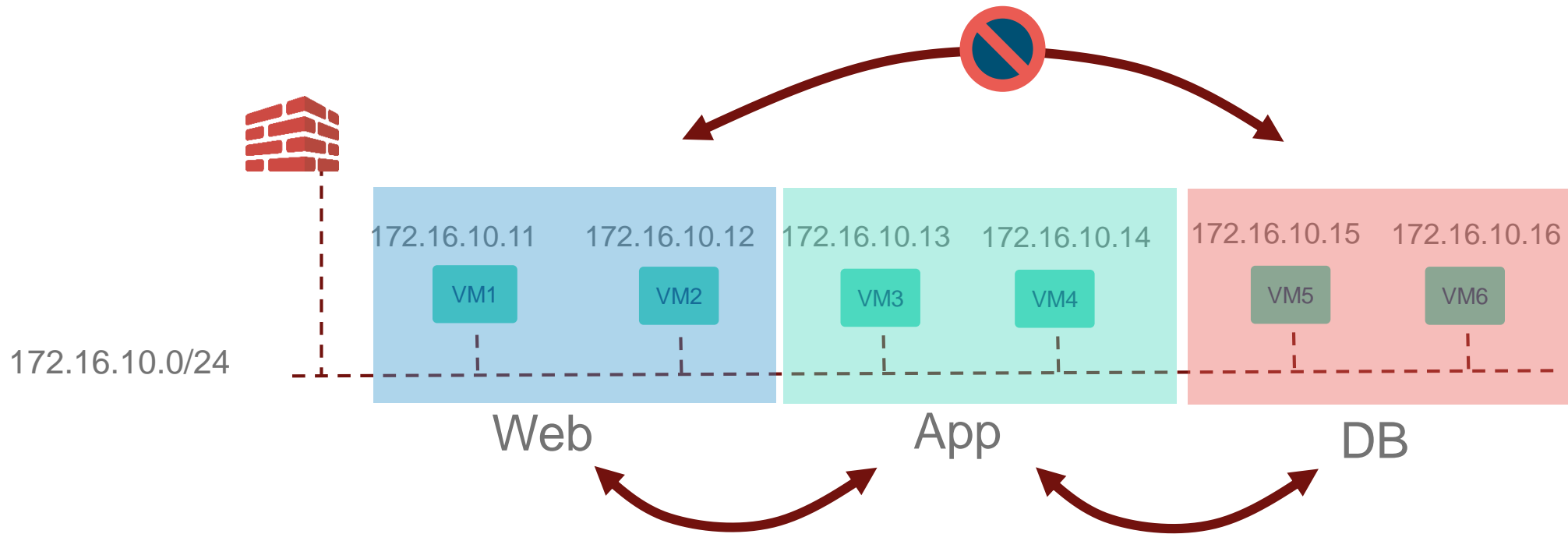
Risque de sécurité : VMs ou Serveurs sur un seule subnet



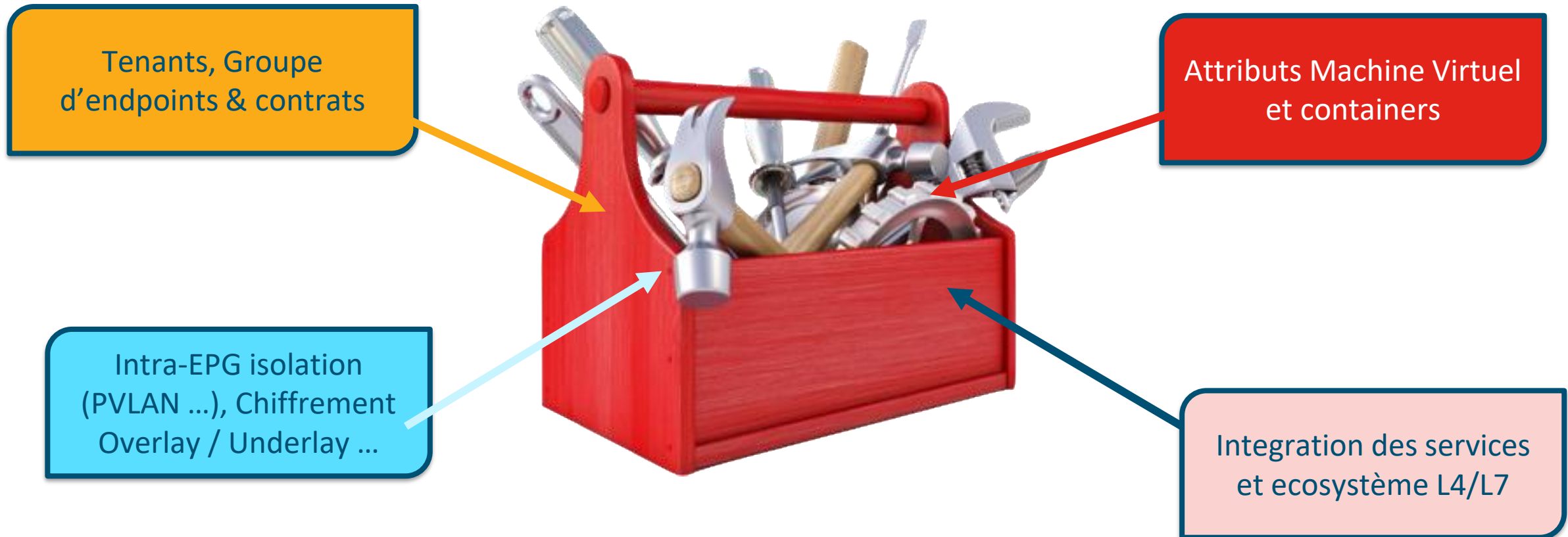
Cas d'usage de segmentation – sans SDN



Cas d'usage de segmentation – avec SDN



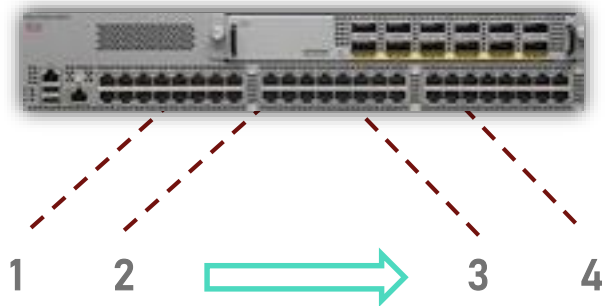
La boîte à outils de la micro-segmentation



SDN Whitelist Policy - “Zero Trust” Model

TRUST BASED ON LOCATION

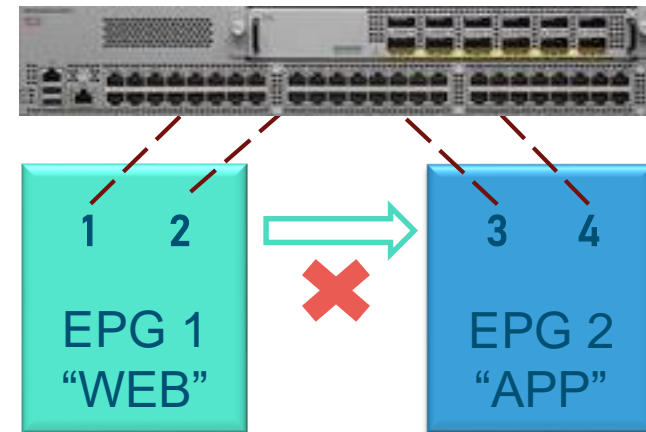
(Traditional DC Switch)



Les serveurs 2 and 3 peuvent communiquer sauf si explicitement **interdit**

ZERO TRUST ARCHITECTURE

(Nexus 9K with ACI)

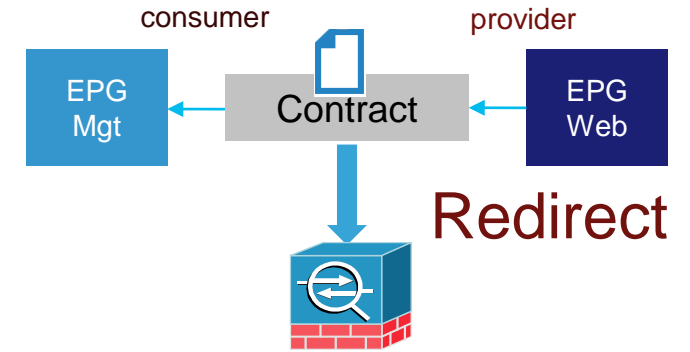


Aucune communication n'est autorisée entre les serveurs 2 and 3 tant qu'une règle ne l'autorise pas :

WHITELIST POLICY

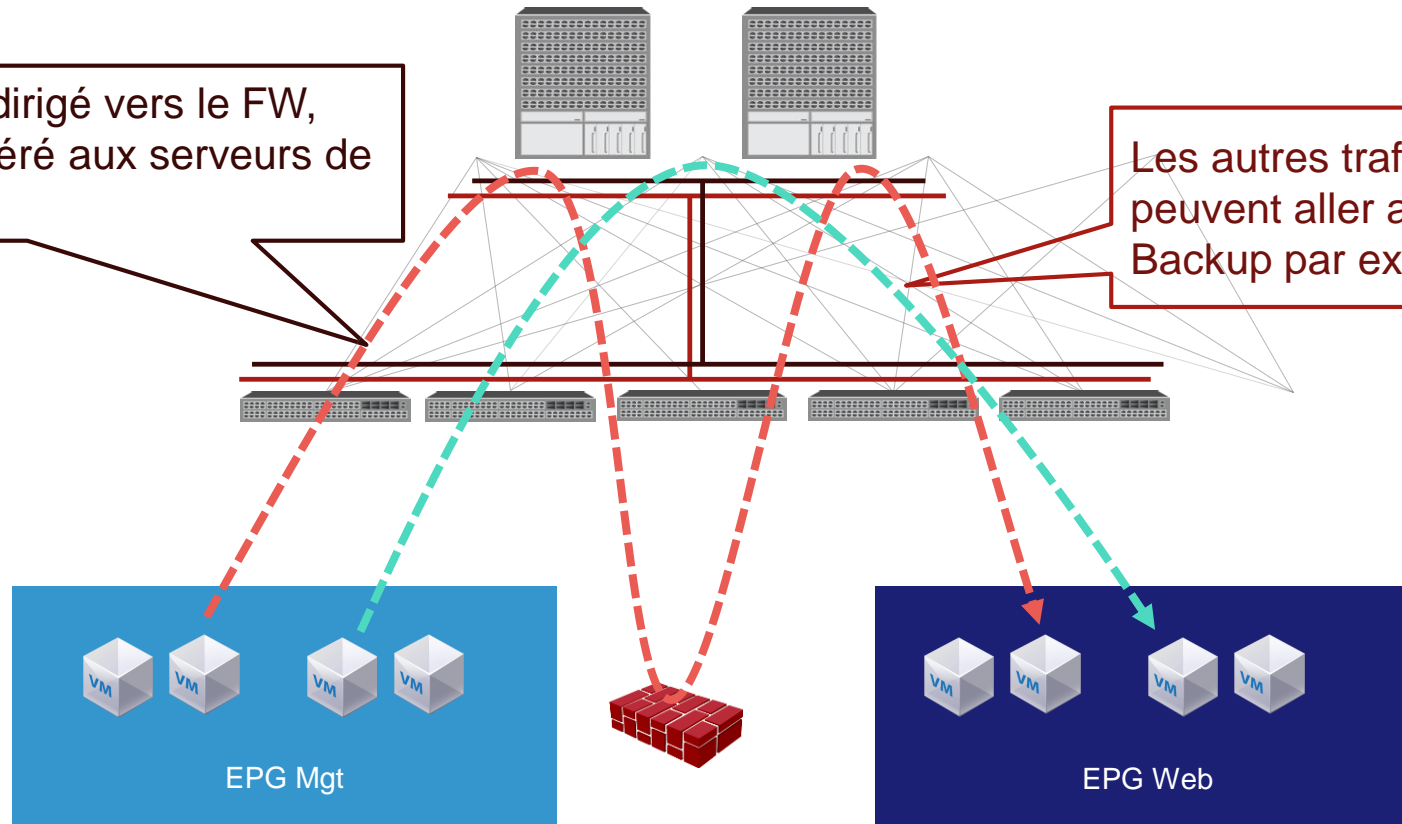
PBR: Cas d'usage

Inspect specific traffic by FW

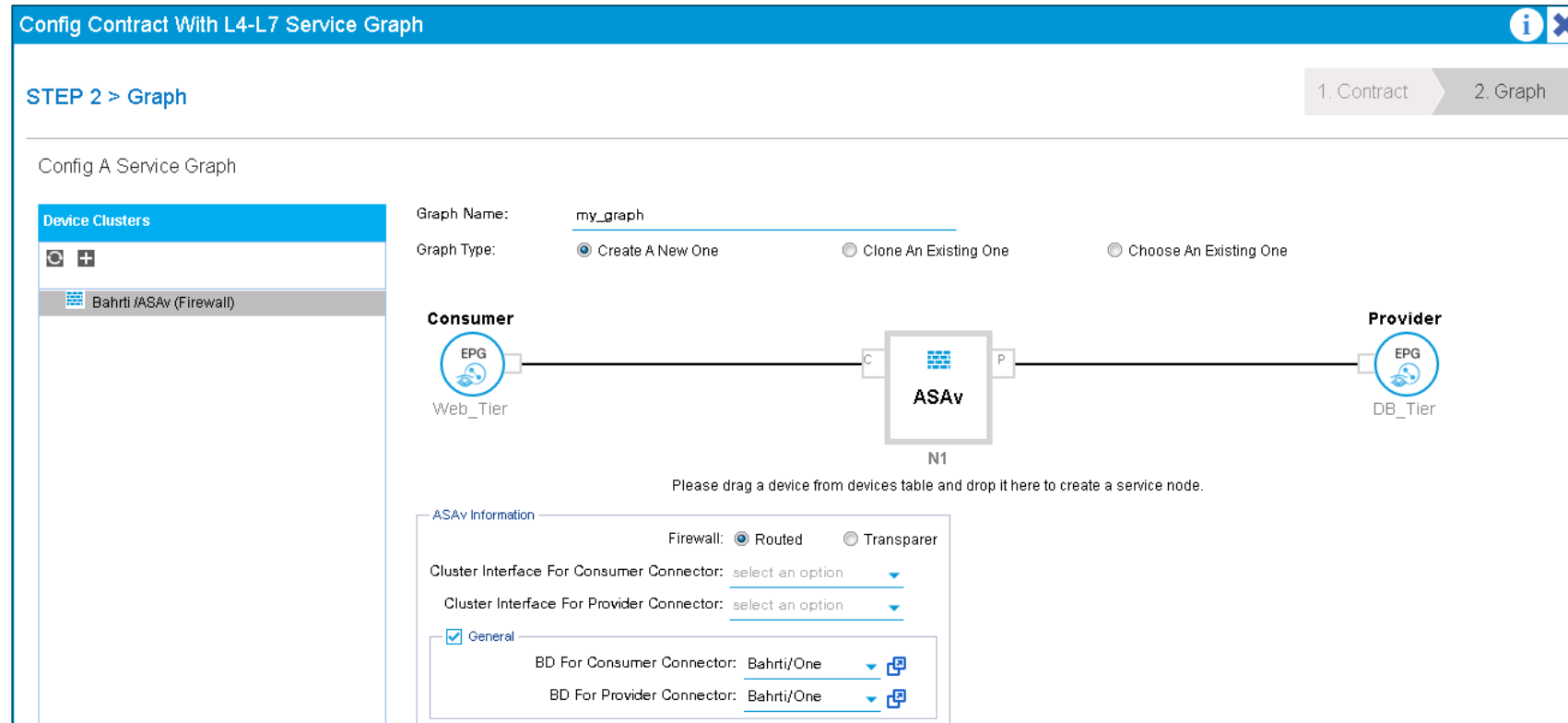


Seul le trafic HTTP est redirigé vers le FW, ensuite le trafic est transféré aux serveurs de mgt. Monitoring par ex.

Les autres trafics permis par contrat peuvent aller au client directement. Backup par ex.



Simplified L4-L7



Managed and unmanaged devices can be combined in a single graph.

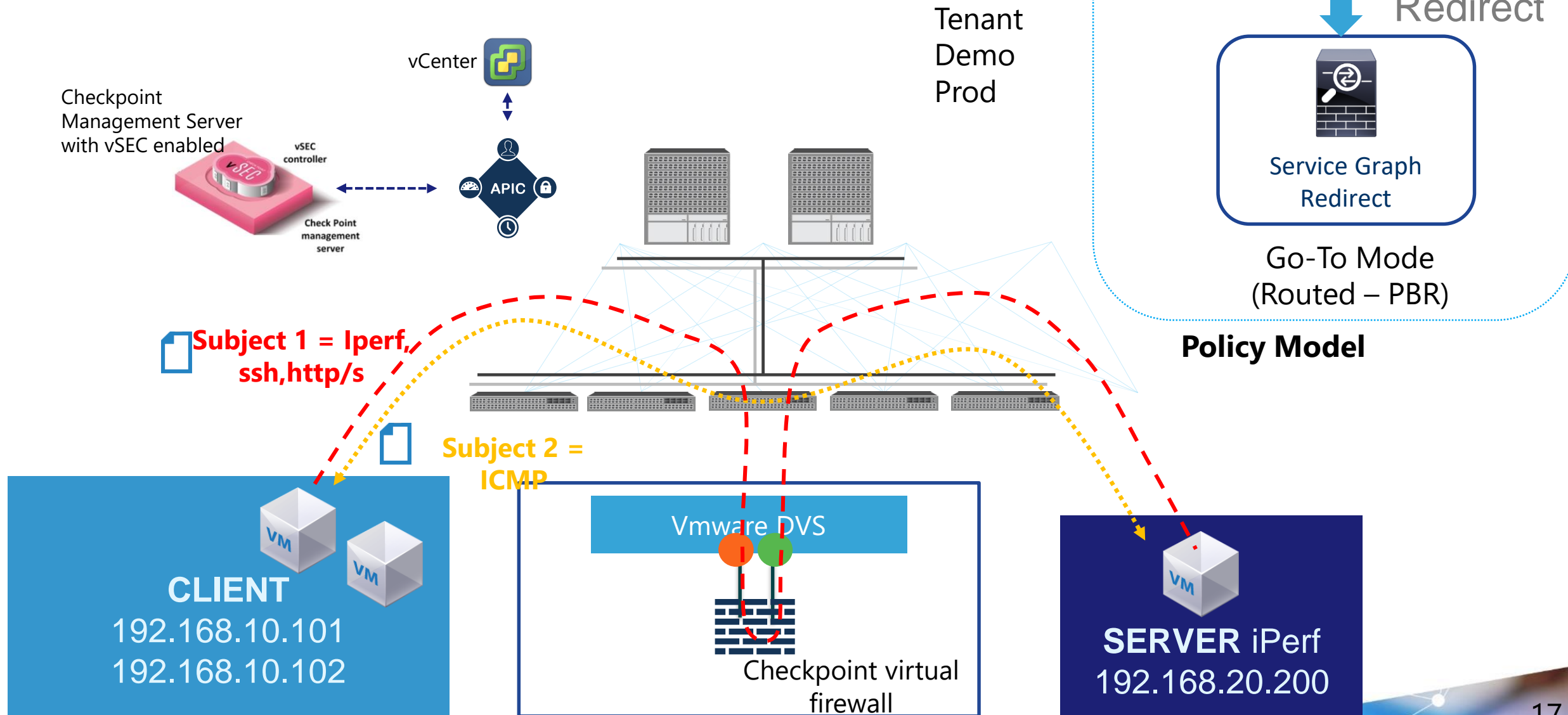


Démo

*Et si on pouvait combiner les avantages
de l'insertion d'un firewall en L2 et L3*

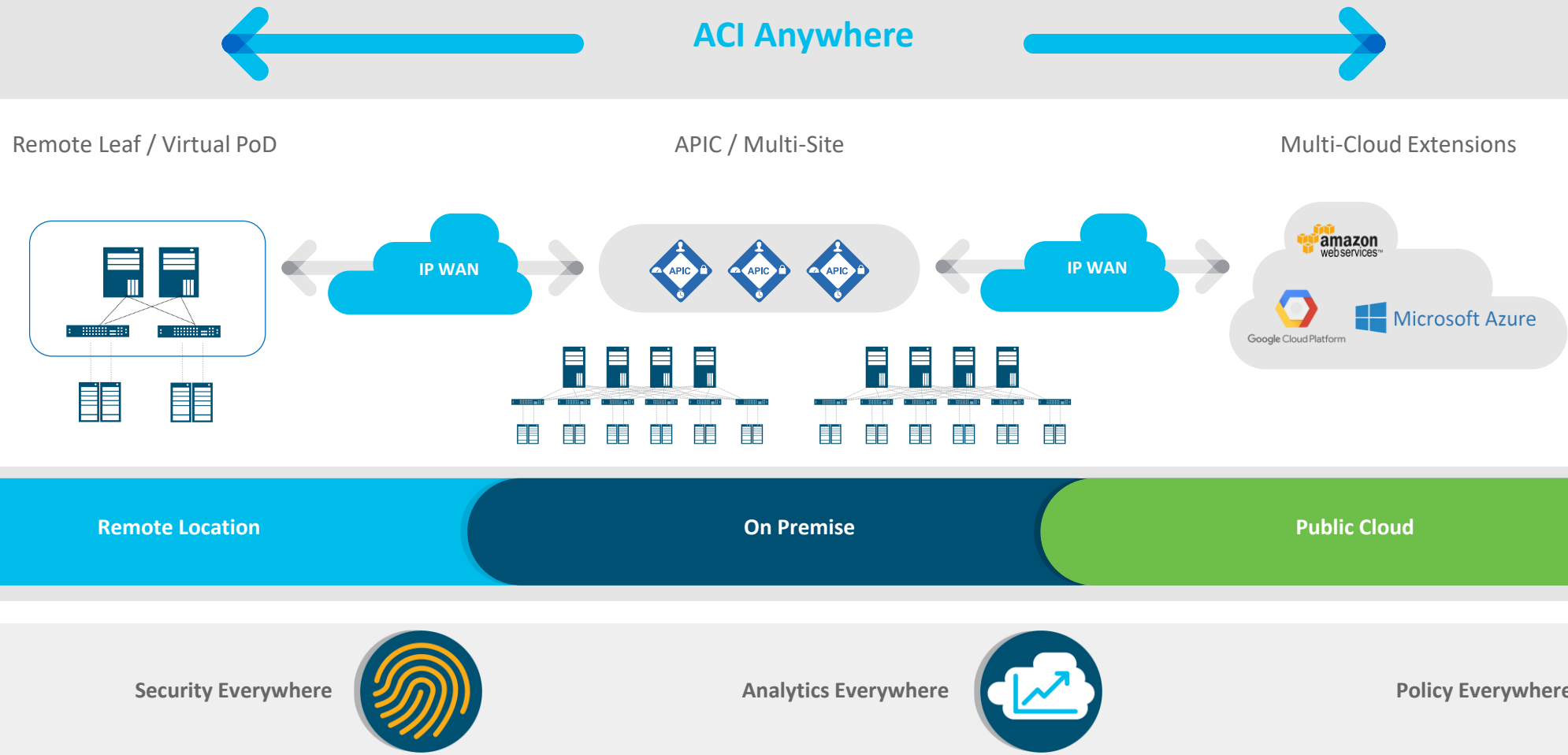
Démo – Intégration Firewall avec PBR

Scénario Inspecter certains flux par le FW



Vision - Cisco ACI Anywhere

Any Workload, Any Location, Any Cloud



Votre configuration doit ressembler à cela ...



Mais elle peut rapidement ressembler à ceci ...



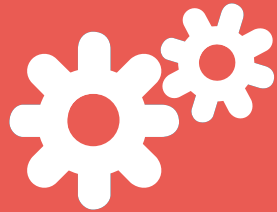
Les clef du succès



Analyse et conseils



Connaissance des applications



Définition des règles



Plannification

Webconférence

Réseaux datacenter : comment relever les challenges du futur ?



groupe-t2i.com/9avril

Infos et inscriptions





Merci !

Contact :

Yves Rey-Bellet

yves.rey-bellet@groupe-t2i.com

Charley Eveno

ceveno@cisco.com

