

---

# Rapport de conception

Mini projet IAE-TBS

---

Florian Clanet  
Rama Desplats  
Yuxiao Mao

5 SDBD INSA Toulouse

# Sommaire

[I- Présentation de l'existant](#)

[II- Interface graphique du projet](#)

[Les abréviations](#)

[Étape 1 : Gestion de l'adaptation transparente, à l'initiative de l'opérateur](#)

[Diagramme des uses cases :](#)

[Use case 0 : Initialisation du système](#)

[Use case 1 : Déploiement d'une gateway intermédiaire sur le DC](#)

[Use case 2.1: Créer une nouvelle règle de redirection](#)

[Use case 2.2: Éditer une règle de redirection dans la liste des règles de redirection](#)

[Use case 2.3: Supprimer une règle de redirection dans la liste des règles de redirection](#)

[Use case 3: Supprimer une gateway du data-center](#)

[Diagramme des classes](#)

[Étape 2 : Gestion de l'adaptation transparente de façon autonome](#)

[Use case 1 : Initialisation des politiques par défaut du manager automatique](#)

[Use case 2 : Définition des politiques du manager automatique par l'administrateur](#)

[Use case 3 : Le Manager automatique monitore l'état du système et actionne des réponses si nécessaire.](#)

[Use case 4 : Déploiement d'une gateway intermédiaire sur le DC](#)

[Use case 5: Equilibrer l'utilisation des ressources en agissant sur les règles de redirection](#)

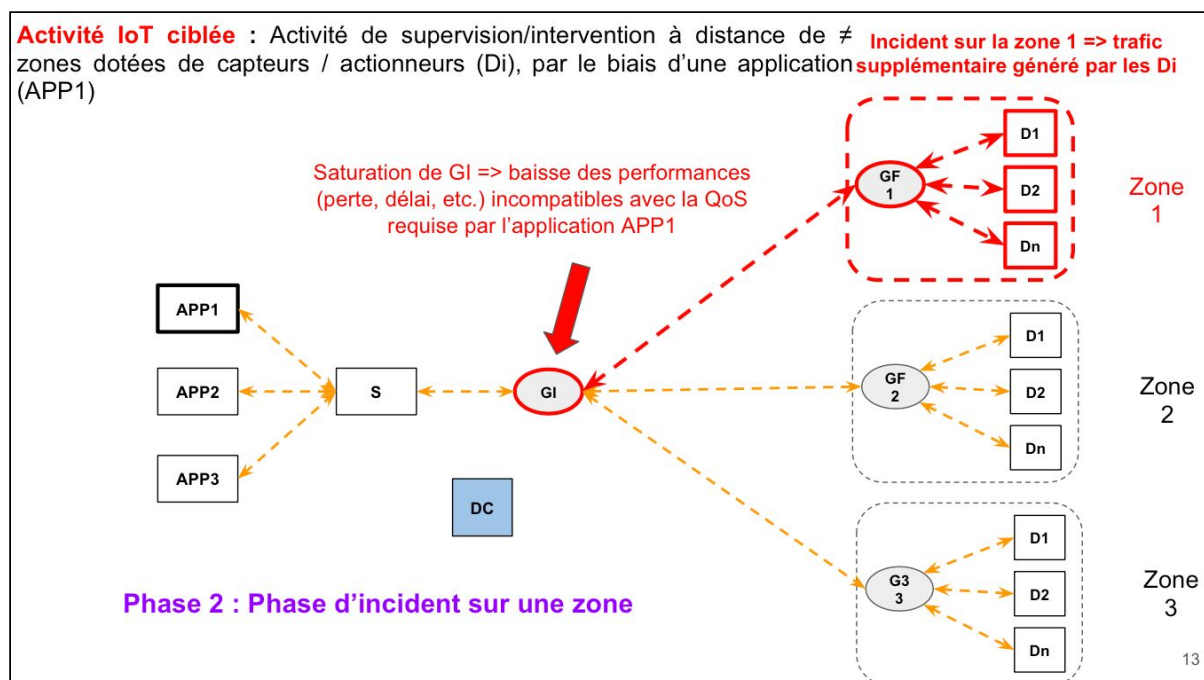
[Use case 6 : Supprimer une gateway du data-center](#)

[Use case 7 : Déploiement d'un reverse proxy sur le Datacenter](#)

[Use case 8 : Déploiement d'un firewall sur le DC](#)

[Améliorations possibles](#)

## I- Présentation de l'existant



Ce mini projet s'articule autour de nombreux concepts important de demain, comme entre autres : les fonctions virtuels de réseaux, la technologie Mininet, l'Autonomic Computing, etc.

Le sujet prend place dans un réseau reliant des applications à des zones dotées de capteurs/actionneurs par le biais d'un serveur applicatif et d'une gateway initial. Cependant, des incidents sur les zones de capteurs/actionneurs peuvent entraîner une génération trop importante de données et saturer le réseau. Une saturation qui entrainera inévitablement une dégradation des qualités de services proposées par le réseau.

Afin de répondre à cette problématique, nous présenterons comment nous avons conçus un système capable de rétablir ces qualités de service. Cette réponse sera apportée en deux étapes différentes.

La première étape nécessite une utilisation proactive de notre système par l'administrateur du réseau. Ainsi, l'administrateur ayant une connaissance avancée du réseau et de son état sera en mesure de répondre aux différents incidents via ce qui sera proposé par notre système (les réponses seront détaillées ultérieurement dans ce dossier).

La seconde étape serait de tirer bénéfice du concept d'Autonomic Computing et de se reposer que de façon initiale sur l'administrateur. En effet, celui-ci indiquerait à notre systèmes quelles qualités de service il souhaite conserver afin que le système puisse détecter une situation anormale et y répondre. L'administrateur n'aura donc plus besoin d'intervenir ultérieurement puisque le système sera en mesure de contrôler le réseau de façon automatique.

## II- Interface graphique du projet





### Mini projet INSA

#### Liste des Gateway finales

Nom	Adresse IP
Parc IOT	10.0.0.1
Parc IOT2	10.0.0.2
Parc TOI	10.0.0.3












#### Liste des Gateway intermédiaires

[+ Créer](#)

Nom	Adresse IP	Actions
Gateway intermédiaire1	10.0.0.5	
Gateway intermédiaire2	10.0.0.6	
Gateway intermédiaire3	10.0.0.7	
Gateway intermédiaire4	10.0.0.8	

#### Liste des liaisons

[+ Créer](#)

Nom	Adresse IP		Nom	Adresse IP	Actions
Parc IOT	10.0.0.1		Gateway intermédiaire1	10.0.0.5	 
Parc IOT2	10.0.0.2		Gateway intermédiaire2	10.0.0.6	 
Parc TOI	10.0.0.3		Gateway intermédiaire3	10.0.0.7	 
Parc TOI2	10.0.0.4		Gateway intermédiaire4	10.0.0.8	 
Parc TOI3	10.0.0.10		Gateway intermédiaire5	10.0.0.9	 

Dans l'intérêt du projet, nous avons cherché à produire l'interface graphique la plus simple et claire possible. En effet, l'administrateur réseau possède déjà une connaissance pointue de la topologie du réseau dans son état normal.

Ainsi, nous nous sommes concentré sur la possibilité de lui apporter une plus-value vis-à-vis de notre interface graphique. C'est pourquoi nous pouvons, dans un premier temps, retrouver la liste des gateway finales (supposées non modifiables) et la liste des gateway intermédiaires. Ces dernières peuvent être supprimées et créés via l'interface graphique (sauf la gateway initiale supposée immuable). En effet, lorsque l'administrateur ne souhaite pas garder une gateway intermédiaire deux choix s'offrent à lui grâce aux propriétés de la virtualisation:

- Il pourrait simplement stopper la gateway, supprimer les règles de routage associés et ne la rallumer que si nécessaire
- Il pourrait supprimer la gateway et les règles de routage associés et la re-crée si nécessaire

Nous avons choisi de supprimer les gateway intermédiaires parce que cela permettait de supprimer la nécessité de sauvegarder des informations vis à vis des gateways arrêtés. Au vu des use-case décrits après, il était plus simple de supprimer la gateway et la créer à nouveau plus tard. Cette décision serait éventuellement à rediscuter à la lumière de l'offre du fournisseur de service, en fonction de la nature des éléments facturés.

Enfin, nous pouvons trouver la liste des liaisons entre gateway finales et gateway intermédiaires. Après questionnement du sujet, nous avons estimé que l'état standard (l'état originel) du réseau impliquait que toutes les gateway finales transitent via la gateway initiale. Ainsi, il est aisé de se dire que l'administrateur réseau ne serait intéressé de connaître seulement les éléments différents de cet "état standard". C'est pourquoi nous avons choisi de ne lister que les liaisons entre les gateway finales et les gateway intermédiaires. Ces liaisons peuvent être créées, modifiées et supprimées sur demande de l'utilisateur. En effet, lister la totalité de la topologie pourrait, dans le cas où le réseau serait plus complexe (plus de gateway finales et gateway intermédiaires), masquer à l'administrateur les informations qui nous semblent importantes (les éléments qui diffèrent de l'état standard).

## Mini projet INSA

### Liste des Gateway finales

Nom	Adresse IP
GF Parc IOT	10.0.0.1
GF Parc IOT2	10.0.0.2
GF Parc TOI	10.0.0.3

### Liste des Gateway intermédiaires

+ Créer

Nom	Adresse IP	Actions
Gateway initial	10.0.0.5	
Gateway intermédiaire2	10.0.0.6	
Gateway intermédiaire3	10.0.0.7	
Gateway intermédiaire4	10.0.0.8	

Créer un nouveau container

Espace disque:  Go

RAM:  Mo

Processeur:  CPU

Créer
Annuler

### Liste des liaisons

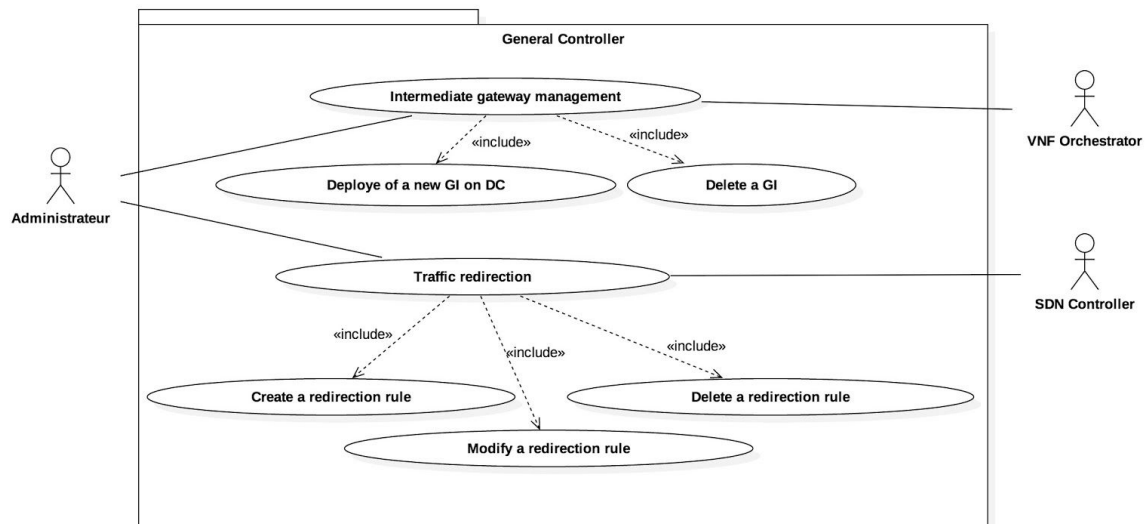
+ Créer

Nom	Adresse IP		Nom	Adresse IP	Actions
GF Parc IOT	10.0.0.1		Gateway initial	10.0.0.5	
GF Parc IOT2	10.0.0.2		Gateway intermédiaire2	10.0.0.6	
GF Parc TOI	10.0.0.3		Gateway intermédiaire3	10.0.0.7	
GF Parc IOT2	10.0.0.2		Gateway intermédiaire4	10.0.0.8	
GF Parc TOI	10.0.0.3		Gateway intermédiaire2	10.0.0.6	

Notre interface graphique disposera de popups offrant à l'administrateur une liberté totale de configuration de son réseau. Par exemple, la popup ci-dessus permet à l'administrateur de personnaliser le container dans lequel il souhaitera déployer sa gateway.

GC : General controller  
DC : Datacenter  
GF : Gateway Finale  
GI : Gateway intermédiaire, les gateways créés dans Datacenter  
Gateway initiale : Gateway intermédiaire initialement existant, à l'extérieur du DC

### Diagramme des uses cases :



Acteurs : Administrateur, IHM, GC Core, SDN adapter, SDN Controller, VNF adapter

## Objectif : Construire la topologie du réseau dans GC Core

Aperçu : Au lancement, le système prend la connaissance de la topologie du réseau à manipuler. Cette récupération se fait via le GC Core qui analyse la topologie du réseau en interrogeant le réseau SDN. Le GC Core va ensuite communiquer au VNF adapter les informations concernant la gateway initiale.

Déclencheurs : Lancement de l'interface graphique

Pré-conditions :

- Le réseau SDN est déjà construit
- Aucune GI n'existe dans le DC
- Aucune règles de redirection n'existe

Post-conditions : Le GC Core dispose d'une topologie complète du réseau à manipuler

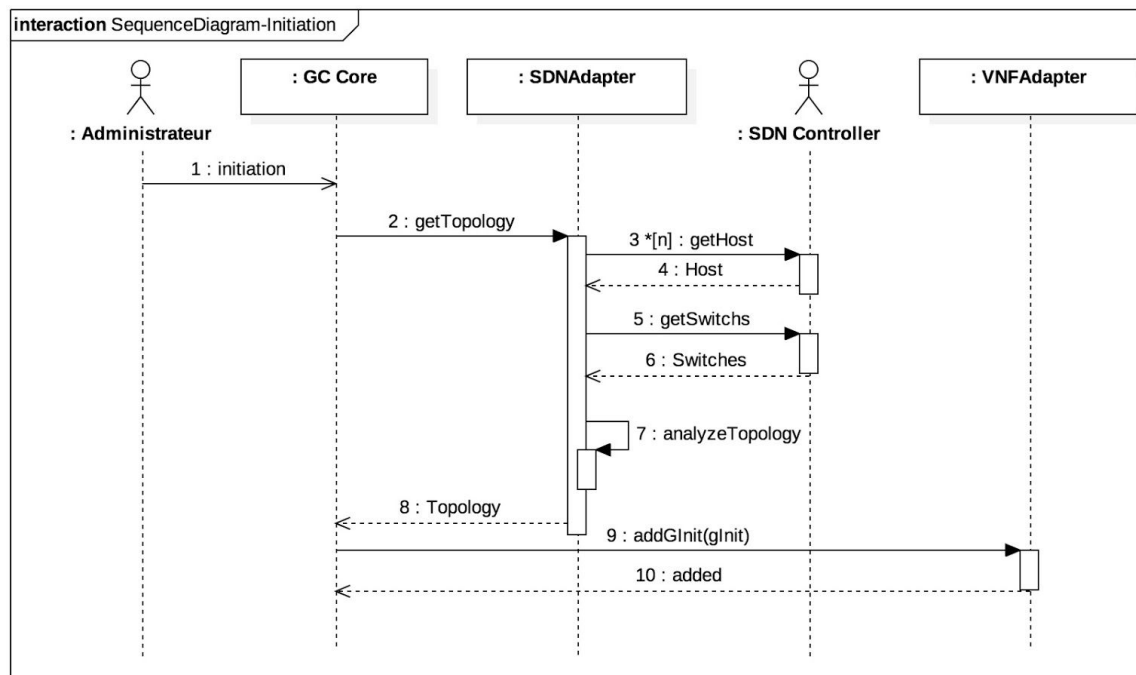
Action de l'acteur :

- L'administrateur lance le panel d'administration (IHM)

Réponse du système :

- Actions de l'interface graphique
  - Lancer l'initialisation du GC Core
  - Une fois l'initialisation terminée, mettre à jour l'affichage
- Actions du GC Core
  - Récupérer la topologie via le SDN adapter
  - Mettre à jour la topologie
  - Donner au VNF Adapter les informations concernant la gateway initiale
- Actions du SDN Adapter
  - Récupérer les informations des GF, la Gateway Initial, le Serveur applicatif et le réseau
- Actions du VNF Adapter
  - Stocker les informations concernant la gateway initiale

Diagramme de séquence:





## **Use case 1 : Déploiement d'une gateway intermédiaire sur le DC**

Acteurs : Administrateur, IHM, GC Core, VNF Adapter, VNF Orchestrateur

Description : Le système mis en place doit être en mesure de laisser la possibilité à l'administrateur de déployer une gateway intermédiaire. En effet, lorsque l'administrateur constate une dépréciation des qualités de services, il peut déployer une gateway intermédiaire afin de rétablir les qualités de services initiales.

Objectif : Déployer une gateway intermédiaire après action de l'administrateur.

Aperçu : L'administrateur doit être en mesure de se connecter à l'interface graphique afin de déployer une nouvelle gateway intermédiaire. Le déploiement et les actions suivantes seront effectuées en mode "boîte noire" vis à vis de l'opérateur. L'opérateur n'aura alors plus qu'à vérifier que les qualités de services soient à nouveau acceptables.

Déclencheurs : L'administrateur clique sur le bouton de déploiement.

Pré-conditions : L'administrateur lance le panel d'administration (IHM).

Une image docker de la gateway intermédiaire aura été créée au préalable à l'aide d'un dockerfile et stockée afin d'être accessible par le VNF Orchestrateur. Un Datacenter aura été créé au préalable afin de permettre le déploiement des conteneurs gateway intermédiaires.

Post-conditions : La réussite ou non du déploiement est loguée à partir de la réponse du VNF Orchestrateur. En cas de succès, la nouvelle gateway est ajoutée à la liste des gateway déployées. En cas d'échec, la nouvelle gateway n'est pas sauvegardée.

Action de l'acteur :

- L'administrateur lance le panel d'administration et clique sur le déploiement d'une nouvelle gateway
- L'administrateur saisit les propriétés du conteneur à créer telles que RAM, CPU, Disk

Réponse du système :

- Actions de l'interface graphique :
  - L'interface graphique s'affiche avec le bouton permettant l'action de déploiement d'une gateway intermédiaire
  - L'interface graphique s'affiche avec une pop-up permettant de saisir les propriétés du conteneur à créer telles que RAM, CPU, Disk
  - L'interface graphique affiche si le déploiement requis par l'utilisateur s'est déroulé avec succès ou non
  - Si le déploiement est un succès, alors les informations de cette gateway intermédiaire sont stockées dans la liste des gateway.

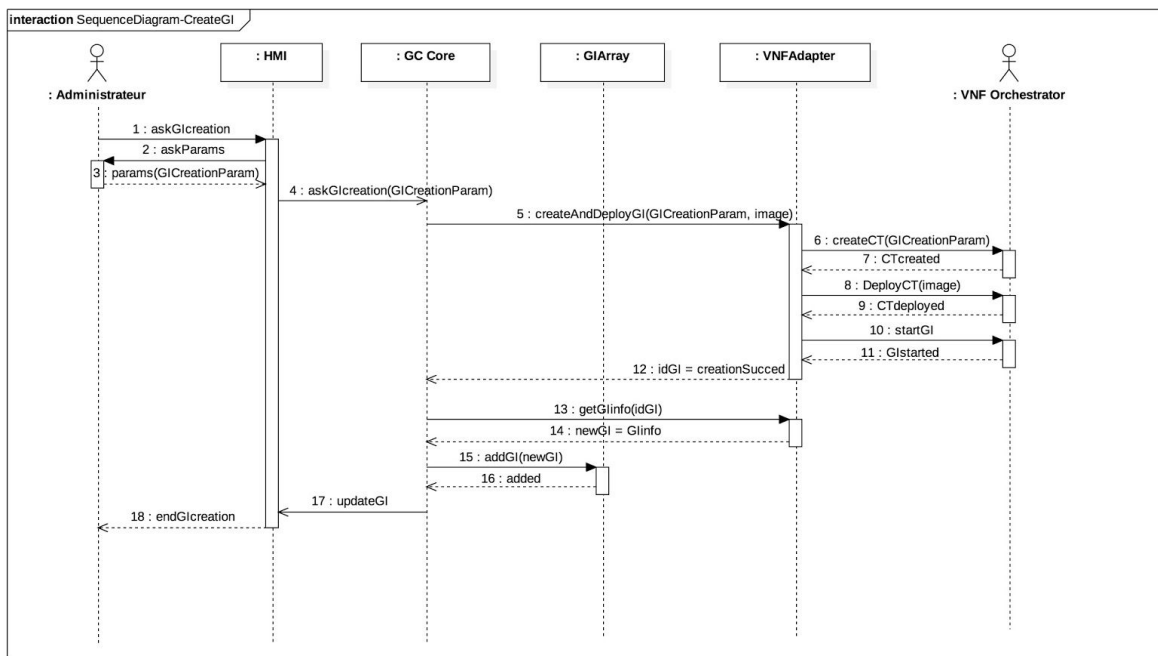
- Actions du GC Core :

- Commander au VNF Orchestrator la création à partir d'une image connue, d'un conteneur avec les propriétés RAM, CPU, Disk Spécifiées
- Mettre à jour la liste des GI selon le résultats de déploiement
- Transmettre le notification à l'interface graphique

Actions du VNF Orchestrator :

- Créer sur le datacenter le conteneur demandé.
- Déployer le conteneur à partir de l'image créée au préalable, et embarquant l'application gateway.
- Démarrer le conteneur et l'application embarquée.
- En cas d'échec ou succès, envoyer une notification à GC Core

Diagramme de séquence :



## Use case 2.1: Créer une nouvelle règle de redirection

Acteurs : Administrateur, IHM, GC Core, SDN Adapter, SDN Controller

Description : Le système mis en place doit être en mesure de pouvoir créer une règle de redirection dans la liste des règles proposées par l'IHM.

Objectif : Opérer la redirection du trafic de la gateway finale vers la gateway intermédiaire et de la gateway intermédiaire vers le serveur applicatif.

Aperçu : Afin d'alléger le volume de paquets internets transitant via la gateway initiale (entraînant une dégradation de la qualité de service), le système doit être en mesure de

créer les règles de routage nécessaires afin de rediriger le trafic. Cela permettra aux paquets dont la source/destination est la gateway finale du réseau, d'être redirigés vers la gateway intermédiaire choisie. La qualité de service sera donc améliorée.

Déclencheurs :

- L'administrateur clique sur le bouton "Créer une nouvelle redirection".

Pré-conditions : N/A

Post-conditions : Mise à jour de l'interface graphique en conséquence.

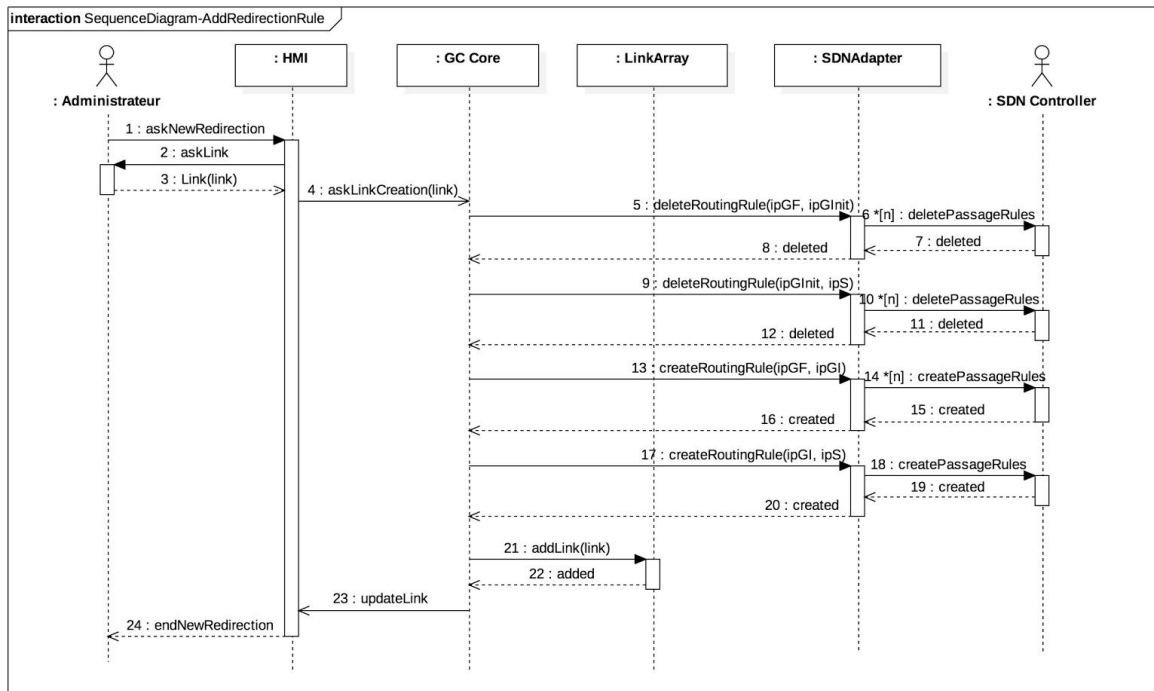
Action de l'administrateur :

- Cliquer sur le bouton "Créer une nouvelle redirection"
- Choix d'un élément dans la liste des gateways intermédiaires et une gateway finale
- Clic sur le bouton "Confirmer" ou clic "Annuler"

Réponse du système :

- IHM :
  - Une fois que l'administrateur a cliqué sur le bouton "Créer une nouvelle redirection", afficher 2 listes déroulantes (respectivement "Gateway Finale" et "Gateway Intermédiaire") et 2 boutons ("Confirmer" et "Annuler").
  - Si l'administrateur clique sur le bouton "Confirmer", une demande sera transmise au GC core. Si l'administrateur clique sur le bouton "Annuler", l'IHM est mise à jour et il n'y a pas de demande transmise.
  - Après avoir reçu la réponse du GC core, l'IHM se met à jour.
- GC Core
  - Après avoir reçu la demande d'une création de règle, le GC Core modifie toutes les règles de routage concernant la GF choisie pour que les trames sortant de la GF choisie passent maintenant par la GI ciblée
    - Suppression des règles de routage entre la gateway finale et la gateway initiale, et entre la gateway initiale et le serveur applicatif
    - Création des règles de routage entre la gateway finale et la gateway intermédiaire, et la gateway intermédiaire et le serveur applicatif
    - Modifier les paquets qui transitent afin de modifier les entêtes IP (En effet, le serveur applicatif attend une réponse de GF et non GI. Il faut faire la modification sinon il va rejeter le paquet).
  - GC Core envoie une réponse à l'IHM pour informer l'administrateur de la réussite ou non de la redirection.
  - Si c'est un succès, le GC core sauvegarde la redirection effectuée dans la liste des redirections

Diagramme de séquence :



## Use case 2.2: Éditer une règle de redirection dans la liste des règles de redirection

Acteurs : Administrateur, IHM, GC Core, SDN Adapter, SDN Controller

Description : Le système mis en place doit être en mesure de pouvoir modifier une règle de redirection dans la liste des règles proposé par IHM.

Objectif : Opérer la redirection du trafic de la gateway finale vers la gateway intermédiaire et de la gateway intermédiaire vers le serveur applicatif.

Aperçu : Afin de pouvoir adapter l'utilisation des Gateways Intermédiaires, le système doit être en mesure de modifier les règles de routage nécessaires à la redirection du trafic internet. Cela permettra aux paquets dont la source/destination est la gateway finale du LAN d'être redirigés vers la gateway intermédiaire choisie. Les qualités de services seront donc améliorées si l'administrateur a bien fait son choix.

Déclencheurs :

- L'administrateur clique sur le bouton "Edit" d'une règle de redirection

Pré-conditions : La règle de redirection est valable

Post-conditions : Mise à jour de l'interface graphique en conséquence

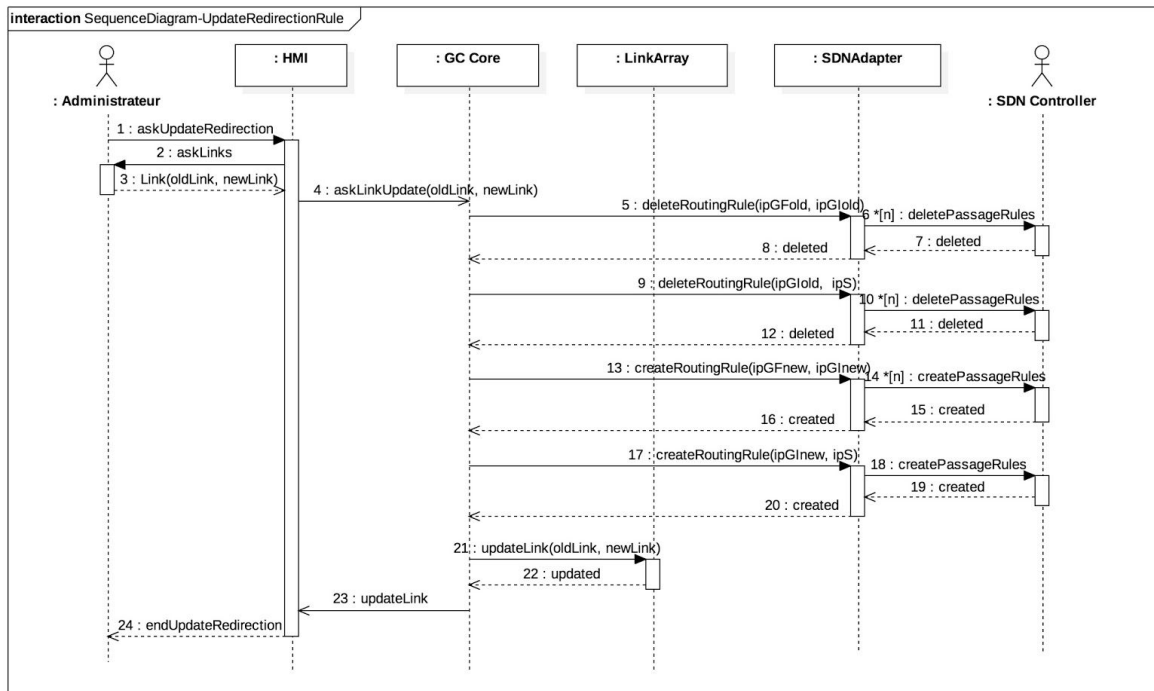
Action de l'administrateur :

- Choisir un élément dans la liste des règles de redirection
- Cliquer sur le bouton "Edit"
- Choisir dans le menu déroulant, la nouvelle gateway intermédiaire par laquelle le trafic provenant de la gateway finale va passer
- Cliquer sur le bouton "Confirmer"

Réponse du système:

- IHM
  - Une fois que l'administrateur a cliqué sur le bouton "Edit" d'une règle de redirection, une pop-up s'ouvre et la règle devient éditable. La gateway intermédiaire est contenu dans une liste déroulante, à l'instar de la gateway finale
  - Une fois que l'administrateur a cliqué sur le bouton "Confirmer", l'IHM transmet une demande de redirection au GC Core seulement si la gateway intermédiaire choisi est différente de la gateway intermédiaire initialement utilisée.
  - l'IHM attend la réponse du GC Core pour mettre à jour son affichage
- GC Core
  - Une fois la demande venant de l'IHM reçue, le GC Core modifie toutes les règles de routage (ciblant la Gateway Intermédiaire d'origine) afin que les paquets sortant de la Gateway Finale choisie passent maintenant par la Gateway Intermédiaire ciblée
  - GC Core envoie une réponse à l'IHM pour informer de la réussite ou non de la redirection.
  - Si c'est réussi, le GC Core sauvegarde la redirection effectuée dans la liste des redirections

Diagrammes de séquences :



### Use case 2.3: Supprimer une règle de redirection dans la liste des règles de redirection

Acteurs : Administrateur, IHM, GC Core, SDN Adapter, SDN Controller

Description : Le système mis en place doit être en mesure de pouvoir supprimer une règle de redirection dans la liste des règles proposé par l'IHM.

Objectif : Opérer la redirection du trafic de la gateway finale vers la gateway intermédiaire et de la gateway intermédiaire vers le serveur applicatif.

Aperçu : Afin de pouvoir adapter l'utilisation des Gateway Intermédiaire, le système doit être en mesure de modifier les règles de routage nécessaire afin de rediriger le trafic internet. Cela permettra aux paquets dont la source/destination est la gateway finale du LAN d'être redirigés vers la gateway intermédiaire choisie. La suppression d'une règle de redirection signifie que les paquets venant du la Gateway Finale concernée seront dirigés vers la gateway initiale.

Déclencheurs :

- L'administrateur clique sur le bouton "Supprimer" d'une règle de redirection.

Pré-conditions : La règle de redirection est valable.

Post-conditions : Mise à jour de l'interface graphique en conséquence.

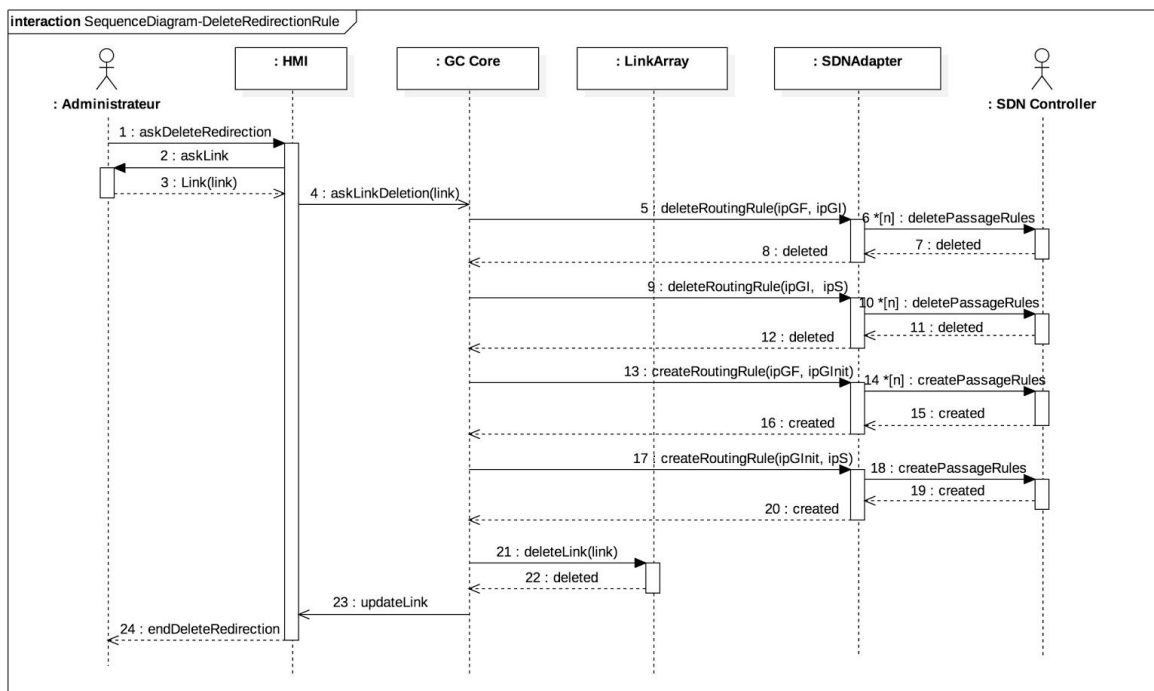
Action de l'administrateur :

- Choix d'un élément dans la liste des règles de redirection.
- Cliquer sur le bouton "Supprimer"

Réponse du système :

- IHM :
  - Une fois que l'administrateur a cliqué sur le bouton "Supprimer" d'une règle de redirection, l'IHM transmet une demande de redirection au GC Core pour que le trafic venant de la Gateway finale concernée soit redirigé vers la gateway initiale.
  - l'IHM attend la réponse du GC Core pour mettre à jour son affichage
- GC Core :
  - Une fois la demande venant de l'IHM reçue, le GC Core modifie toutes les règles de routage (ciblant la Gateway Intermédiaire d'origine) pour que les trames sortant de la Gateway Finale choisie passent maintenant par la Gateway Initiale
  - Le GC Core envoie une réponse à l'IHM pour informer de la réussite ou non de la redirection.
  - Si c'est un succès, le GC Core sauvegarde la redirection effectuée dans la liste des redirections.

Diagrammes de séquences :



### **Use case 3: Supprimer une gateway du data-center**

Acteurs : Administrateur, IHM, GC Core, VNF Adapter, VNF Orchestrateur

Description : Le système mis en place doit être en mesure de laisser la possibilité à l'administrateur de supprimer une gateway intermédiaire. En effet, lorsque l'administrateur constate que les qualités de services sont revenues à la normale et que la gateway n'est plus nécessaire, il peut supprimer une gateway intermédiaire afin de réduire la dépense de ressources inutile par le datacenter.

Objectif : Limiter l'utilisation des ressources du datacenter

Aperçu : L'administrateur doit être en mesure de se connecter à l'interface graphique afin de supprimer une gateway intermédiaire. La suppression et les actions suivantes seront effectués en mode "boîte noire" vis à vis de l'opérateur.

Déclencheurs : L'administrateur lance le panel d'administration (interface graphique).

Pré-conditions : La gateway cible est déployée et accessible au sein du système.

Post-conditions : La gateway cible n'apparaît plus dans la topologie du réseau.

Déroulement des événements : Actions de l'acteur et réponse du système

Action de l'acteur :

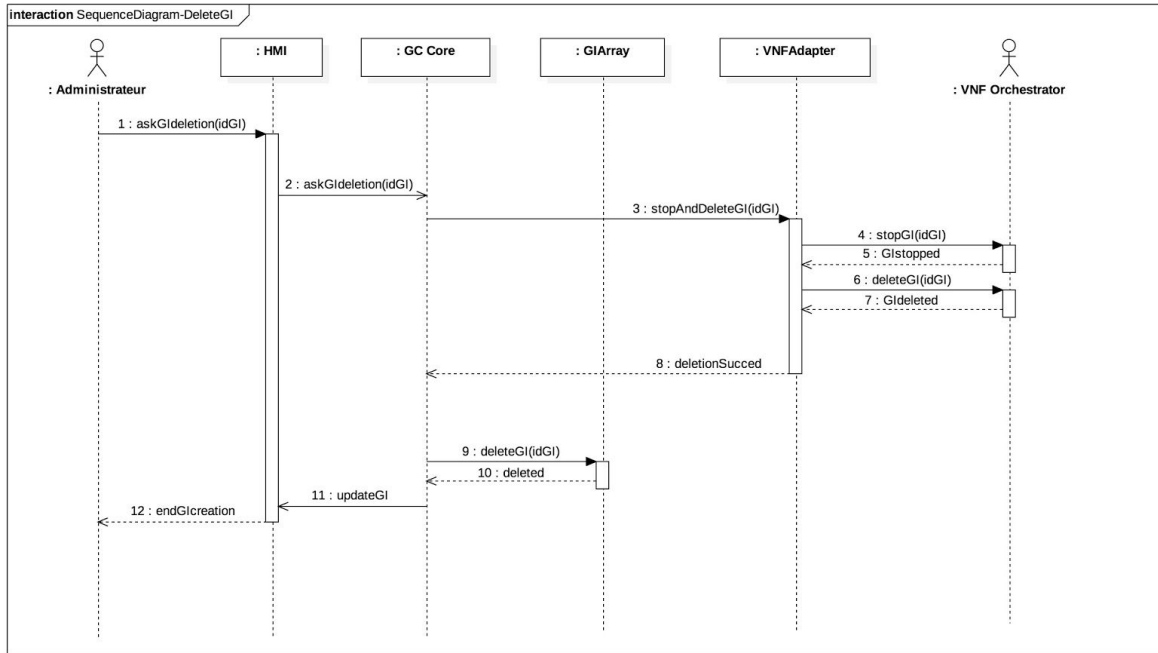
- L'administrateur lance le panel d'administration et clique sur l'option de suppression d'une gateway existante.

Réponse du système :

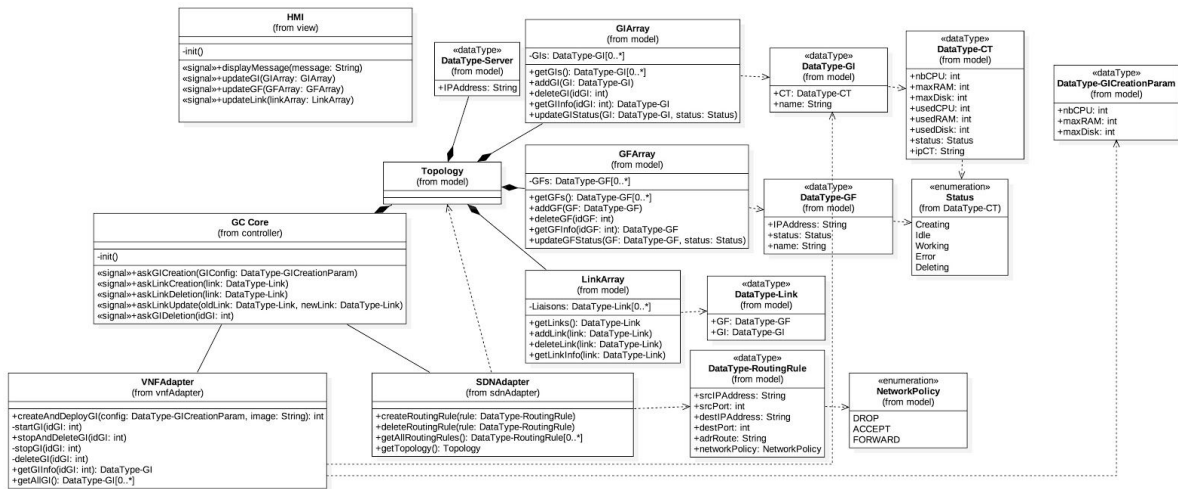
- Actions de l'interface graphique :
  - L'interface graphique affiche la liste des gateway intermédiaire avec la possibilité de suppression
  - L'interface graphique refuse la suppression s'il n'existe qu'une gateway intermédiaire (gateway initiale comprise)
  - L'interface graphique affiche un message d'alerte et demande la confirmation de l'administrateur, si cette gateway intermédiaire est utilisée par au moins une gateway finale
  - L'interface graphique affiche si la suppression requise par l'utilisateur s'est déroulée avec succès ou non
  - Si la suppression est un succès, alors les informations de cette gateway intermédiaire sont supprimées de la liste des gateway déployées.
- Actions du GC Core:
  - Le GC Core supprime via le VNF Orchestrateur le conteneur gateway cible.
  - Il notifie d'une réussite ou non de l'opération.

Diagramme de séquence :





## Diagramme des classes



## Étape 2 : Gestion de l'adaptation transparente de façon autonome

Le modèle de l'autonomic computing proposé par IBM présente différentes fonctions d'auto-gestion possibles pour les systèmes. Au sein de ce projet, nous avons décidé d'en implanter certaines.

La capacité de configuration et de reconfiguration (**self-configuring**) nous semblait particulièrement intéressante dans le cadre de la problématique traitée. À travers un système de monitoring de certaines caractéristiques de l'environnement (RAM, CPU, [A COMPLETER] des gateways), il aura la possibilité de modifier en temps réel et de manière autonome la topologie du réseau en, entre autres, déployant/supprimant des gateways.

De plus, nous avons pensé à une amélioration possible du système de monitoring qui autoriserait l'administrateur à renseigner des caractéristiques de trafic qu'il considère optimales, une limite haute ou encore une moyenne. Ces informations seraient alors régulièrement comparées à l'état de la plateforme et déclencherait une procédure d'adaptation adéquate en fonction de la situation afin d'optimiser le trafic ou d'économiser les ressources du datacenter (**self-optimizing**).

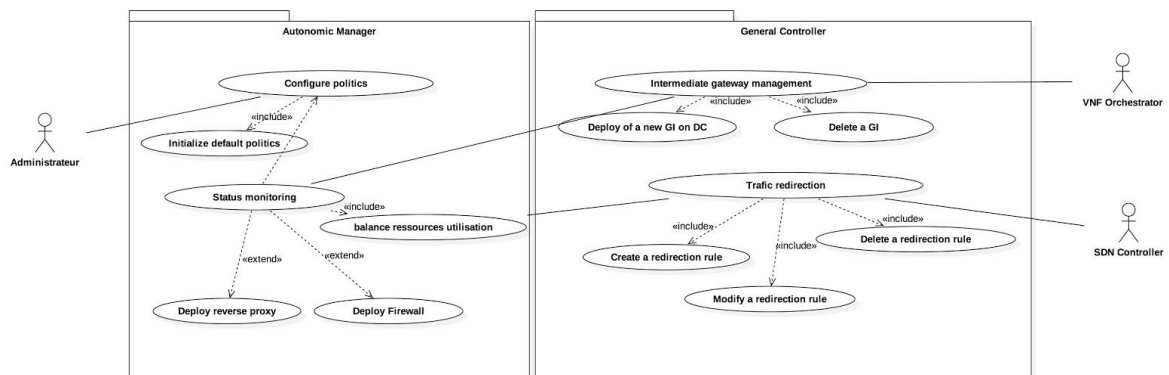
Une autre fonction présentée dans le modèle IBM concerne la capacité de self-healing  
[DES IDÉES ???]

Dans le cadre de notre problématique, la fonction de **self-protecting** ne paraît à première vue pas particulièrement pertinente. Cependant, afin de proposer l'assurance d'une qualité de service continue et optimale, il convient de prendre aussi en compte l'action d'acteurs extérieurs au système, potentiellement dangereux quant au bon fonctionnement de ce dernier. Ainsi, des menaces de flooding par exemple pourraient venir déstabiliser la plateforme. Le système que nous proposons repose sur le déploiement de reverse proxy avec fonction de cache qui contribuent par la même occasion à une amélioration du temps de réponse du système sur certaines requêtes. Ainsi, certaines informations peuvent être conservées au niveau du reverse proxy durant un temps raisonnable (à définir selon le type de données et le contexte d'utilisation) afin d'éviter à certaines requêtes (celles renvoyées à cause d'une perte par exemple) de se propager jusqu'aux gateway finales.

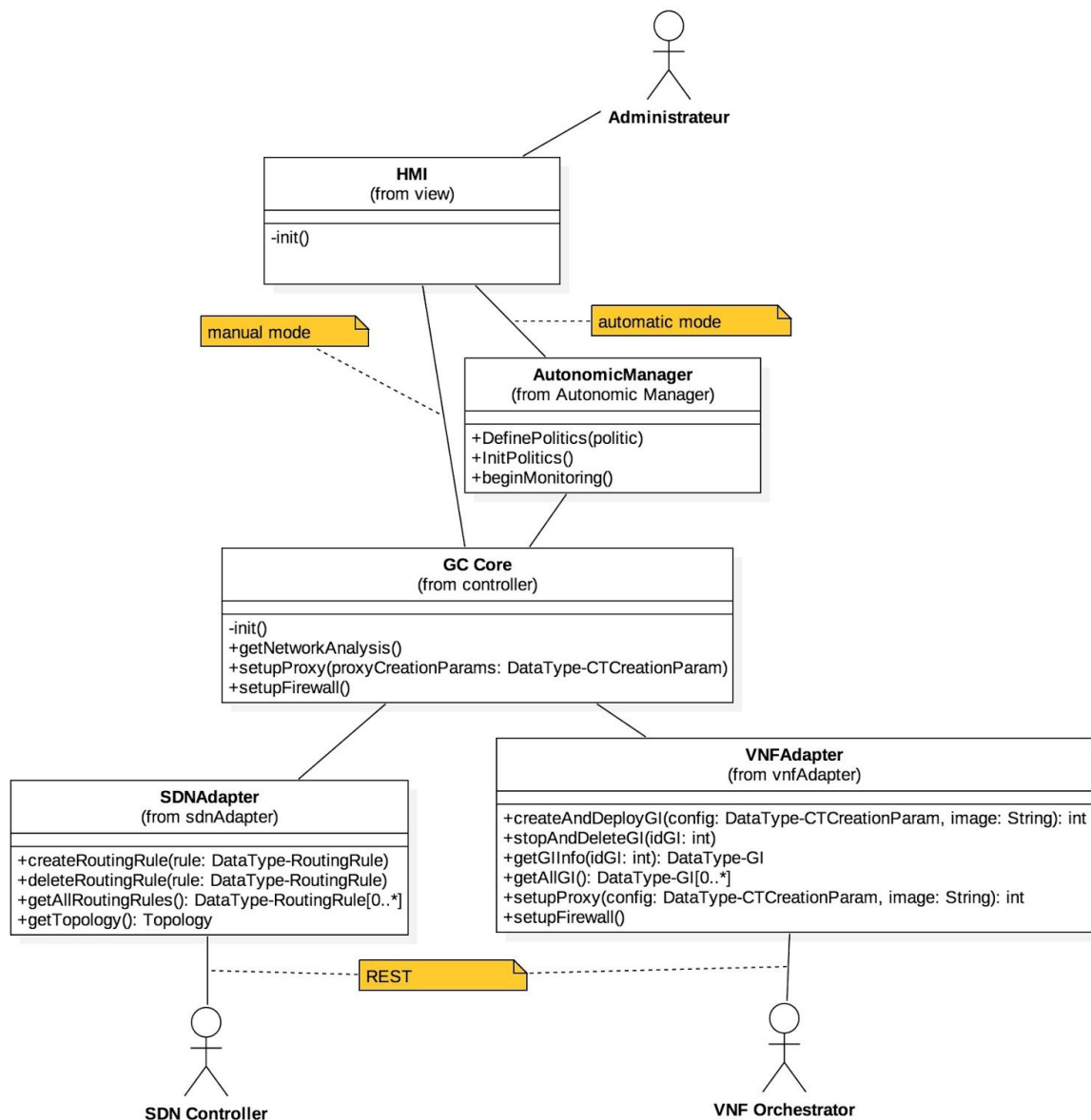
Une autre possibilité consiste à déployer un firewall lorsque le système de monitoring détecte un comportement suspect au niveau du réseau.

Arrivé à ce niveau d'auto-gestion, il existe un intérêt certain à l'implémentation d'une solution d'apprentissage permettant au système d'assimiler et d'utiliser les données collectées par le monitoring réalisé afin de réagir plus rapidement aux incidents ou encore de les anticiper par une analyse plus approfondie.

### Diagramme des uses cases:



**Diagramme des structures composites:**



### **Use case 1 : Initialisation des politiques par défaut du manager automatique**

Acteurs : Manager automatique, GC Core, Administrateur via l'interface graphique

Description : Le système mis en place doit être en mesure d'initialiser les politiques par défaut permettant au manager automatique de réguler le réseau. Cela afin de pouvoir analyser le réseau sans que l'administrateur n'ait à entrer ces politiques au préalable.

Objectif: Initialiser de façon automatisée les politiques par défaut du manager automatique.

Aperçu : Le système va lancer une période d'analyse de 3 min afin de définir les valeurs par défaut des métriques à analyser. Les métriques étant le nombre de paquets sortants pour les gateways finales, le nombre de requêtes faites par le serveur et le pourcentage d'utilisation du CPU pour les gateways intermédiaires. Cela lui permettra de définir la valeur moyenne acceptable pour ces différentes métriques et la valeur maximum acceptable (valeur maximum = valeur moyenne + 20%), qui si elle est dépassée entraînera la création d'une alerte.

Déclencheurs : L'administrateur lance l'interface graphique pour la première fois.

Pré-conditions : Le réseau est dans un état considéré comme normal (i.e. sans phase d'incident)

Post-conditions : Les valeurs par défaut sont affichées sur l'interface graphique et éditables par l'administrateur.

Déroulement des événements : Actions de l'acteur et réponse du système

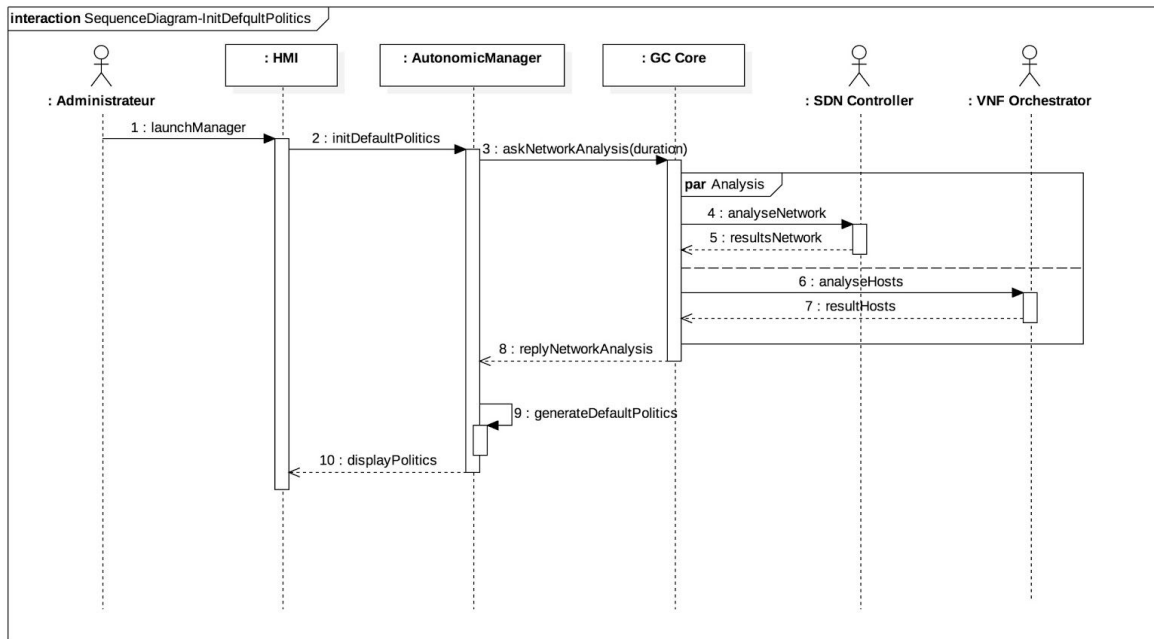
Action de l'acteur :

- L'administrateur lance l'interface graphique

Réponse du système :

- Actions du manager automatique :
  - Le manager automatique lance la période d'analyse du réseau et transmet ses résultats au GC Core
- Actions du GC Core :
  - Le GC Core enregistre les valeurs des métriques par défaut
- Actions de l'interface graphique :
  - L'interface graphique notifie l'administrateur du succès de la période d'analyse et affiche les valeurs des métriques par défaut

Diagramme des séquences:



## Use case 2 : Définition des politiques du manager automatique par l'administrateur

Acteurs : L'administrateur, IHM, Manager automatique

Description : Le système peut avoir une liste des politiques définies par l'administrateur.

Objectif : Guider le comportement du manager automatique.

Aperçu : L'administrateur peut construire des politiques concernant l'état des gateways intermédiaires, l'état du système... Celles-ci vont remplacer celles définies initialement par le système. Le manager automatique va prendre en considération ces politiques pour prendre des décisions de création/suppression de Gateways intermédiaires, modifier les règles de redirections, implémenter ou adapter d'autres réponses du systèmes disponibles telles que le déploiement du Firewall.

Déclencheurs :

- L'administrateur ouvre le panel d'administration et clique sur "Edit" pour modifier des politiques.

Pré-conditions : N/A

Post-conditions : N/A

Action de l'administrateur :

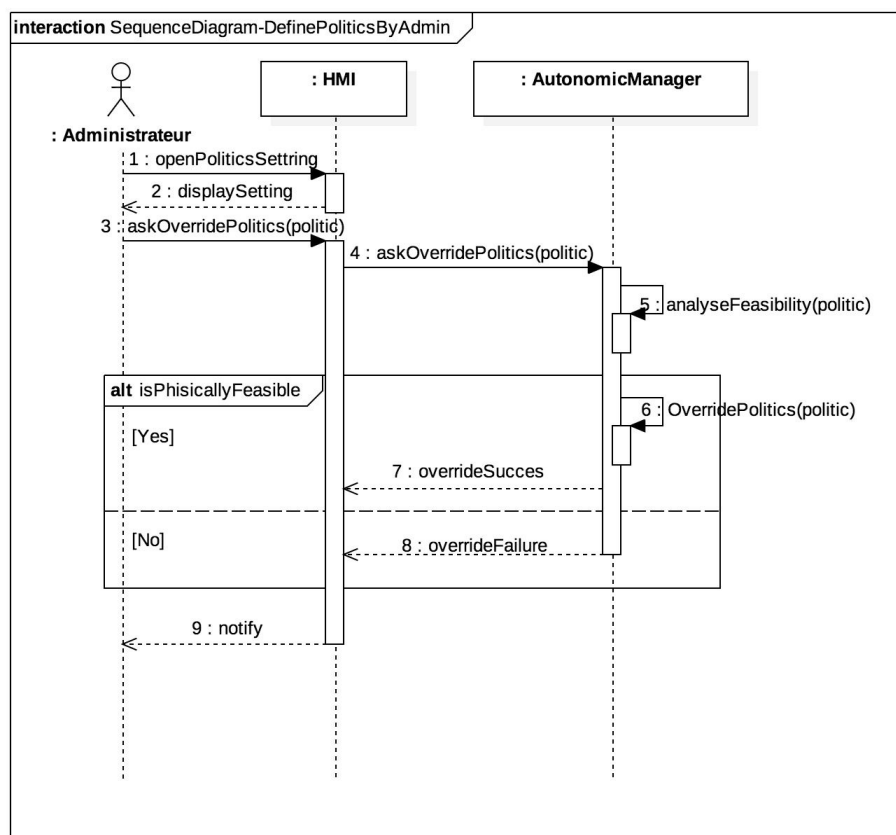
- L'administrateur ouvre le panel de configuration et clique sur "Add" ou "Edit" d'une politique.

- L'administrateur choisit dans les menus déroulants jusqu'à ce qu'il construise une politique (pour quelle(s) gateway(s), pour quelle métrique, quelle est son/ses contrainte(s))
- L'administrateur confirme son choix en cliquant sur le bouton "Confirmer"

Réponse du système :

- IHM
  - L'IHM affiche les politiques du système
  - L'IHM affiche des menus déroulants pour que l'administrateur puisse construire la/les politique(s) désirée(s)
  - L'IHM envoie ces politiques au manager automatique
  - L'IHM attend la réponse du manager automatique pour l'afficher
- Manager automatique :
  - Le manager automatique reçoit une requête de création/modification/suppression de politique
  - Le manager automatique analyse si cette demande est applicable ou pas
  - Le manager met à jour ses contraintes et ses processus de décision si besoin pour appliquer ses contraintes
  - Le manager automatique envoie la réussite ou non de cette redéfinition de politiques. Si cette action n'a pas réussi, le Manager Automatique renvoie la cause de l'échec (ambiguïté avec l'ancienne règle, valeur illégale...)

Diagramme de séquence:



### **Use case 3 : Le Manager automatique monitore l'état du système et actionne des réponses si nécessaire.**

Acteurs : Manager automatique, GC Core, IHM

Description : Le Manager automatique monitore l'état du système et agit en conséquence de son analyse

Objectif : Améliorer le système selon les politiques définies

Aperçu : Le Manager automatique monitore l'état du système dont principalement celui les Gateway Initiales et les Gateways finales. Si le manager automatique détecte une anomalie ou une amélioration possible vis-à-vis des politiques définies, le manager va demander au GC Core d'effectuer des actions.

Déclencheurs : Fin d'initialisation des politiques par défaut

Pré-conditions : Des politiques par défaut sont définies

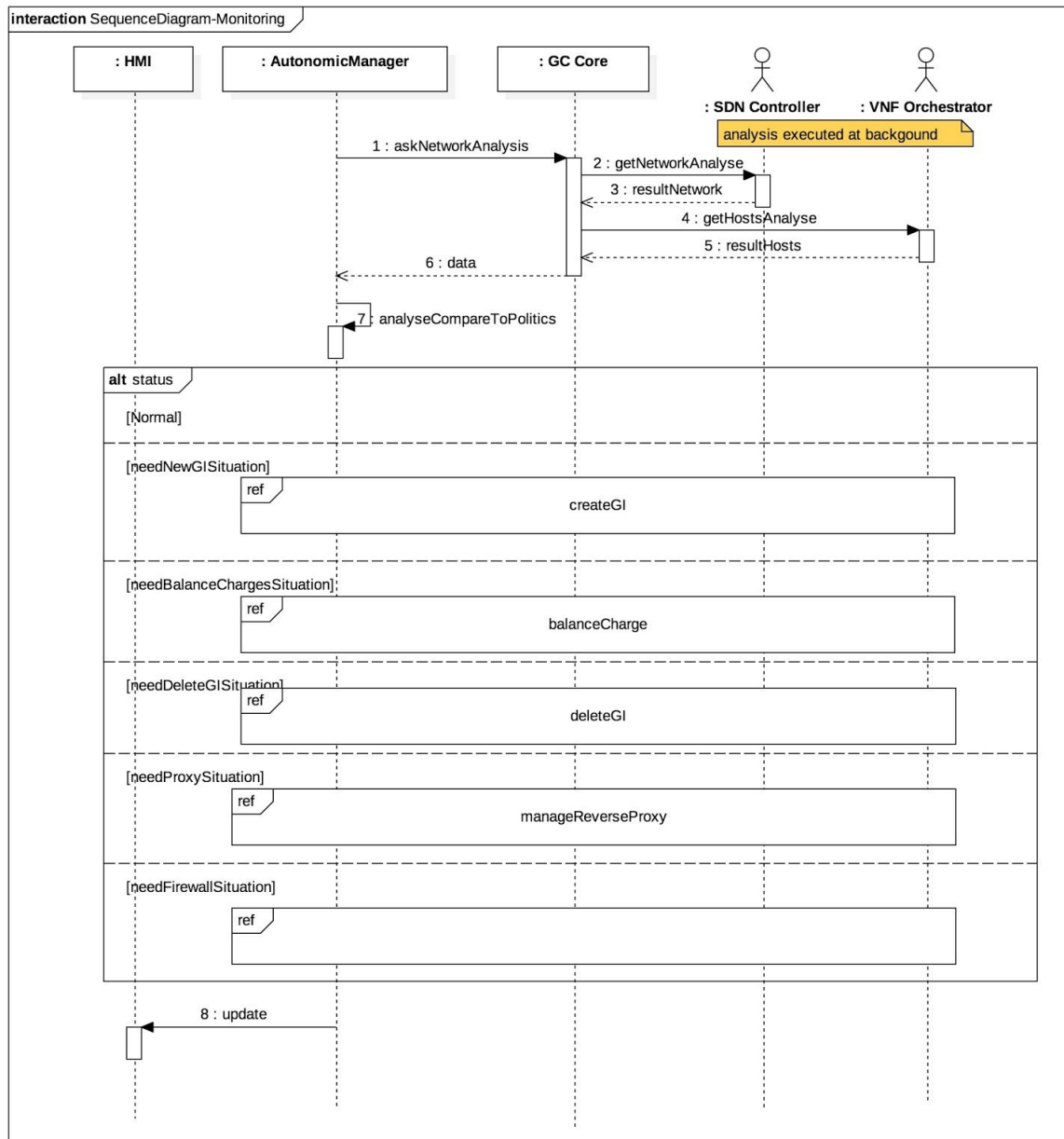
Post-conditions : N/A

Réponse du système :

- Manager automatique :
  - Le manager automatique effectue périodiquement des observations du système global et les stocke dans sa base de connaissances si besoin
  - S'il détecte une anomalie :
    - Si une des GI est trop chargée par rapport à la valeur moyenne espérée ou dépasse la valeur maximale, le manager automatique va voir si un équilibre de charge est possible et s'il résout ce problème. Si l'équilibre de charge n'est pas possible ou qu'il ne résout pas le problème, une nouvelle Gateway intermédiaire sera créée, la moitié des charges des GI surchargées seront redirigées vers la nouvelle GI
    - Si une des GI est trop vide par rapport à la valeur moyenne espérée, et qu'après un calcul la suppression de cette GI n'entraîne pas la surcharge du système, le manager automatique va demander au GC Core de supprimer cette GI en question, et de faire un équilibrage des charges par la suite.
    - Si une GF envoie beaucoup de trames par rapport à son taux d'envoi normal, le manager automatique demande au GC Core de créer une nouvelle GI et de rediriger les paquets concernant cette GF vers la nouvelle GI. Si le nombre de trames dépasse la limite définie dans les politiques, le manager automatique demande au GC Core d'ajouter la fonctionnalité de Firewall pour cette GF.

- Si une GI tombe en panne, il est possible de rediriger tout les trafics vers une autre GI disponible. Si la redirection n'est pas possible, il faut créer une autre GI. Le Manager automatique renvoi un signal d'alerte à l'IHM pour informer l'administrateur de cette anomalie

Diagramme de séquence:



#### Use case 4 : Déploiement d'une gateway intermédiaire sur le DC

Acteurs : Manager automatique, GC Core, Datacenter

Description : Le système mis en place doit être en mesure de déployer automatiquement une gateway intermédiaire. En effet, lorsque le système constate une dépréciation des



qualités de services, il peut déployer une gateway intermédiaire afin de rétablir les qualités de services initiales.

Objectif : Déployer une gateway intermédiaire sur décision du manager automatique.

Aperçu : Le système reçoit une alerte du manager automatique vis à vis de la dégradation de qualité de services et si la politique de décision correspond à l'alerte alors le système va déployer automatiquement une nouvelle gateway intermédiaire. Le déploiement et les actions suivantes seront effectués en mode "boîte noire" vis à vis de l'opérateur. Le système n'aura alors plus qu'à vérifier que les qualités de services soient de nouveau acceptables.

Déclencheurs : Le système reçoit une alerte correspondant à la politique de décision correspondant à ce use case.

Pré-conditions : Un snapshot de la gateway intermédiaire aura été créé au préalable et stocké afin d'être accessible par le Contrôleur général. Un data-center aura été créé au préalable afin de permettre le déploiement des gateway intermédiaires.

Post-conditions : La réussite ou non du déploiement est loguée à partir de la réponse du datacenter. En cas de succès, la nouvelle gateway est ajoutée à la liste des gateway déployées. En cas d'échec, la nouvelle gateway n'est pas sauvegardée.

Déroulement des événements : Actions de l'acteur et réponse du système

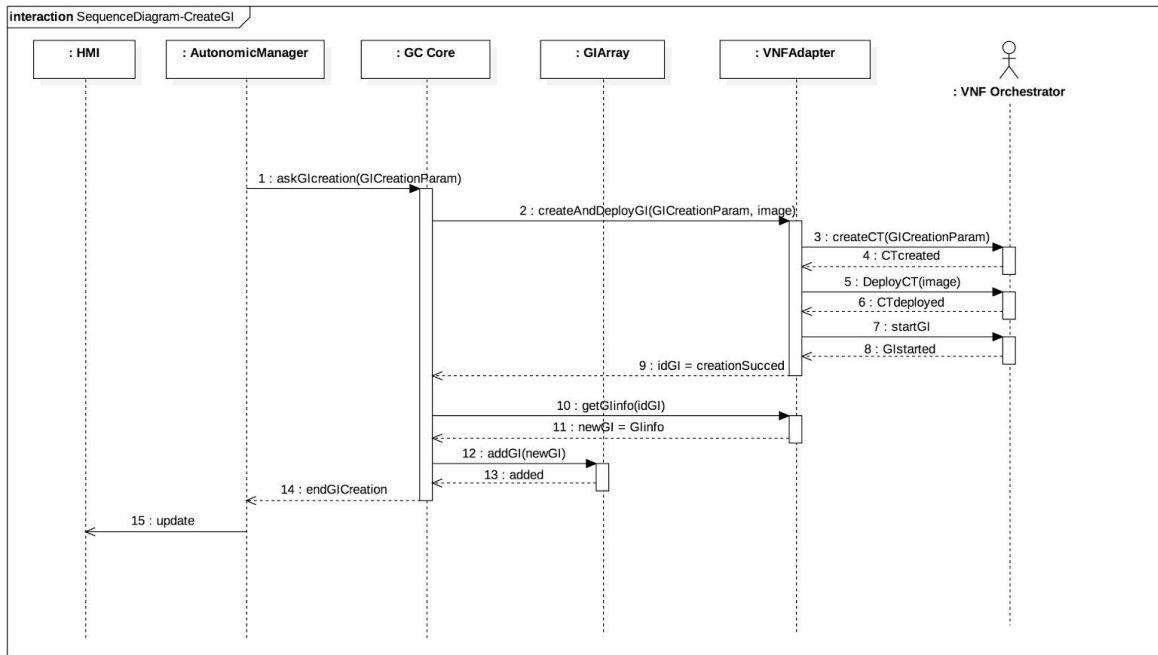
Action de l'acteur :

- Le manager automatique lève une alerte et fait exécuter au système la solution correspondante

Réponse du système :

- Actions du Contrôleur général:
  - Le contrôleur général accède à l'image de la gateway à déployer et instancie cette gateway sur le data-center prévue à cet effet.
  - Si le déploiement est un succès, alors les informations de cette gateway intermédiaire sont stockées dans la liste des gateway.
- Actions du conteneur :
  - Le data-center renvoie une réponse OK si le déploiement s'est déroulé avec succès, et not OK sinon. Le VNF Orchestrateur transmet ensuite cette réponse au Général Controller.

Diagramme de séquence:



## Use case 5: Equilibrer l'utilisation des ressources en agissant sur les règles de redirection

Acteurs : Manager automatique, GC Core, SDN Contrôleur, Réseau étendu SDN

Description : Le système mis en place doit être en mesure de pouvoir agir sur les règles de redirection afin d'optimiser l'utilisation des ressources et répondre aux politiques prédéfini.

Objectif : Opérer la redirection du trafic de la gateway finale vers la gateway intermédiaire et de la gateway intermédiaire vers le serveur applicatif.

Aperçu: Afin de bien utiliser tous les gateway intermédiaire disponibles, le système doit être en mesure de modifier les règles de routages afin de rediriger le trafic internet. Cela permettra aux paquets dont la source/destination est la gateway finale du LAN d'être redirigés vers la gateway intermédiaire choisie. Les qualités de services seront donc améliorées.

Déclencheurs :

- Le Manager automatique décide qu'il y a une équilibrage de charge à faire

Pré-conditions : Au moins 2 gateway intermédiaire (gateway initiale incluse) sont disponibles

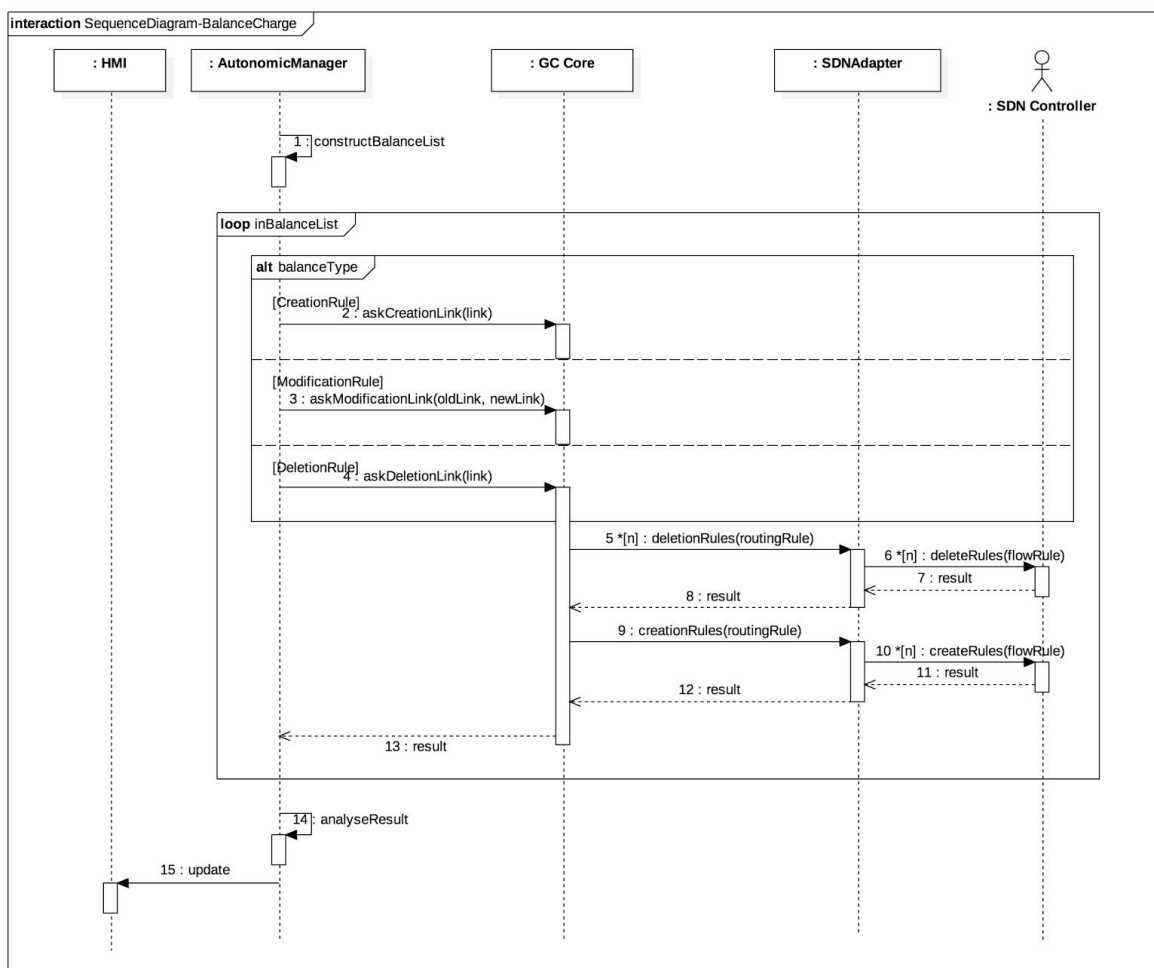
Post-conditions : Mise à jour de l'interface graphique en conséquence

Déroulement des événements : Actions de l'administrateur et réponse du système

Réponse du système :

- Manager automatique :
  - Le manager automatique constate un besoin d'équilibrage des charges
  - Le manager automatique décide de créer, modifier, supprimer certaines règles de redirection, et transmet ces demandes au GC Core
  - Le manager reçoit les résultats de la redirection
  - Le manager informe l'IHM de l'état du système
- IHM :
  - Une fois informée par le manager automatique, l'IHM se met à jour
- GC core :
  - Traitement des demandes de création, modification, suppression des règles de redirections données par le Manager automatique

Diagramme de séquence:



## Use case 6 : Supprimer une gateway du data-center

Acteurs: Manager automatique, GC Core, data-center

Description : Le système mis en place doit être en mesure de supprimer de façon automatique une gateway intermédiaire. En effet, lorsque le manager automatique constate que les qualités de services sont revenues à la normale et que la gateway n'est plus nécessaire, le système peut supprimer une gateway intermédiaire afin de réduire la dépense de ressources inutile par le data-center.

Objectif : Limiter l'utilisation des ressources du data-center.

Aperçu : Le système reçoit une alerte du manager automatique notifiant le fait que les qualités de services sont revenues à la normale. Le système va supprimer automatiquement la nouvelle gateway intermédiaire. La suppression et les actions suivantes seront effectués en mode "boîte noire" vis à vis de l'opérateur.

Déclencheurs : Une alerte notifiant que les qualités de services sont revenues à la normale est reçue par le système

Pré-conditions : La gateway cible est déployée et accessible au sein du système.

Post-conditions : La gateway cible n'apparaît plus dans la topologie du réseau.

Déroulement des événements : Actions de l'acteur et réponse du système

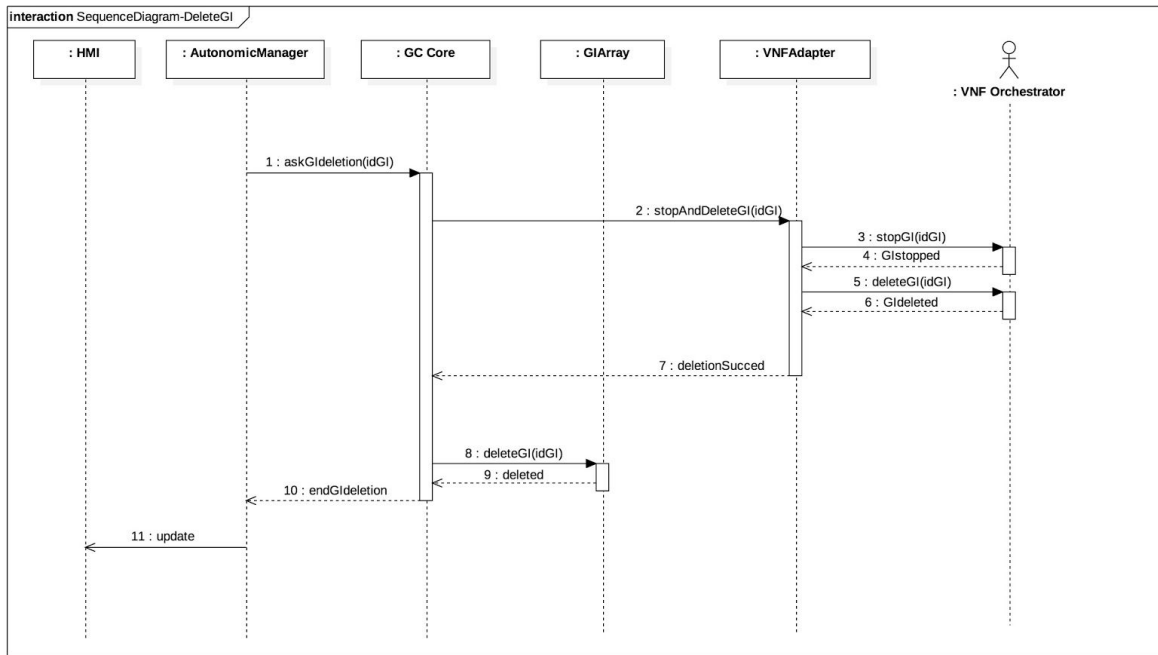
Action de l'acteur :

- Le manager automatique lève une alerte, fait modifier les règles de redirections si besoin et fait exécuter au système la suppression

Réponse du système :

- Actions du Contrôleur général :
  - Le contrôleur général supprime via l'orchestrateur VNF la gateway cible.
  - Si la suppression est un succès, alors les informations de cette gateway intermédiaire sont supprimées de la liste des gateway déployées.

Diagramme de séquence:



## Use case 7 : Déploiement d'un reverse proxy sur le Datacenter

Acteurs : Manager Automatique, Contrôleur général, Datacenter.

Description : Le déploiement d'un reverse proxy proposant une fonction de cache, devant une gateway en contact avec le switch lié au serveur applicatif, permet d'éviter une surcharge du réseau en amont. En effet, dans le cas d'une perte de paquets sur des données récurrentes entre le serveur applicatif et la gateway, il est par exemple intéressant de conserver en cache les données récurrentes afin d'éviter de propager la requête jusqu'au dispositif IoT concerné. De plus, ce dispositif permet aussi de prévenir d'éventuelles attaques de type DDoS.

Objectif : Déployer un reverse proxy proposant un service de cache.

Aperçu : Le système doit être en mesure de créer une politique de cache permettant de limiter le nombre de requêtes propagées jusqu'au device ciblé.

Déclencheur : L'Autonomic Manager décide que la situation actuelle nécessite le déploiement d'un reverse proxy.

Pré-conditions : Un snapshot du reverse proxy aura été au préalable créé et stocké afin d'être accessible par le GC Core. Un datacenter aura été créé afin de permettre le déploiement du reverse proxy. Les politiques de cache sont définies.

Post-conditions : La réussite ou non du déploiement est loguée à partir de la réponse du datacenter. En cas de succès, le reverse-proxy est ajouté à la liste des instances VNF déployées. En cas d'échec, le nouveau reverse proxy n'est pas sauvegardé.

Déroulement des évènements :

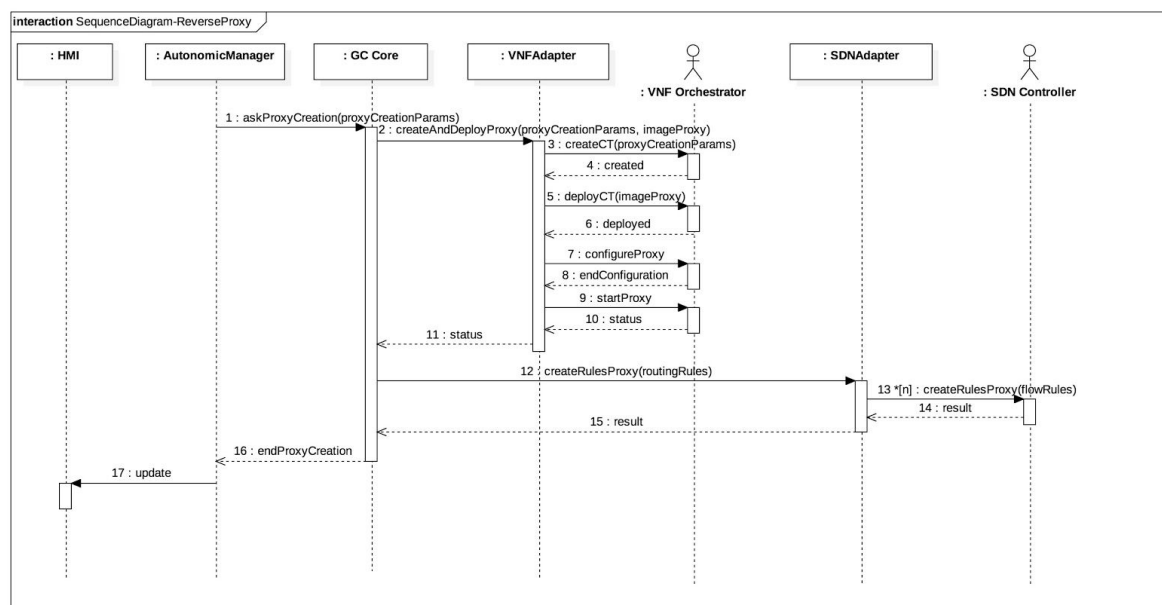
Action de l'Autonomic Manager :

- L'Autonomic Manager lève une alerte.
- L'Autonomic Manager détermine la politique de cache à mettre en place pour améliorer la situation.
- L'Autonomic Manager décide de déployer un reverse proxy et confie cette tâche au GC Core.

Réponse du système :

- Actions du GC Core :
  - Le GC Core accède à l'image du reverse proxy à déployer et l'instancie sur le Datacenter.
  - Le GC Core réalise la configuration nécessaire pour satisfaire la politique de cache demandée par l'Autonomic Manager.
  - Si le déploiement se déroule correctement, les informations du reverse proxy sont stockées dans la liste des VNF déployées
- Actions du Datacenter :
  - Le datacenter renvoie une réponse OK si le déploiement s'est déroulé correctement, et NOT OK sinon. Le VNF Orchestrator transmet ensuite cette réponse au Contrôleur Général.

Diagramme de séquence:



## Use case 8 : Déploiement d'un firewall sur le DC

Acteurs : Manager Automatique, GC Core, Datacenter

Description : Le système doit permettre le déploiement automatique d'un Firewall. En effet, lorsque le système détecte une anomalie dans les couches proches du serveur applicatif, cette dernière peut être la source d'une perturbation du réseau en amont.

Objectif : Mettre en place sur décision du Manager Automatique une politique discriminante.

Aperçu : Le système reçoit une alerte du Manager Automatique qui l'informe d'une activité anormale sur le réseau. La raison peut provenir d'une simple forte hausse de trafic mais aussi d'un comportement suspect. Dans chacun des deux cas, la situation nécessite le déploiement d'un Firewall afin d'appliquer une politique discriminante sur les data en transit.

Déclencheurs : Le Manager Automatique décide que la situation actuelle nécessite le déploiement d'un Firewall.

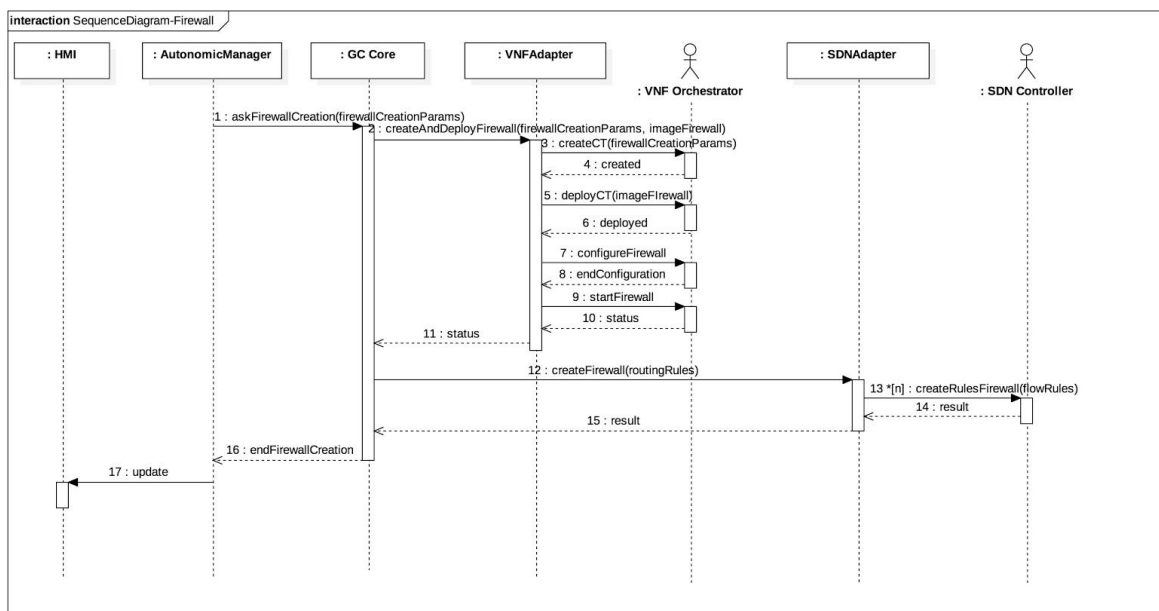
Pré-condition : Un snapshot du Firewall aura été au préalable créé et stocké afin d'être accessible par le contrôleur général. Un datacenter aura été créé afin de permettre le déploiement du Firewall. Les politiques de sécurité liées aux attaques DDOS sont définies.

Post-conditions : La réussite ou non du déploiement est loguée à partir de la réponse du Datacenter. En cas de succès, le nouveau Firewall est ajouté à la liste des instances VNF déployées. En cas d'échec, le nouveau Firewall n'est pas sauvegardé.

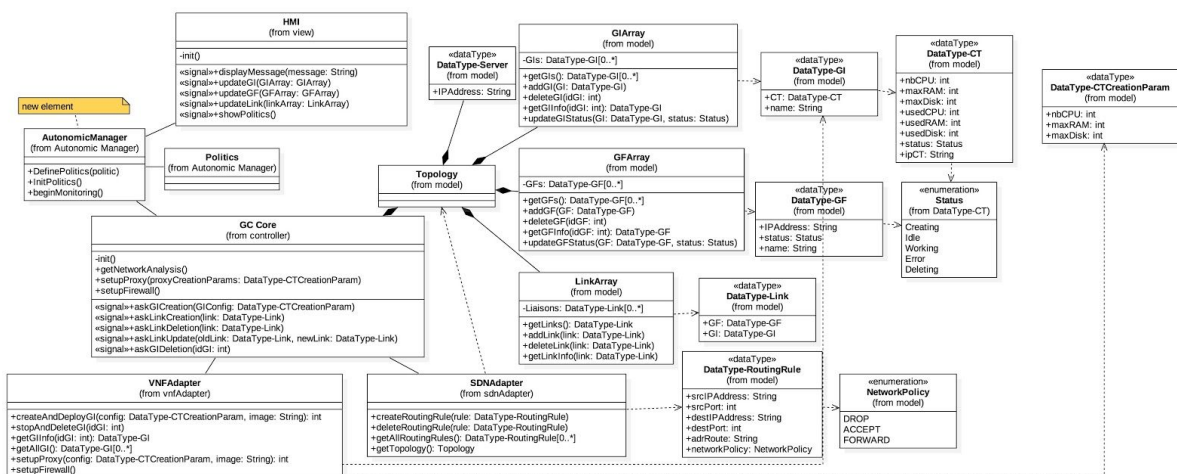
Déroulement des évènements :

- Action du Manager Automatique:
  - Le Manager Automatique lève une alerte.
  - Le Manager Automatique détermine la politique à mettre en place pour améliorer la situation.
  - Le Manager Automatique décide de déployer un firewall et confie cette tâche au GC Core.
- Actions du Contrôleur Général :
  - Le GC Core accède à l'image du firewall à déployer et l'instancie sur le Datacenter
  - Le VNF Adapter réalise la configuration nécessaire pour satisfaire la politique requise par le Manager Automatique
  - Si le déploiement se déroule correctement, les informations du reverse proxy sont stockées dans la liste des VNF déployées
- Actions du Datacenter :
  - Le datacenter renvoie une réponse OK si le déploiement s'est déroulé correctement, et NOT OK sinon. Le VNF Orchestrateur transmet ensuite cette réponse au GC Core.

Diagramme de séquence:



### Diagramme des classes:



## Améliorations possibles

Lorsque nous avons réalisé le travail de conception, nous l'avons réalisé en considérant le temps imparti pour l'implémentation. Nous n'avons donc pas extrapolé la conception plus que ce que nous aurions eu effectivement le temps de réaliser.

C'est pourquoi nous avons décidé de consacrer la dernière partie de ce rapport aux améliorations possibles que nous pourrions apporter à ce système.



Afin de le rapprocher un peu plus de la définition d'Automatic Computing, nous pourrions ajouter une fonctionnalité de machine learning qui permettrait au système d'adapter les politiques.

Cela modifierait le fonctionnement présent dans l'étape 2 puisque ce changement nécessite une phase d'apprentissage non présente dans la conception actuelle. Il faudrait ajouter la possibilité à l'administrateur de venir prendre la main sur le système et d'ajouter/supprimer des GI, firewall, etc. A chaque fois que le système subirait cette reprise en main, il analysera l'état du système et l'action qui a été faite pour apprendre et à terme, déduire un nouveau comportement.

Par exemple, dans le cas de l'ajout d'une GI, le système réduira le seuil maximum acceptable au vu des valeurs du moment de la reprise en main.

Nous pensions à rajouter un principe que nous qualifions de principe de sûreté. En effet, nous pouvons imaginer que la dégradation des qualités de service n'est pas un phénomène que instantané mais qu'il peut aussi s'effectuer de façon croissante et dans un laps de temps plus grand.

Ainsi, lorsque le système détectera que les qualités de service se situent dans une zone acceptable mais bientôt inacceptable depuis trop longtemps, il estimera que la nécessité de déployer une solution devient réelle. Cela se traduira par le fait de déployer/rallumer une GI (en fonction de la solution choisie) par sécurité afin d'accélérer le déploiement de la réponse si le besoin se traduit effectivement.

1. Load balancer, pour 1 GF peut utiliser 2 GI (? création d'une nouvelle GF)