RESG/GTS/RET/APS

Security Group

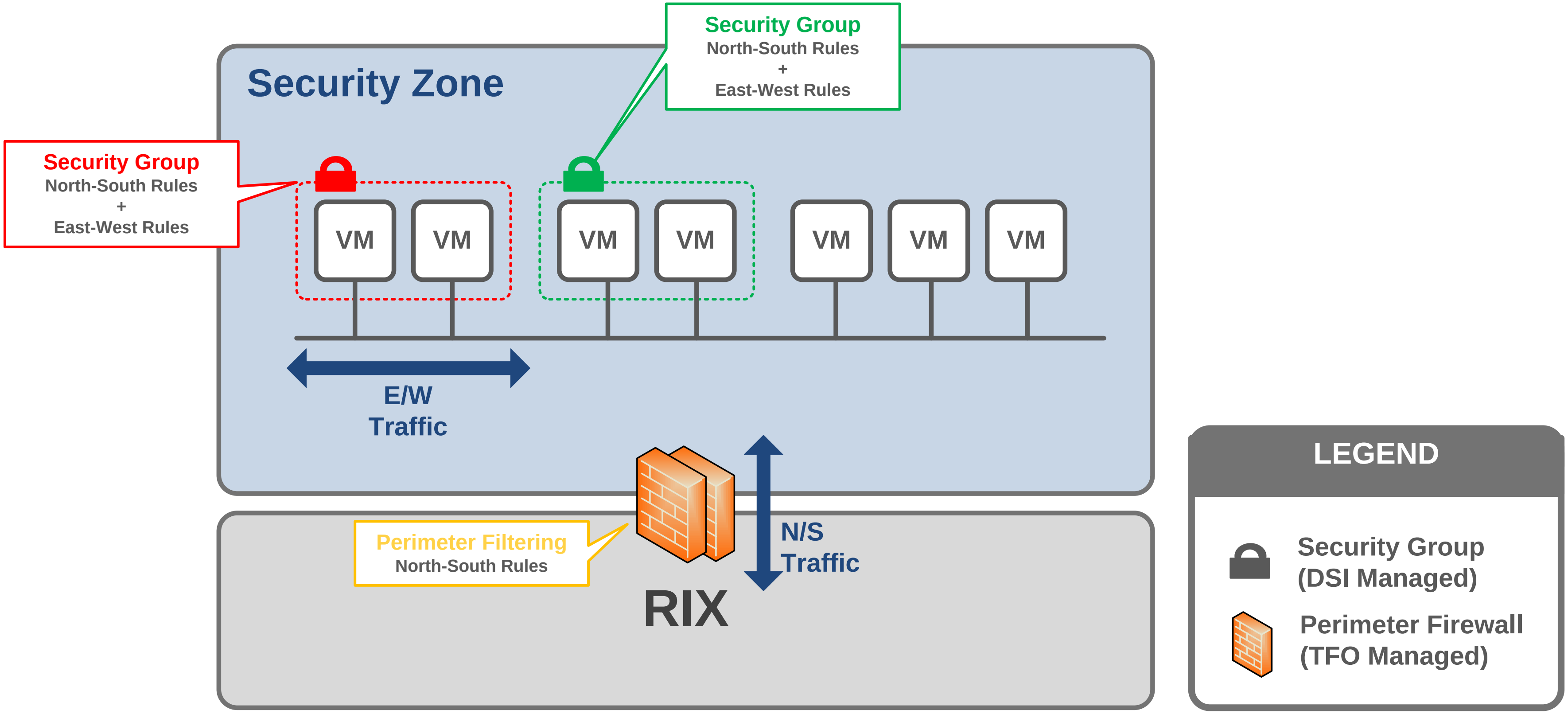
GTS Private Cloud

25/10/2017

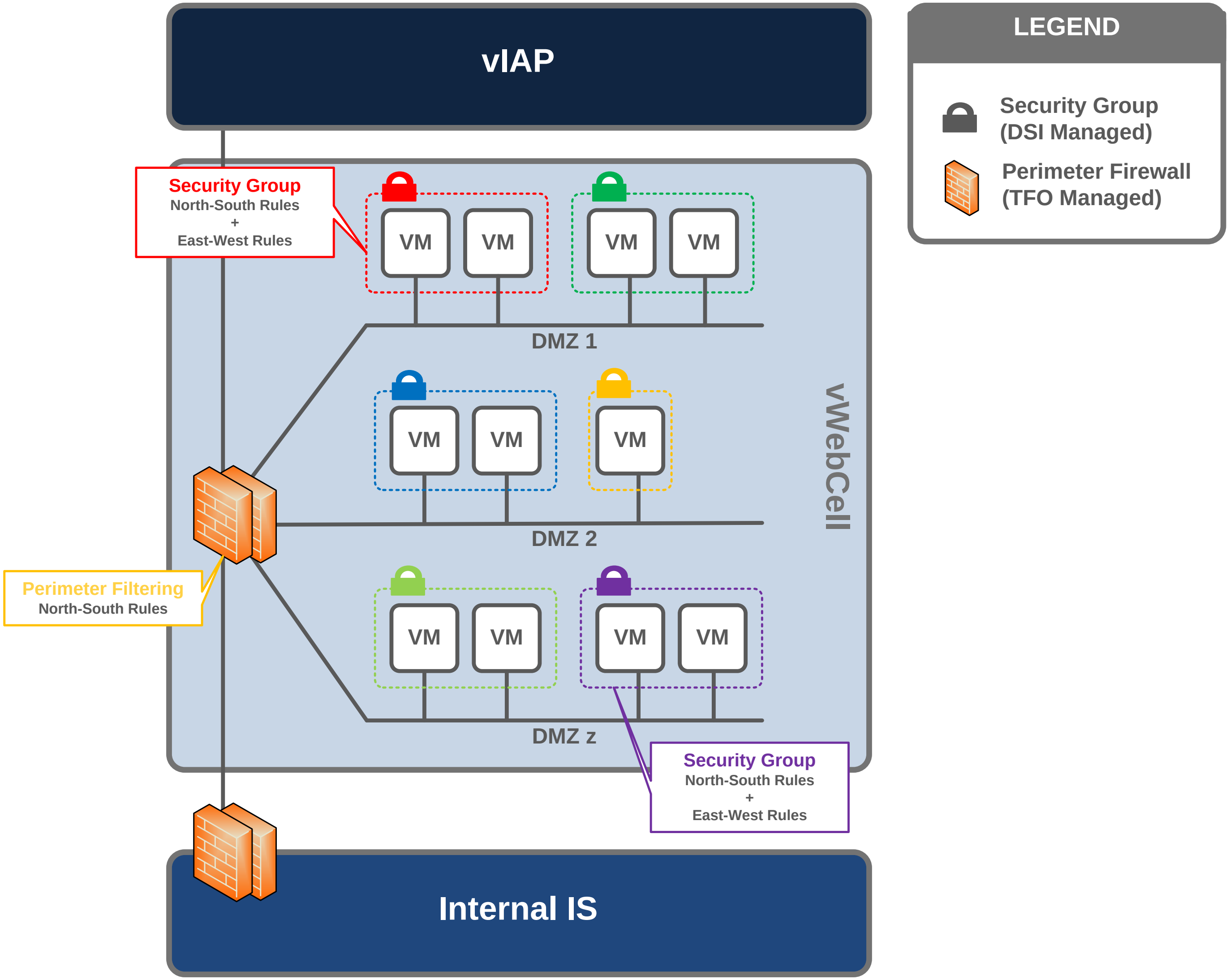
Security Group | Introduction

- GTS Private Cloud instances and Security Group can be deployed on :
  - Internal Security Zones (L1-P,L1-H, DCITS, Shared Services, CDN PROD, CDN DEV…)
  - Exposed DMZs (vWebCell)
- Those internal Security Zones and DMZs are protected from the rest of the Information System by Perimeter Firewalls
- A Security Group acts as a virtual firewall that controls the ingress/egress traffic for one or more Cloud instances.
- Security Group filtering is provided in addition to the Perimeter Firewalls' filtering and is optional. It provides protection for E/W as well as N/S traffic.
- The Security Group and its associated Rules is managed by the DSI whereas the Perimeter Firewall is managed by GTS Network & Security Team (TFO).
- Rules of a Security Group can be modified at any time (API/Portal)
- New rules are automatically applied to the associated instances

Security Group | Internal Security Zone



Security Group | Exposed DMZ (vWebCell)



Security Group | Principles

Global Principles

- **One or more** Security Groups can be associated to an instance.
- Security Group will only be provided for **non replicated** Cloud Instance
- Security Group will be **local to an Availability Zone**
- Cloud Instance can only be member of Security Group that is for the **same environment** and in the same **Availability Zone**
- A Security Group contains **inbound** as well as **outbound** rules
- **Only** filtering base on a **White list approach** will be allowed. An implicit **deny all** will exist at the end of inbound and outbound rules.
- In **outbound**, a **permit ip any/any** will be provided **by default** for each user defined Security Group
- By default, a **maximum of 5 End User Security Groups** will be allowed for **each Application Trigram** and **Environment** (PROD, DEV, TST, INT, UAT), in addition to the Infra Security Group (Infra Forced Rules)
- Once a End User Security Group is associated to an instance (or a group of instance), a default **Infrastructure Security Group** is **automatically** applied to the instance (or the group of instance). This behavior will **ensure** a **minimal access** for the Infrastructure/management feeds to the instance.
- An Infrastructure Security Group has been created for each Customer. The Infrastructure Security Group rules can be different for Production (PRD) and Non Production environments (DEV, UAT, TST and INT) depending on the Customer. There are also different for Internal Private Cloud and for Exposed Private Cloud (vWebCell).
- The Infrastructure Security Group's set of rules **can't be modified by the end user**. Only the customer's infrastructure team can request addition/deletion of rules of the Infrastructure Security Group (Manual update through Cloud Admin team)
- A maximum of **25 inbound rules and 25 outbound rules** will be allowed **per End User Security Group**

Security Group | Principles

- **Name of User Security Group** is **auto-generated** and follows the hereunder rule:

  - **Internal Private Cloud Security Group :** LSG_**XXX_YYY_ZZZZZ_AZ**
  - **vWebCell Security Group :** LSGWCE_**XXX_YYY_ZZZZZ_AZ**

Where

XXX = Environment (3 digit)
YYY = Application Trigram (3 digit)
ZZZZZ = Number – Starts with 00001 an ends with 99999
AZ = Availability Zone without dash (ex : eufrparis2)

- **The following are the default rules applied to a Security Group at its creation:**
  - Deny all inbound traffic [Implicit]
  - Allows all outbound traffic [Explicit]

After you've created a security group, you can change its inbound rules to reflect the traffic allowed to reach your associated instances. In the same way, you can change its outbound rules to reflect the traffic allowed from your associated instances.

Security Group | Access Management

- As requested by the Information Security Offices, **two Active Directory groups** will exist **per Application Trigram and Business Group environment** (PROD and NON_PROD):
  - **Cloud AD Group**
  - **Security Group AD group**

- The Cloud AD Group is the **historical AD Group** that defines the users authorized to manage Cloud Instances, Cloud Load Balancers, Cloud Replication and Cloud Backup.

- The **Security Group AD** group defines the users authorized to **manage Cloud Security Group**.

- The owner of the Security Group AD group will be defined by each DSI and its Information Security Office and will be **accountable of the security provided by the Security Group**.

- Owner and members of the Security Group AD group will be authorized to perform the following actions:
  - Create / List / Delete a Security Group
  - Add / List / Delete Security Group Rules

- The Owner and members of the Cloud AD Group will be authorized to perform the following actions related to Security Group:
  - List Security Group
  - List Security Group Rules
  - Add / List / Remove Cloud Instances to / of / from a Security Group
  - Add / List / Remove Tags to / of / from a Security Group