Offre de Service DMZinCloud

24/10/2017

v1.1

RESG/GTS/RET/APS

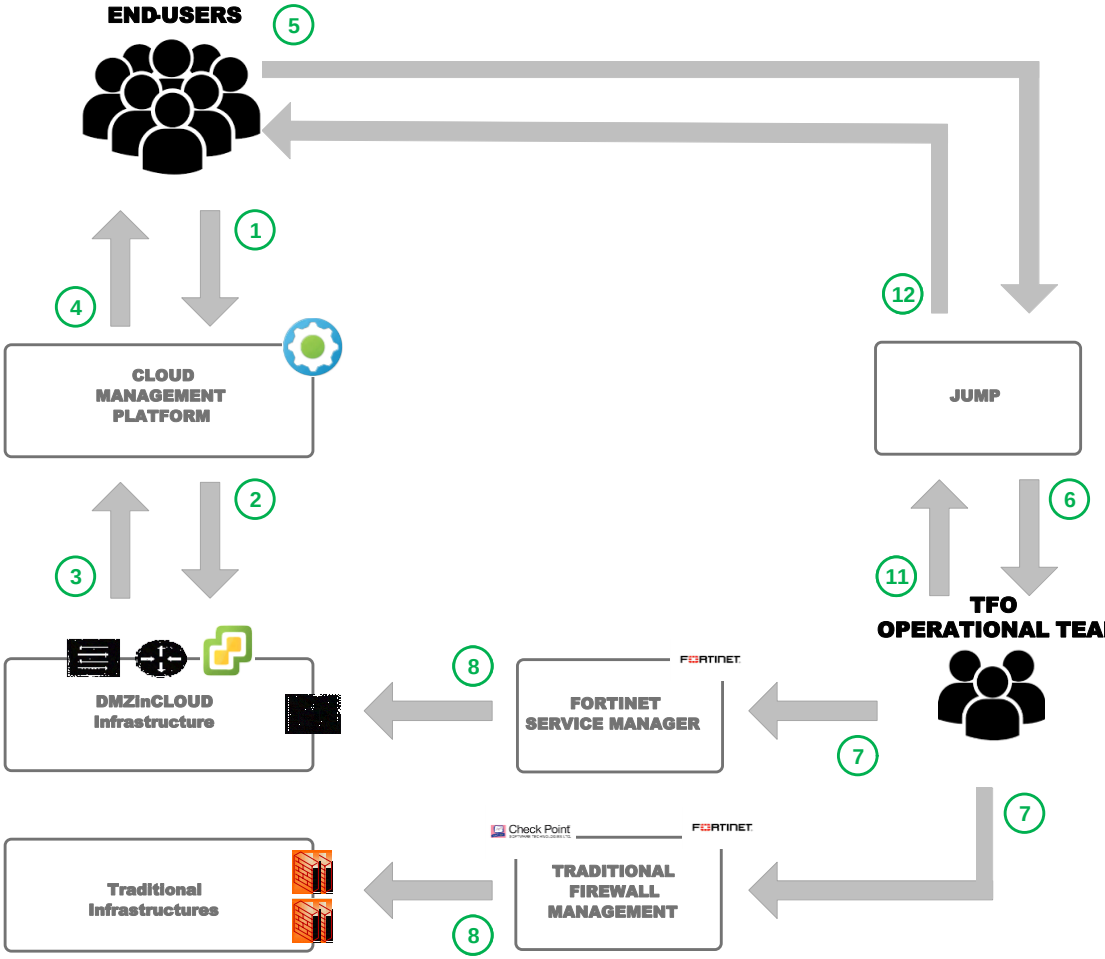
Synthèse

Fonctionnalité		Création de DMZ (zone cloisonnée) en mode As A Service sur l'infrastructure Cloud	
Besoins couverts		Besoin de cloisonnement d'une application non exposée	
Applications éligibles		C0, C1, C2 (le Cloud SG n'est pas homologué C3)	
Dimensionnement subnets		25 (/27) à 57 (/26) *Le nombre d'@IP inclus les adresses des services applicatifs*	
Filtrage		- Firewall virtuel en entrée de DMZ (filtrage Nord-Sud) - VM groups pour le filtrage Est-Ouest et Nord-Sud - Le paramétrage des VM Groups est à la main des DSI	
Automatisation	Création/Suppression de DMZ	Oui	
	Création/Suppression de VM	Oui	
	Création	Oui	
	Création/suppression de règles dans les VM Groups	Via ticket JUMP	
VM Groups	Nombre de VM Groups	5 VM Groups /trigramme et environnement	
	Règles de filtrage (VM Groups)	IN : 25	OUT : 25
	Limites	Les VM répliquées ne peuvent être associées à un VM Group	
Backup et Résilience		Il n'y a pas de backup ni de réplication prise en charge par l'infrastructure Cloud.	

Qu’est-ce que DMZinCloud

- Le service DMZinCloud permet de provisionner et supprimer des DMZ en mode service
  - DMZinCloud est disponible dans chaque AZ
  - A l’instanciation de la DMZ, un subnet pré-provisionné en /26 (62 @IP) ou /27 (30 @IP) lui est associé
    - Le nombre d’@IP inclus les adresses des services applicatifs
  - Lors de la suppression de la DMZ, le subnet sera libéré
- La création et la suppression de la DMZ est prise en charge par le portail HP CSA au travers de services à exécuter.
- Une DMZ créée via le service DMZinCloud permet de disposer d’une zone cloisonnée sur le Cloud interne GTS
  - Les applications C0, C1 et C2 sont éligibles
- Lors de la création de la DMZ, le firewall d’entrée sur la DMZ se voit appliquer des flux techniques RET grâce à une matrice implémentée à la volée par TFO.
  - Les autres flux sont à faire ouvrir via un ticket Jump

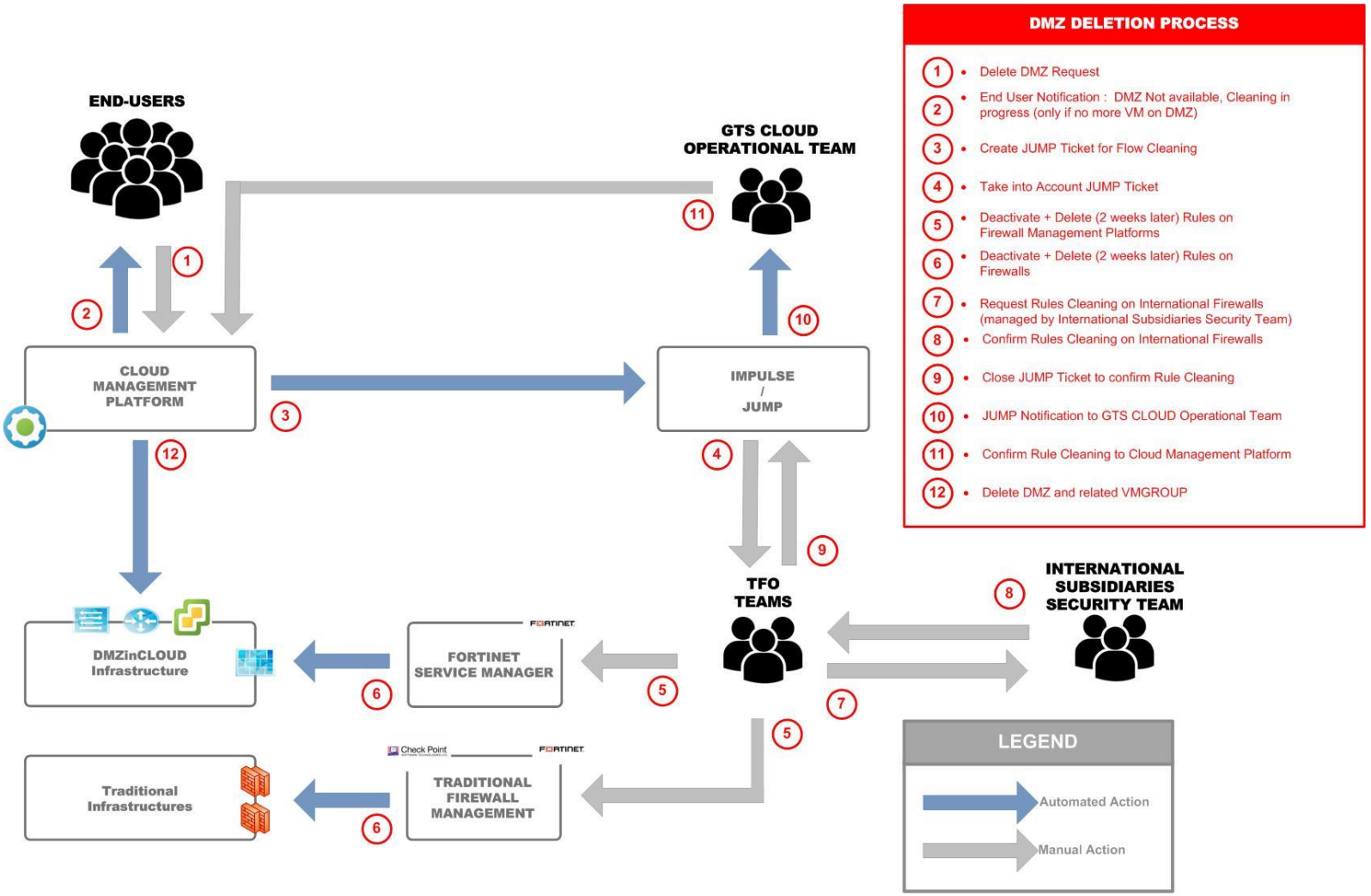
Process de création



DMZ CREATION PROCESS

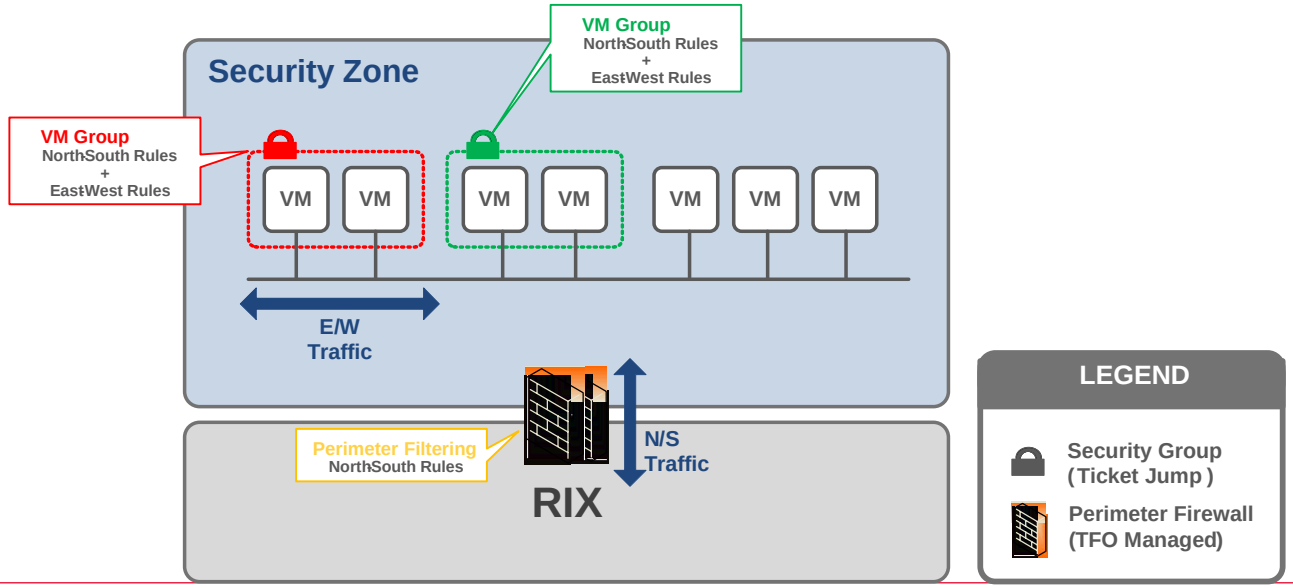
1. Create DMZ , VMGROUP , VM
2. Provision DMZ , VMGROUP , VM on DMZinCLOUD Infrastructure
3. Provisionning Done
4. End User Notification : Provisionning Done
5. Create JUMP Ticket for Flow Opening
6. Take into Account JUMP Ticket
7. Create Rules on Firewall Management Platforms
8. Request Rules Opening on International Firewalls (managed by International Subsidiaries Security Team)
9. Confirm Rules Opening on International Firewalls
10. Deploy Rules
11. Close JUMP Ticket
12. End User Notification : Flow Opening proceeded

Process de suppression



Le filtrage des flux pour les DMZinCloud

- Le filtrage Nord-Sud (inter-DMZ) est assuré par un firewall
  - Les VM Groups peuvent aussi assurer le filtrage Nord-Sud en complément du firewall
- Le filtrage Est-Ouest (intra-DMZ) est assuré par les VM Groups
  - Les VM Groups sont gérés par les DSI
- Les VM Groups suivent les mêmes principes que les Security Groups
  - Les VM Groups s'appliquent aux zones exposées (vWebcells) et les VM Groups d'appliquent aux DMZinCloud
  - La technologie sous-jacente est différente
  - La création/suppression des règles dans un VM Group est fait par ticket Jump
- VM Group et Infrastructure Security Group
  - Lorsqu'une VM est associée à un VM Group, un Infrastructure Security Group est automatiquement créé pour permettre les flux minimaux de managent de l'infrastructure
  - Un Infrastructure Security Group ne peut être modifié par un utilisateur final. Seule l'équipe responsable de sa mise en place peut demander l'ajout ou la suppression de règles
  - Les Infrastructure Security Groups sont crées pour chaque client. Ils peuvent être différents selon l'environnement (Production et Non-Production) et le type de zone (Cloud Interne et zone exposée (vWebcell))



VM Groups : Principes et Contraintes

- Une VM peut être associée à un ou plusieurs VM Groups
- Les VM Groups ne peuvent pas être associés à une VM répliquée par l'infrastructure Cloud
  - Si besoin de réplication, il est nécessaire de créer les VM et le VM Group sur le site primaire et la même infrastructure sur le site secondaire et de procéder à une réplication applicative
- Il n'est pas possible de dupliquer les règles de VM Groups
  - Les VM Groups sont locales à une AZ
- Une VM peut être associée à plusieurs VM Groups dans un même environnement et une même AZ
- Par défaut, un maximum de 5 VM Groups sont autorisés par trigramme et environnement
- Un maximum de 25 règles en entrée et 25 règles en sortie peuvent être définies par VM Group
- Il n'y a pas de backup sur les VM des DMZinCloud
- Il n'y a pas de réplication des VM des DMZinCloud. Pour une résilience, il est nécessaire de créer une DMZinCloud sur le site de secours et d'effectuer une réplication applicative,