OFFRE
DMZINCLOUD & SECURITY GROUP

GTS/RCR/AST

INTRODUCTION

- **Les offres DMZinCloud et Security Group sont des services de type Software Defined Network) disponible sur le Cloud interne GTS.**

- **Ces offres apportent des capacités de cloisonnement réseau pour des ressources Cloud sans aucune action sur les équipements réseaux physique.**

- **DMZinCloud est basé sur l'offre Fortinet (// VPC chez AWS)**

- **Les Security Group sont basés sur l'offre NSX (// SG chez AWS)**

SECURITY GROUP

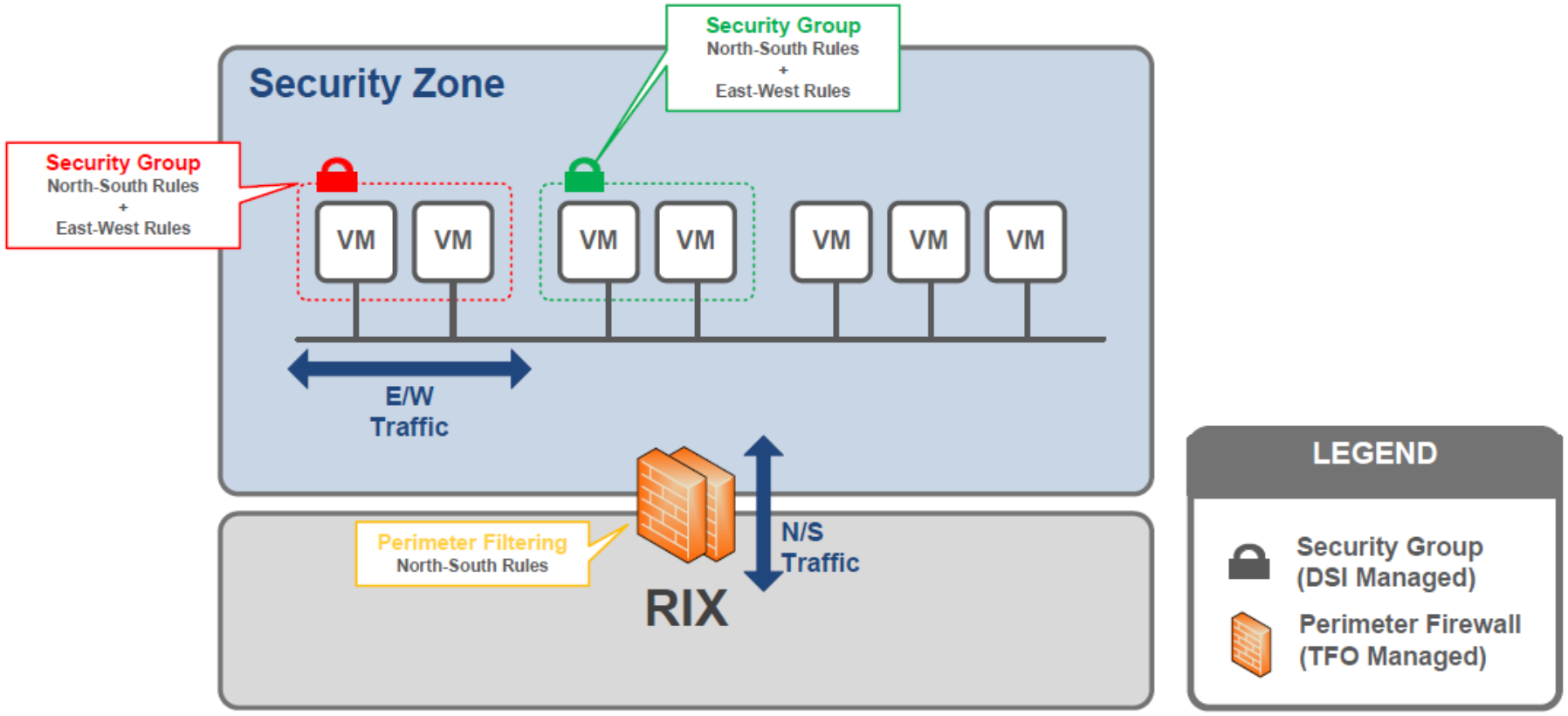
- **Les Security Group sont des objets NSX faisant office de firewall virtuels. Ils permettent donc de contrôler l'ensemble des flux entrants et sortant d'une VM du Cloud Interne (N➔S et E➔ O)**

- **Ils peuvent être déployés sur la plupart des CSR internes (L1-P, L1-H, DCITS, zones CDN..,) ainsi que sur les zones exposées (vWebCell).**

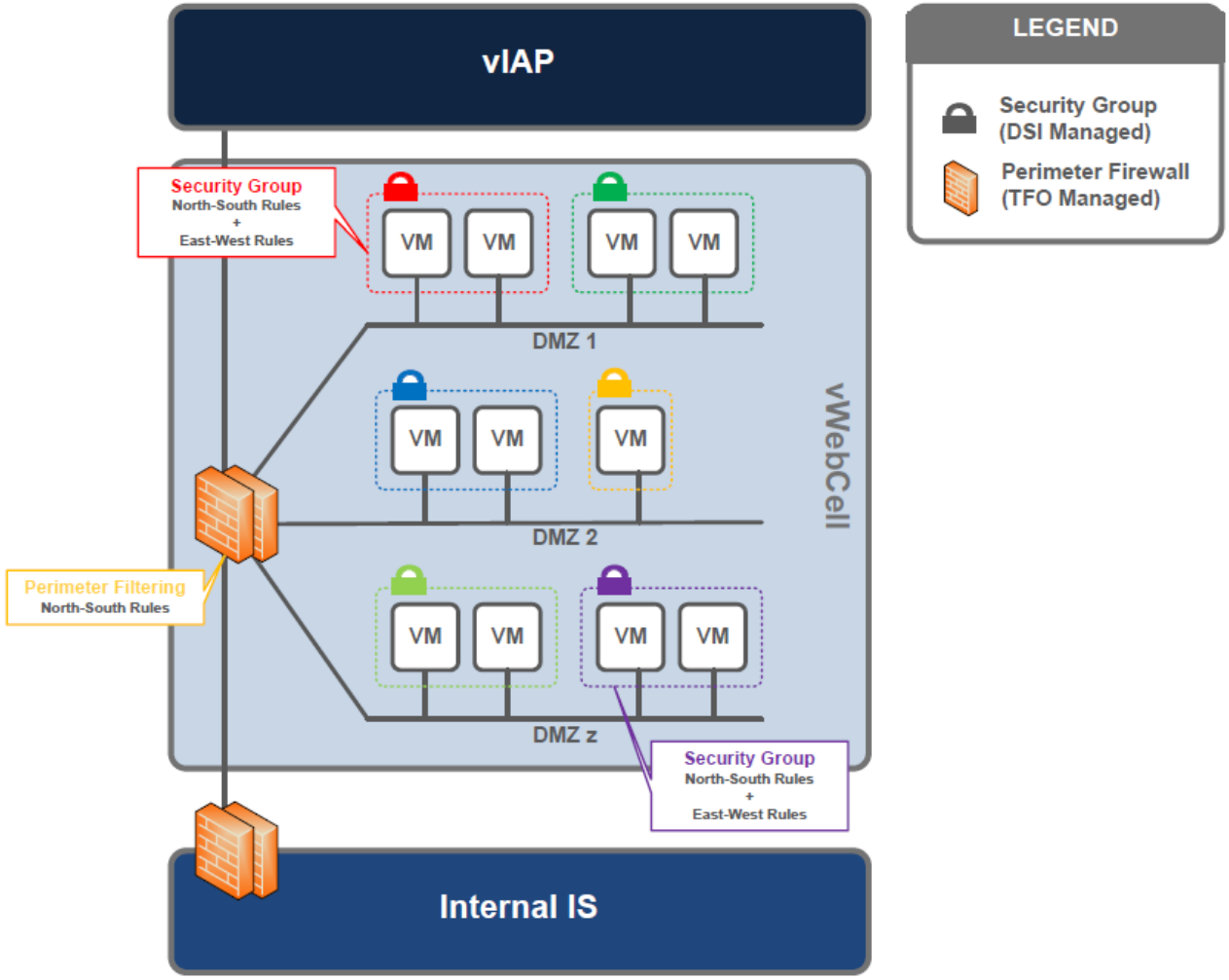
- **Les Security Group représentent une couche de firewall supplémentaire à celles déjà existante au travers des firewall physique.**

- **L'implémentation des Security Group et de leurs règles associées est entièrement à la charge des DSI.**

SECURITY GROUP | CSR INTERNES



SECURITY GROUP | VWEBCELL



SECURITY GROUP | PRINCIPES GLOBAUX

- **Un ou plusieurs Security Group peuvent être associés à une instance.**
- **Les Security Group ne s'appliquent pas à des VM répliquées, ils sont donc locaux à une AZ.**
- **A la création d'un Security Group, les règles par défaut sont: « Deny all » pour le traffic entrant et « Allows all » pour le traffic sortant.**
- **Une règle any-any sur l'IP du créateur de la DMZ est mise en place à la création.**
- **Les principes de filtrage positionnées par la suite sont basées sur des White List.**
- **Par défaut, un maximum de 5 Security Group est autorisé par trigramme et par environnement.**
- **Un maximum de 25 règles en entrée et 25 règles en sortie est permis sur un Security Group donnée.**

<u>Nomenclature</u>:

Security Group interne: LSG_XXX_YYY_ZZZZZ_AZ

Security Group exposé: LSGWCE_XXX_YYY_ZZZZZ_AZ

XXX = environnement | YYY=Trigramme | ZZZZZ = nombre entre 00001 et 99999 | AZ = site

SECURITY GROUP | MANAGEMENT D' ACCES

- **Deux Annuaires ont été mis en place pour la gestion des ressources Cloud:**
  - **Cloud AD Group ➔ Déclare les utilisateurs pouvant consommer les ressources Cloud habituelles (VM, LB, réplication, etc…)**
  - **Security Group AD group ➔ Déclare les utilisateurs pouvant consommer des Security Group**
- **Le propriétaire d'un Security Group AD group sera définie par les DSI.**

- **Les propriétaires et les membres d'un Security Group AD group pourront effectuer toutes les opération de type CRUD sur les Security Group et leurs règles associées.**

- **Les propriétaires et les membres d'un Cloud AD group, pourront effectuer les opérations ayant un lien avec les Security Group suivantes:**
  - **Lister les Security Group.**
  - **Lister les règles associées.**
  - **Ajouter, supprimer et lister des instances Cloud appartenant à un Security Group.**
  - **Ajouter, supprimer et lister des tags appartenant à un Security Group.**

DMZINCLOUD

- **L'offre de service DMZinCloud permet de provisionner un VLAN dédié au sein du Cloud Interne. (en dehors des CSR habituels). /!\ Pas d'offre sur les vWebCell**

- **L'offre est actuellement disponible via le SGCloud et le portail HP-CSA, et en cible sur DoitNow couplé à l'IAMaaS.**

- **DMZincloud est disponible dans chaque AZ, mais n'est pas applicable au VM répliquées.**

- **L'offre permet de provisionner des subnet de type /26(62 IP) ou /27(30 IP) et est éligible aux projets de classification C0, C1 et C2.**

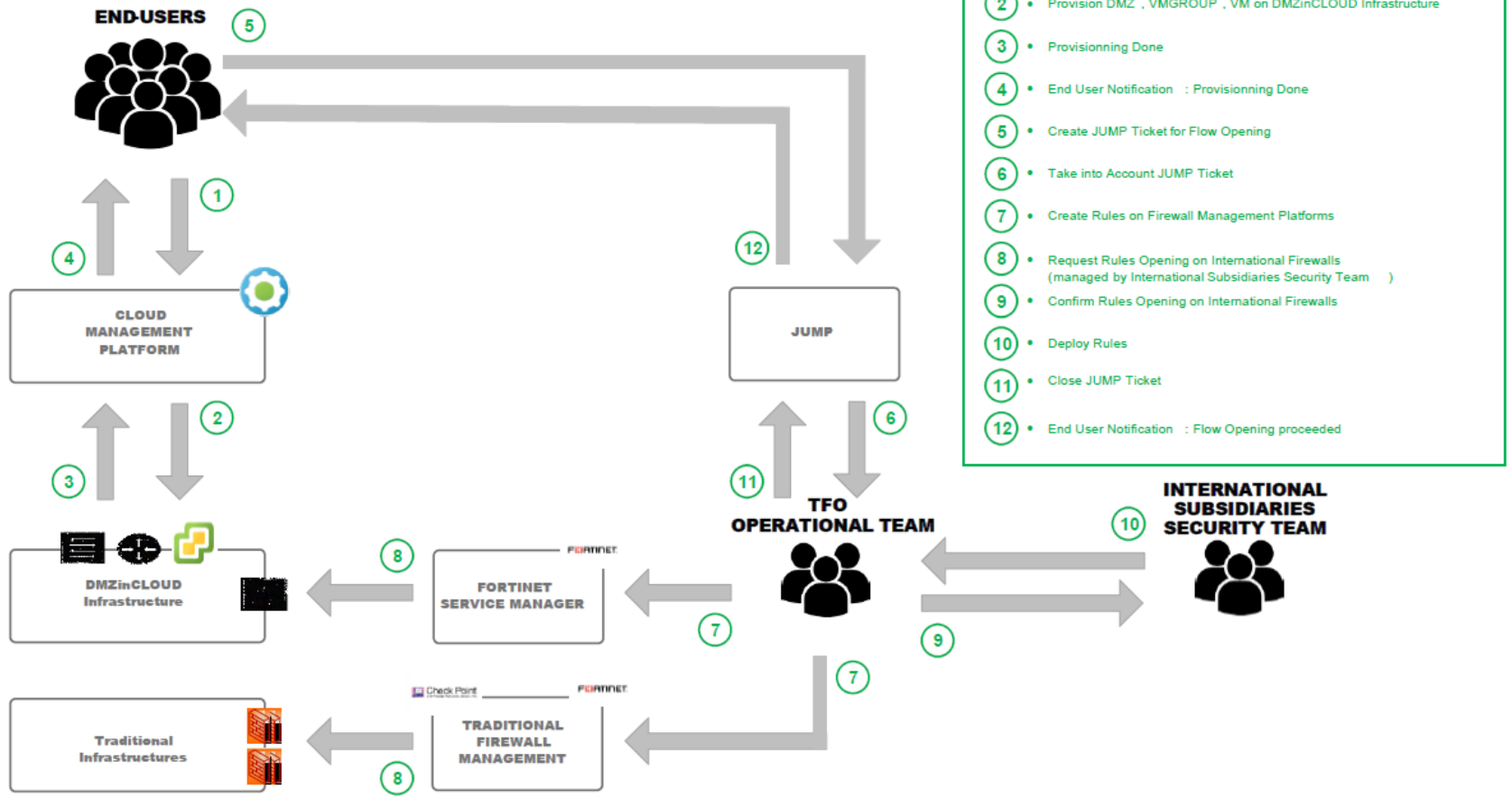
- **Notion de DMZVMGroup:**

  Les DMZVMGROUP sont des tag positionnés sur une VM ou un ensemble de VM de la DMZ.

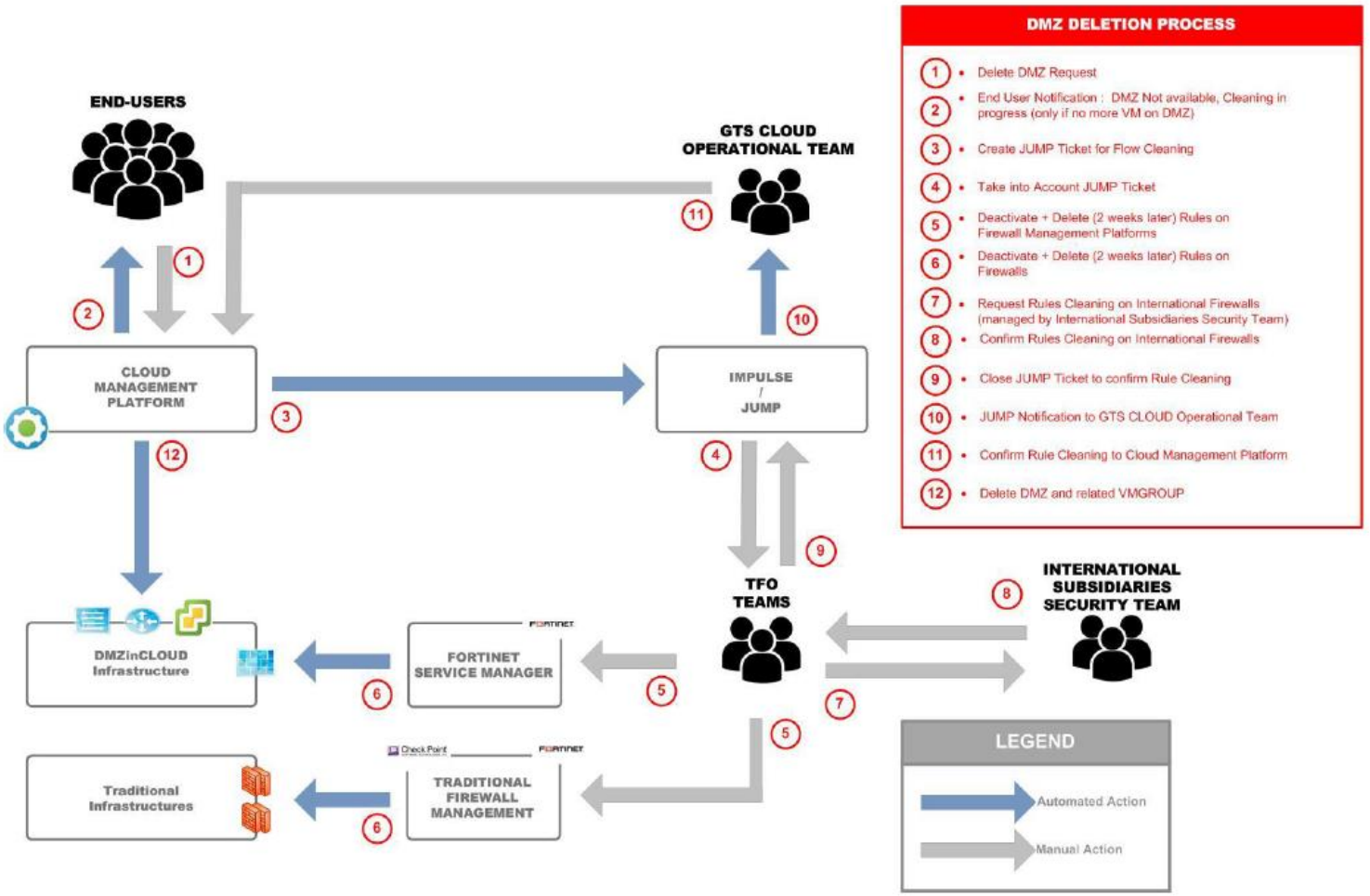
  Des règles de sécurité sont associées au DMZVMCloud. (filtrage N->S E->O)

  Toutes les VM appartenant au même DMZVMGroup hériteront de règles positionnées préalablement.

DMZINCLOUD | CRÉATION

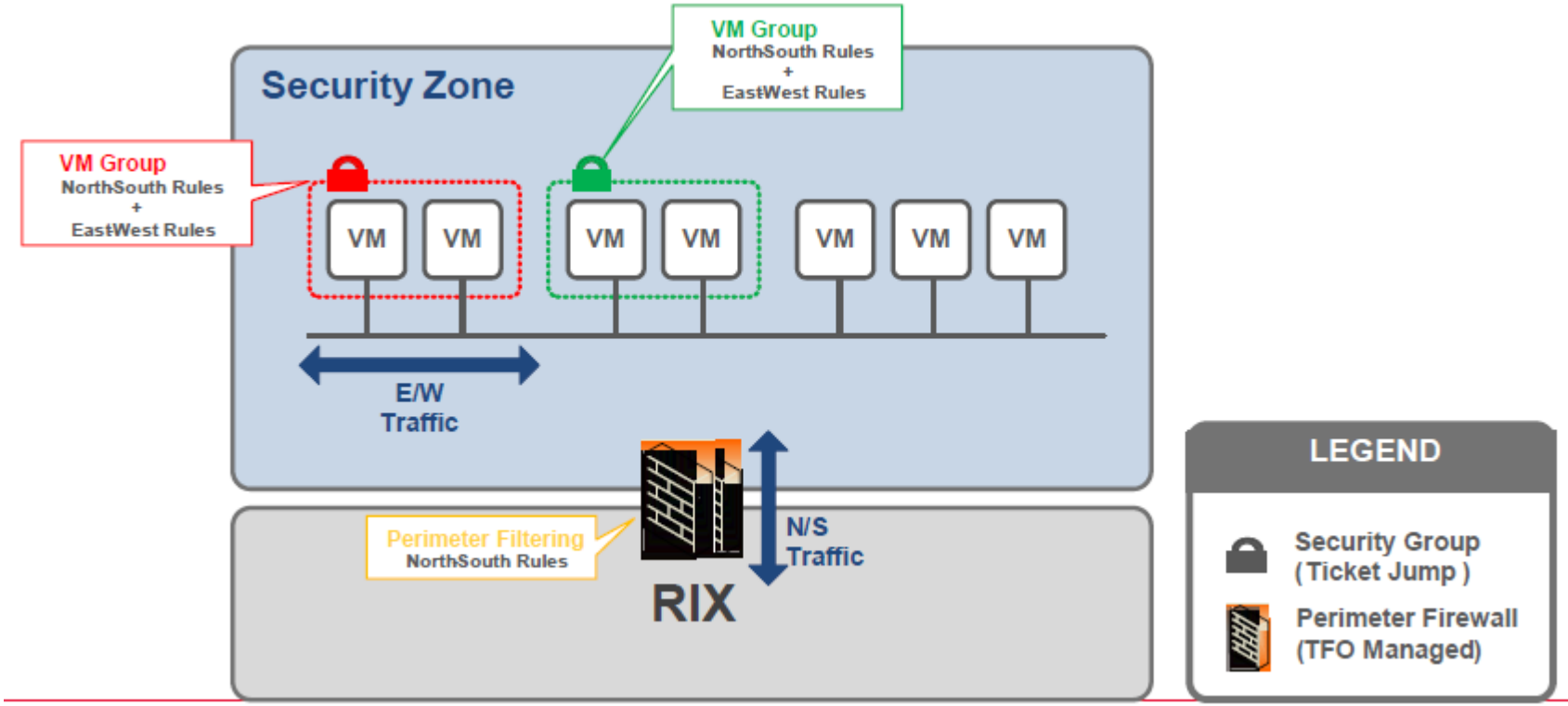


DMZINCLOUD | SUPPRESSION



Click to enter source information or delete this box; please duplicate this box for additional source boxes

DMZINCLOUD | FILTRAGE



DMZINCLOUD | PRINCIPES GENERAUX

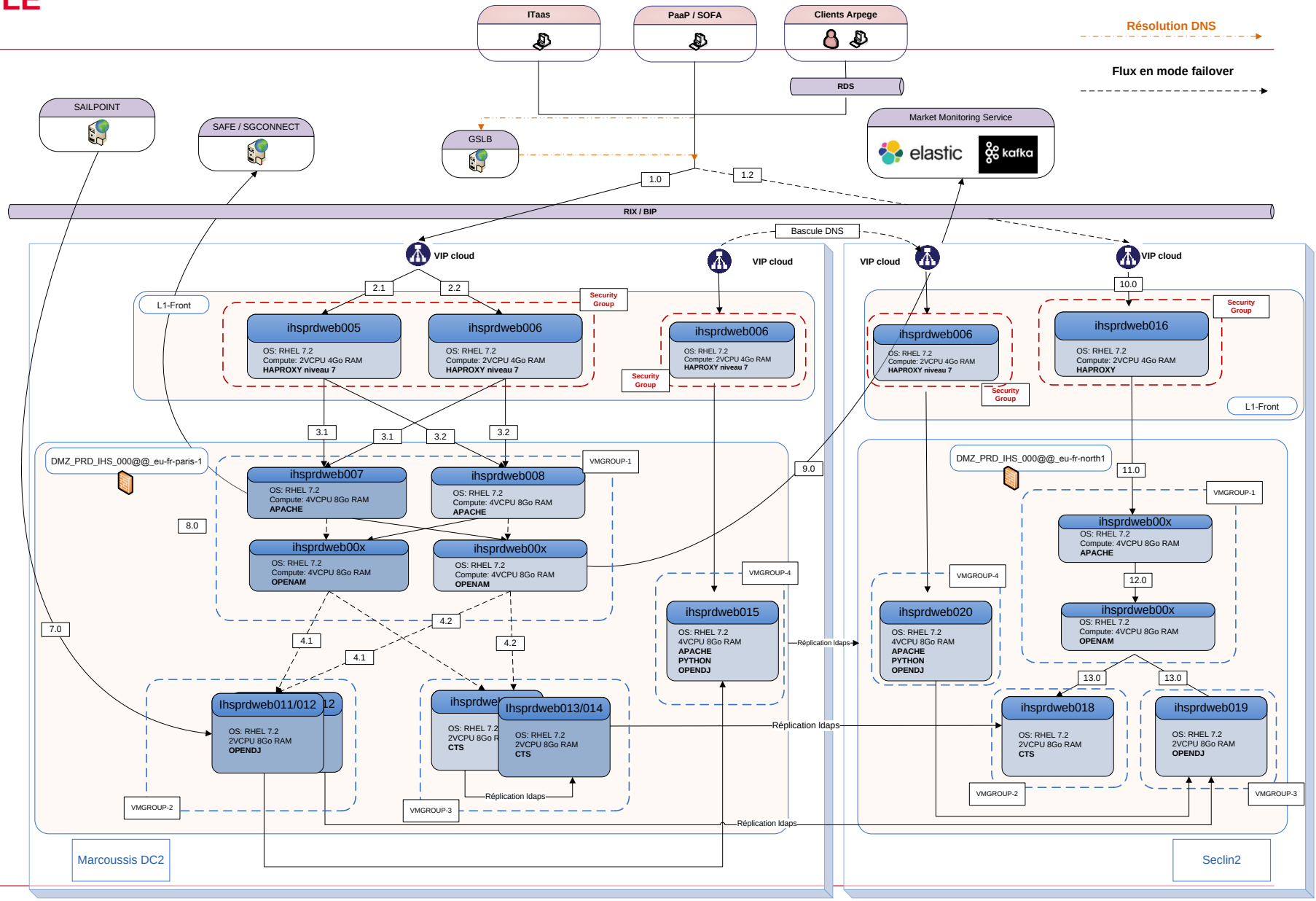
- **Une VM peut-être associée à un ou plusieurs VMGroup au sein d'une même AZ et d'un même environnement.**
- **Un maximum de 5 VMGroup peut être créé par trigramme et par environnement.**
- **Un maximum de 25 règles en entrée et 25 règles en sortie peut être positionné par VMGroup.**
- **La mise en place des DMZinCloud est soumise à des ouvertures de routes.**
- **A ce jour, les subnet DMZinCloud ne disposent pas d'offre de Load Balancing.**
- **Par défaut, les VM au sein d'un même DMZVMGroup ne communiquent pas entre elles.**

EN RESUME

- **Security Group:**
  - **Peuvent être déployés dans les CSR et les vWebCell**
  - **Peuvent s' appliquer à une ou plusieurs VM**
  - **L'Implémentation est entièrement à la main de la ME**

- **DMZinCloud:**
  - **Réseau dédié**
  - **Mise en place nécessitant une collaboration avec HCS (ouverture de route)**
  - **Pas de service de LB à ce jour vers, ni au sein de la DMZ**

EXEMPLE


ITaas
PaaP / SOFA
Clients Arpege
Résolution DNS
Flux en mode failover
RDS
SAILPOINT
SAFE / SGCONNECT
GSLB
Market Monitoring Service
elastic
kafka
1.0
1.2
RIX / BIP
Bascule DNS
VIP cloud
VIP cloud
VIP cloud
VIP cloud
2.1
2.2
10.0
L1-Front
Security Group
ihsprdweb005
OS: RHEL 7.2
Compute: 2VCPU 4Go RAM
HAPROXY niveau 7
ihsprdweb006
OS: RHEL 7.2
Compute: 2VCPU 4Go RAM
HAPROXY niveau 7
ihsprdweb006
OS: RHEL 7.2
Compute: 2VCPU 4Go RAM
HAPROXY niveau 7
ihsprdweb016
OS: RHEL 7.2
Compute: 2VCPU 4Go RAM
HAPROXY
3.1
3.1
3.2
3.2
DMZ_PRD_IHS_000@@_eu-fr-paris-1
VMGROUP-1
ihsprdweb007
OS: RHEL 7.2
Compute: 4VCPU 8Go RAM
APACHE
ihsprdweb008
OS: RHEL 7.2
Compute: 4VCPU 8Go RAM
APACHE
8.0
ihsprdweb00x
OS: RHEL 7.2
Compute: 4VCPU 8Go RAM
OPENAM
ihsprdweb00x
OS: RHEL 7.2
Compute: 4VCPU 8Go RAM
OPENAM
9.0
VMGROUP-4
ihsprdweb015
OS: RHEL 7.2
4VCPU 8Go RAM
APACHE
PYTHON
OPENDJ
Réplication ldaps
7.0
4.2
4.1
4.1
4.2
lhsprdweb011/012
OS: RHEL 7.2
2VCPU 8Go RAM
OPENDJ
lhsprdweb013/014
OS: RHEL 7.2
2VCPU 8Go RAM
CTS
Réplication ldaps
Réplication ldaps
VMGROUP-2
VMGROUP-3
Réplication ldaps
Marcoussis DC2
DMZ_PRD_IHS_000@@_eu-fr-north1
11.0
VMGROUP-1
ihsprdweb00x
OS: RHEL 7.2
Compute: 4VCPU 8Go RAM
APACHE
12.0
ihsprdweb00x
OS: RHEL 7.2
Compute: 4VCPU 8Go RAM
OPENAM
VMGROUP-4
ihsprdweb020
OS: RHEL 7.2
4VCPU 8Go RAM
APACHE
PYTHON
OPENDJ
13.0
13.0
ihsprdweb018
OS: RHEL 7.2
2VCPU 8Go RAM
CTS
ihsprdweb019
OS: RHEL 7.2
2VCPU 8Go RAM
OPENDJ
VMGROUP-2
VMGROUP-3
Seclin2