

BUILDING TOGETHER TEAM SPIRIT  SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET	Projet NGIM lot 3 Ad Server Dossier Architecture Hébergement	 Diffusion interne SG
---	---	---

# NGIM lot 3 – Ad Server

## Dossier d'Architecture Hébergement (DAH)

Nom	NGIM lot 3 – Ad Server
IRT	A5142
Trigramme	DCA
Criticité métier (STAMP)	Source « Questionnaire d'évaluation de la Sensibilité »
Ecolience	Référence vers les documents « ecolience »
Demande client	CVTI

**Version : 1.2**

**Statut : Validé**

BUILDING TOGETHER <b>TEAM SPIRIT</b> SOCIETE GENERALE ITIM – GTS/RET	<b>Projet NGIM lot 3 Ad Server</b> <b>Dossier Architecture Hébergement</b>	 Diffusion interne SG
---	---	---

## FICHE DE CONTROLE DU DOCUMENT

### Caractéristiques du document

<b>Statut</b>	Document Initial / final
<b>Réf. Fichier</b>	DAH application DCA – modele std_v2.8.doc

### Création et suivi du document

Version	Créé le	Auteur	Approuvé le	Par
0.1	14/06/2016	Mejdoub BENBERNOU Peter-Jim PAMEOLE		
0.3	14/06/2016	Peter-Jim PAMEOLE		
0.4	14/06/2016	Mejdoub BENBERNOU		
0.5	29/06/2016	Peter-Jim PAMEOLE		
0.51	30/06/2016	Mejdoub BENBERNOU		
0.6	22/07/2016	Peter-Jim PAMEOLE		
0.7	26/07/2016	Peter-Jim PAMEOLE		
0.8	27/07/2016	Peter-Jim PAMEOLE		
0.9	01/08/2016	Peter-Jim PAMEOLE		
0.91	03/08/2016	Peter-Jim PAMEOLE		
0.92	08/08/2016	Mejdoub BENBERNOU		
0.93	09/08/2016	Peter-Jim PAMEOLE		
1.0	17/08/2016	Mejdoub BENBERNOU Peter-Jim PAMEOLE	19/08/2016	RET/APS
1.1	26/08/2016	Peter-Jim PAMEOLE		
1.2	11/01/2017	Mejdoub BENBERNOU Peter-Jim PAMEOLE	13/01/2017	RET/APS

### Intervenants sur le projet

Entité (ou Société)	Domaine de responsabilité dans le projet	Nom
ITIM/CSB/DCP	Maitrise d'Ouvrage	Ugo MANCONI
ITIM/CSB/DCP	Maitrise d'Œuvre	Dominique NOJEAN Sandrine MALLET Arnaud DECUSSY
ITIM/ASI/SDC	Support Architecture DSI	Thibaut CATHENOZ Philippe DUBOSC
ITIM/ASI/ASE	Support Architecture Cloud DSI	Bruce VINCHON Adrien HOULLIER
ITIM/ASI/SRO	Sécurité et Risques Opérationnels ITIM	Philippe LE MOIGNE Anton SHAKINKO JAD JOUMLAT Raphaël MOLLIMARD
RESG/GTS/RET/API	AM	Jean-Christophe LEJOUX
RESG/GTS/RET/API	Programme Go2AWS	Vincent HORNAIN

BUILDING TOGETHER TEAM SPIRIT  SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET	<b>Projet NGIM lot 3 Ad Server</b> <b>Dossier Architecture Hébergement</b>	 Diffusion interne SG
---	---	---

RESG/GTS/RET/API	Project Manager (SPM)	Isabelle DANCHE (NGIM) Vincent EHRHART (Go2AWS)
RESG/GTS/RET/API	RT	Hervé PETIT
RESG/GTS/RET/APS/ARC	Architecture d'Hébergement GTS/RET	Mejdoub BENBERNOU (NGIM) Gilles STENGER (Go2AWS) Peter-Jim PAMEOLE(NGIM) Jean-Christophe MEYNARD (COE)
RESG/GTS/RET/APS	OSM (sécurité et risques opérationnels)	Sébastien LEFEVRE
RESG/GTS/STP/OSM	OSM (sécurité et risques opérationnels)	Martial RODRIGUEZ Vincent FERRIE
RESG/GTS/RET/MDB/MFA	Expert Infrastructure Middleware	Abdelmajid BOUAZZA Laurent VERBIESE
RESG/GTS/RET/MDB/DBA	Expert Infrastructure Base de données	Philippe GUFFROY
RESG/GTS/RET/OPM	Expert Infrastructure Sécurité	Tiburce GIROUX
RESG/GTS/RET/INF/Linux	Expert Infrastructure Linux	DANY AFAHOUNKO
RESG/GTS/RET/INF/VCD	Expert Infrastructure Virtualisation	Sylvain BALLARD
RESG/GTS/RET/INF/SBA	Expert Infrastructure Sauvegarde	Emmanuel BOVE
RESG/GTS/RET/MDB/MFI	Expert Infrastructure Supervision	Ségolène JIMENEZ
RESG/GTS/TFO/SIS	Architecte réseaux	Lucas BARRIERE
RESG/GTS/TFO/CTY	Expert Infrastructure réseaux	Yoan ALLAIN Joel LUBIN Sébastien BERY
RESG/GTS/TFO/CRM	CRM TFO BDDF	Rached BEN MAHMOUD

#### Liste de diffusion

Entité	Nom des destinataires	Objet de la diffusion
	Intervenants du projet	Information
RESG/GTS/RET/APS	G. RIHANA	Validation
RESG/GTS/RET/DIR	Jean CADROY	Information
RESG/GTS/RET/APS	T ZULIAN, C DUMOULIN, JA EUDE, F. PAUMIER, <a href="mailto://PAR-Ret-Aps-lac">mailto://PAR-Ret-Aps-lac</a>	Information
RESG/GTS/RET/MDB	Thierry BOURDON	Information

BUILDING TOGETHER TEAM SPIRIT  SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET	Projet NGIM lot 3 Ad Server Dossier Architecture Hébergement	 Diffusion interne SG
---	---	--

RESG/GTS/RET/MDB	Dominique BISSONNIER	Information
RESG/GTS/RET/MDB	Leijiong SHAN	Information
RESG/GTS/RET/API	Denis CHOUTEAU-CLERC	Information
RESG/GTS/TFO/CRM	R. BEN MAHMOUD	Information
RESG/GTS/RET/INF	Corinne GEHANNIN	Information
RESG/ GTS/STP/OSM	Laurent PONS, Gérard LE COMTE	Information
RESG/GTS/ATO		Information
RESG/GTS/EUS/ENG		
	ME	Validation
	RSSI Fonctionnelle	Information

### CHARTE COULEUR, A UTILISER AVEC MODERATION

EN **ROUGE**, LES POINTS NON STANDARDS

EN **FLUO**, LES POINTS NON CLOS AVANT PRESENTATION AU CVT-Q

### FICHE DE SYNTHESE DU DOCUMENT

Application IRT / Trigramme	<b>NGIM Lot3 - Ad Server DCA / A5142</b>	
Applications impactées	NGIM Ad server est un service de la banque à distance hébergé chez AWS. Ce service est hors écolience E04A de la B@D (BDDF)	
Typologie Architecture	<b>Web Transactionnel</b>	
Préconisations de GTS <b>non retenues</b> par la ME	Statut : Lister les préconisations non retenues de manière synthétique Les points sont détaillés dans le § « 1.2 vision architecture »	
<b>Description de l'Architecture de production ExaStacks</b>		
Site primaire d'hébergement	<b>Hébergement AWS en Région Irlande sur 2 AZ (zones de disponibilité)</b>	
Site de secours ou secondaire	<b>Hébergement étendu sur 2 AZ (pas de secours hors région)</b>	
Modèle d'architecture de résilience	* <b>2+0 : A/A</b> (* ) n1 + n2 : n1= nombre d'AZ en région, n2= nombre d'AZ hors région	
Modèle de solution de résilience	Robustesse sur 2 AZ en région Irlande <b>Objectif de délai de rétablissement GTS (panne) : Sans objet</b> Le projet sera déployé sur 2 zones de disponibilité en A/A basé sur les services d'autoscaling et de remédiation automatique	
Niveau d'exercice de secours <b>atteignable</b>	Sans objet pour NGIM Ad server (modèle A/A) L'écolience de la B@D est exercisable indépendamment du service NGIM Ad server	
Couche métiers	Basée sur la solution open source Revive AdServer	
Services d'échanges	Sans objet	
Services d'application	Apache / PHP	Ajout
Services Données	Service AWS RDS PostgreSQL	Ajout

 <p>BUILDING TOGETHER TEAM SPIRIT SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET</p>	<p>Projet NGIM lot 3 Ad Server</p> <p>Dossier Architecture Hébergement</p>	 <p>Diffusion interne SG</p>
--	--	--

Services AWS	EC2, EBS, ELB, RDS, Autoscaling Group, CloudWatch, CloudTrail, CloudFormation, Route53, IAM, DirectConnect, VPC, S3	
Zones Cellules Sécurité Réseau (CSR)	SI SG: Cloudcell, PAC/CloudBridge (cible), HELIOS, LGN/N2G Amazon: cIAP, VPC Web, VPC Admin, VPC Tech, DirectConnect	
Systèmes d'exploitation	RedHat Linux 7.2	Ajout
Sécurité / durcissement OS requis	Premium+ et politique selinux	
Ressources Techniques	<p><u>Côté SI SG (CloudCell GTS) :</u></p> <ul style="list-style-type: none"> <li>✓ <u>Infrastructure serveurs pour les servitudes mutualisées tout environnement</u> <ul style="list-style-type: none"> <li>✓ <b>Bastion:</b> 1xVM Factory Medium ( 2vCPU, 4Go RAM )</li> <li>✓ <b>Key Host :</b> 1xVM Factory Medium ( 2vCPU, 4Go RAM )</li> <li>✓ <b>Concentrateur Syslog-NG:</b> 1xVM Factory Medium ( 2vCPU, 4Go RAM )</li> <li>✓ <b>Relais NTP:</b> 1xVM Factory Small ( 1vCPU, 2Go RAM )</li> <li>✓ <b>Supervision:</b> 1x VM Factory Custom (2vCPU, 16Go RAM)</li> </ul> </li> <li>✓ <u>Infrastructure serveurs pour les servitudes par environnement</u> <p><u>Production :</u></p> <ul style="list-style-type: none"> <li>✓ <b>Proxy-HTTP:</b> 1xVM Factory Medium ( 2vCPU, 4Go RAM )</li> <li>✓ <b>Relais HAProxy:</b> 1xVM Factory Medium ( 2vCPU, 4Go RAM )</li> </ul> <p><u>Homologation :</u></p> <ul style="list-style-type: none"> <li>✓ <b>Proxy-HTTP:</b> 1xVM Factory Small ( 1vCPU, 2Go RAM )</li> <li>✓ <b>Relais HAProxy:</b> 1xVM 1xVM Factory Small ( 1vCPU, 2Go RAM )</li> </ul> <p><u>Développement :</u></p> <ul style="list-style-type: none"> <li>✓ <b>Proxy-HTTP:</b> 1xVM Factory Small ( 1vCPU, 2Go RAM )</li> <li>✓ <b>Relais HAProxy:</b> 1xVM 1xVM Factory Small ( 1vCPU, 2Go RAM )</li> </ul> </li> <li>✓ <u>Stockage</u> <ul style="list-style-type: none"> <li>• <u>Stockage SAN L0 :</u> 810 Go pour Dev/Homol/Prod</li> </ul> </li> </ul> <p><u>Côté Amazon AWS:</u></p> <ul style="list-style-type: none"> <li>✓ <u>Production / Homologation:</u> <ul style="list-style-type: none"> <li>✓ <u>VPC Web étendu sur 2 AZ :</u> <ul style="list-style-type: none"> <li>• <b>Load Balancing:</b> Service ELB sur 2 AZ</li> <li>• <b>AdServer promotions:</b> Service EC2 en A/A avec autoscaling group sur 2 AZ</li> <li>• <b>AdServer admin:</b> 1xVM EC2 en A/P sur 2 AZ avec auto-remédiation</li> <li>• <b>Base de données :</b> 1 Service RDS PostgreSQL sur 2 AZ en A/A Hot Standby</li> </ul> </li> <li>✓ <u>VPC Admin étendu sur 2 AZ :</u> <ul style="list-style-type: none"> <li>• <b>1 service EC2 en A/P sur 2 AZ avec auto-remédiation pour chaque servitude AWS (ProtectV Manager, nœud de build, Bastion AWS (Jump Host), Proxy HTTP, Serveur NTP (Relai vers les serveurs NTP Internes Société Générale), Relais syslog (collecte des logs systèmes), images AMI)</b></li> </ul> </li> <li>✓ <u>VPC Tech étendu sur 2 AZ :</u> <ul style="list-style-type: none"> <li>• <b>1 service EC2 en A/P sur 2 AZ avec autoremediation pour le référentiel des packages OS et applicatifs</b></li> </ul> </li> </ul> </li> </ul>	
Offres GTS	VM Factory (Cloudcell)	

BUILDING TOGETHER TEAM SPIRIT  SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET	Projet NGIM lot 3 Ad Server Dossier Architecture Hébergement	 Diffusion interne SG
---	---	--

Servitudes GTS	Supervision Patrol Proxification des flux HTTP Centralisation des Logs (Log4All) Synchronisation NTP Centralisation des clefs HSM Bastion SSH	
Ressources réseaux	<i>Côté SI SG (GTS) :</i> <ul style="list-style-type: none"> <li>Chaine d'accès HELIOS (chaîne d'accès au contenu publicitaire LGN&amp; N2G)</li> <li>Accès aux ressources AWS via le PAC</li> </ul> <i>Côté AWS :</i> <ul style="list-style-type: none"> <li>cIAP</li> <li>DirectConnect</li> </ul>	
Poste de Travail	client web PRI International : oui	
Services d'accès	HELIOS, PAC cIAP	Reconduit Nouveau
Processus de livraison des packages applicatifs en production	Recettes Ansible	
Principaux Ecart par rapport à la stratégie ou aux exigences GTS	<b>Domaine</b>	<b>Ecart ? oui/non</b>
	<b>Virtualisation</b>	<b>Non</b>
	<b>Schengen (inclure passeport si écart en annexe)</b>	<b>Sans objet</b>
	<b>Capacité à réaliser des exercices pleine charge ⇔ écosystèmes de données et de flux définis et validés</b>	<b>Non</b>
	<b>RedCat</b>	<b>Non</b>
	<b>Stratégie Datacenter</b>	<b>Non</b>
	<b>Processus de livraison standard</b>	<b>Non</b>

Dans le paragraphe 1.2.2, le récapitulatif des besoins déclinés par offre et par environnement et par site.

<p>BUILDING TOGETHER TEAM SPIRIT  SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET</p>	<p>Projet NGIM lot 3 Ad Server Dossier Architecture Hébergement</p>	<p> Diffusion interne SG</p>
--	---	--

JALONS DU PLANNING		
CVT-I	XX/XX/XXX	
CVT-q / -qa	21/05/16	
CVT-x	XX/XX/XXXX	
Installation en développement	XX/XX/XXXX	
Mise en Homologation-x	22/07/2016	
Mise en Production	30/09/2016	

- ☞ Ce document présente le plan type du Dossier d'Architecture Hébergement (DAH) dont le contenu est sous la responsabilité de GTS/RET/APS.
- ☞ La structure du DAH est sous la responsabilité de l'équipe architecture GTS/RET/APS
- ☞ Le présent document est le résultat de l'étude d'architecture en amont de la CVTq ainsi que des échanges et ateliers ayant eu lieu post CVTq avec la core team NGIM, le COE et les consultants AWS Professional Services.

## TABLE DES MATIERES

<b>1</b>	<b>SYNTHESE .....</b>	<b>12</b>
1.1	CONTEXTE ET ENJEUX DU PROJET .....	12
1.2	VUE MACRO DE LA SOLUTION SUR AWS .....	13
1.3	PERIMETRE .....	13
<b>2</b>	<b>ARCHITECTURE APPLICATIVE NGIM.....</b>	<b>14</b>
2.1	SCHEMA D'ARCHITECTURE APPLICATIVE .....	14
2.2	DESCRIPTION DES COMPOSANTS APPLICATIFS DE NGIM LOT 3.....	14
2.2.1	AD Server – Module promotion .....	14
2.2.2	AD Server – Module Administration.....	14
2.2.3	Base de données PostgreSQL.....	14
2.3	MATRICE DES FLUX APPLICATIFS.....	15
2.4	VOLUMETRIES .....	15
<b>3</b>	<b>CONTEXTE AMAZON WEB SERVICES (AWS) .....</b>	<b>16</b>
3.1	COMPTES AWS .....	16
3.1.1	Définition .....	16
3.1.2	Choix pour NGIM .....	16
3.2	INFRASTRUCTURE D'HÉBERGEMENT AWS .....	17
3.3	ZONE DE DISPONIBILITÉ (AZ).....	18
3.4	CONNECTIVITÉ AWS – SOCIÉTÉ GÉNÉRALE .....	18
3.4.1	Vision globale .....	18
3.4.2	Cloudcell tactique .....	18
3.4.3	Direct Connect.....	19
3.5	VIRTUAL PRIVATE CLOUD (VPC) .....	19
3.5.1	Description.....	19
3.5.2	VPC Mutli-AZ et subnets.....	20
3.5.3	Schéma Comptes/VPC pour NGIM.....	21
3.5.4	Connectivités du VPC .....	21
3.6	SECURISATION DES ECHANGES (NACL ET SECURITY GROUPS).....	24
3.6.1	Network Access Control List (NACL) .....	24
3.6.2	Security Group.....	24
3.6.3	NACL vs Security Group.....	25
3.6.4	Flow Logs.....	25
3.6.5	Règles mises en place pour NGIM lot 3 Ad – server.....	25
3.7	RESOLUTION DES NOMS DE DOMAINES .....	28
3.7.1	Résolution SI SG – AWS.....	28
3.7.2	Route53 : Résolution chez AWS.....	29
3.8	OUTILS D'ADMINISTRATION .....	31
3.8.1	CloudWatch.....	31
3.8.2	CloudTrail.....	32
3.8.3	CloudFormation.....	32
<b>4</b>	<b>ARCHITECTURE RESEAU .....</b>	<b>33</b>
4.1	DESCRIPTION GENERALE .....	33
4.2	MATRICE DE FLUX APPLICATIFS AVEC UNE VISION INFRASTRUCTURE .....	34
4.3	MATRICE DE FLUX TECHNIQUES .....	35
4.4	CINEMATIQUE D'ACCES AUX API AWS .....	36
4.5	CLOUDCELL.....	37
4.6	INTERCONNEXION SOCIETE GENERALE – AWS.....	38
4.7	URBANISATION RESEAU CHEZ AWS.....	39
4.8	INTERCONNEXION INTERNET – NGIM.....	40
<b>5</b>	<b>ARCHITECTURE D'HEBERGEMENT DES SERVITUDES POUR AWS .....</b>	<b>41</b>
5.1	DESCRIPTION GENERALE DES SERVITUDES TECHNIQUES .....	41
5.2	SERVITUDE « PROXY DES FLUX HTTPS » .....	41
5.3	SERVITUDE « COLLECTE DES LOGS SYSTEMES » .....	41



5.4	SERVITUDE « REDIRECTION DES FLUX KEYSTORES » .....	42
5.5	SERVITUDE « BASTION SSH » .....	42
5.5.1	Généralités .....	42
5.5.2	CryptoAuditor : protocoles pris en charges et fonctionnalités .....	42
5.5.3	CryptoAuditor : Gestion des authentifications en mode bastion .....	43
5.5.4	CryptoAuditor : Règles pour les utilisateurs et groupes d'utilisateurs .....	43
5.5.5	CryptoAuditor : Gestion des utilisateurs .....	44
5.5.6	Key Host .....	45
5.5.7	Jump Host (ou Bastion AWS) .....	45
5.5.8	Schéma de la cinématique globale d'accès SSH aux serveurs AWS .....	46
5.6	SERVITUDE « SUPERVISION ET METROLOGIE » .....	47
5.6.1	Principes .....	47
5.6.2	Solution .....	47
5.6.3	Flux .....	48
5.6.4	Point d'attention .....	48
5.7	SERVITUDE « RELAIS NTP » .....	48
5.8	DESCRIPTION DU SOCLE D'HEBERGEMENT DES SERVITUDES .....	49
<b>6</b>	<b>ARCHITECTURE D'HEBERGEMENT DES COMPOSANTS TECHNIQUES .....</b>	<b>51</b>
6.1	ZONE D'HEBERGEMENT DES COMPOSANTS TECHNIQUES .....	51
6.2	SYNTHESE DES RESSOURCES AWS ALLOUEES .....	52
6.3	RESILIENCE DES BRIQUES TECHNIQUES .....	52
6.3.1	Modèle de résilience .....	52
6.3.2	Principes de remédiation .....	52
<b>7</b>	<b>ARCHITECTURE D'HEBERGEMENT DE NGIM .....</b>	<b>53</b>
7.1	DESCRIPTION DES SOCLES D'HEBERGEMENT DES COMPOSANTS TECHNIQUES .....	53
7.1.1	Description des types d'instances AWS .....	53
7.1.2	Synthèse des ressources AWS allouées .....	53
7.2	RESILIENCE DES INSTANCES EC2 .....	53
7.2.1	Solution de remédiation .....	53
7.2.2	Tableau de synthèse de résilience des instances EC2 .....	53
7.3	RESILIENCE DE LA BASE DE DONNEES .....	54
7.3.1	Principes .....	54
7.3.2	Tableau de synthèse .....	54
7.3.3	Schéma du modèle de résilience en homologation et production .....	54
7.4	NIVEAUX DE SERVICE ATTEINTS .....	55
<b>8</b>	<b>DEPLOIEMENT APPLICATIF .....</b>	<b>56</b>
8.1	OBJECTIFS .....	56
8.2	SCHEMA .....	56
8.3	CINEMATIQUE .....	56
8.4	GESTION DU CHANGEMENT OS ET APPLICATIF .....	57
8.4.1	AMI Factory (Usine à images) .....	57
8.4.2	Cinématique détaillée .....	58
8.5	DEPLOIEMENT BLUE/GREEN .....	59
<b>9</b>	<b>MECANIQUES DE REMEDIATION DES INSTANCES EC2 .....</b>	<b>61</b>
9.1.1	Principes .....	61
9.1.2	Critères de remédiation .....	61
9.1.3	Cinématique de remédiation .....	61
9.1.4	Contraintes/Risques Sécurité .....	61
9.1.5	Contraintes/Risques Opérationnels .....	62
<b>10</b>	<b>SECURITE .....</b>	<b>63</b>
10.1	GESTION DES DROITS ET HABILITATIONS .....	63
10.1.1	IAM .....	63
10.1.2	Authentification SAFE sur NGIM Module administration .....	63
10.1.3	Authentification SAFE sur la console AWS .....	63

10.2	SECURISATION DES ECHANGES .....	63
10.2.1	NACL.....	63
10.2.2	Security Groups.....	63
<b>11</b>	<b>EXPLOITABILITE .....</b>	<b>65</b>
11.1	CINEMATIQUE D'ACCES EXPLOITANTS ET ME AUX SERVEURS AWS.....	65
11.2	SUPERVISION .....	65
11.3	METROLOGIE .....	65
11.4	SAUVEGARDE .....	65
11.5	COLLECTE DES LOGS.....	65
11.6	GESTION DU CHANGEMENT.....	65
11.7	GESTION DES INCIDENTS.....	65
<b>12</b>	<b>ECOLIENGE DE NGIM LOT 3.....</b>	<b>66</b>
<b>13</b>	<b>SOLUTION DE REVERSIBILITE.....</b>	<b>67</b>
13.1	DESCRIPTION DE LA SOLUTION D'HEBERGEMENT EN INTERNE.....	67
13.2	CONTRAINTES TECHNIQUES LIEES A LA SOLUTION PROPOSEE .....	68
13.3	CHEMIN DE MIGRATION DEPUIS LE CLOUD AWS.....	68

## INTRODUCTION

L'objet de ce document est de présenter l'architecture technique et les ressources techniques du socle NGIM lot 3 – Ad Server à mettre en œuvre chez AWS et validée par les différents acteurs dans le cadre du programme « Go2AWS ». Ce projet a pour vocation de déployer une infrastructure d'hébergement chez AWS pour ITIM/CSB et exploitée par GTS/RET. Le document contient la liste exhaustive des briques techniques et applicatives (serveurs, RAM, CPUs, urbanisation réseaux données, sécurité, supervision et sauvegarde) à mettre en place pour assurer le fonctionnement, la sauvegarde et le secours de ces infrastructures.

Par analogie avec une démarche projet (ME), ce document représente la conception générale des projets d'implémentation d'infrastructure pour GTS.

La vision globale de l'architecture d'hébergement de l'activité bancaire est décrite dans deux documents :

- ✓ Un DAH par application (le présent document) qui apporte une vision détaillée de l'application et des flux échangés avec les applications / services de premier niveau,
- ✓ un document global, dont le plan type est en cours de définition, décrivant l'écosystème d'hébergement de l'activité bancaire. Ce document est indiqué en page de garde sous la référence « écolience ».

Le terme N/A dans un des chapitres suivants signifie que ce chapitre ne s'applique pas dans le cadre de ce projet.

# 1 SYNTHÈSE

## 1.1 Contexte et enjeux du projet

Dans le cadre de l'évolution de notre modèle de distribution, le numérique se positionnera comme le principal canal d'accès à la banque, dans un environnement marqué par :

- ✓ Une appétence croissante des clients à utiliser le numérique en self care et à acheter en ligne
- ✓ Une concurrence accrue, qui impose des niveaux très élevés de qualité, de périmètre fonctionnel, de respect de la conformité, de vitesse d'adaptation de nos outils et de nos processus
- ✓ Une multiplication des terminaux permettant d'accéder au numérique et une nécessité de rester à la pointe de la technologie pour servir notre image de banque innovante.

**Le projet NGIM a pour vocation à accompagner la Banque dans le changement de son modèle relationnel** en mettant à disposition des clients et prospects des espaces digitaux homogènes, de qualité.

Plusieurs lots ont été définis par ITIM :



**Le lot 3 de NGIM** se positionne sur l'exploitation d'informations, via un Ad server, issues des données de l'écosystème du marketing opérationnel, dans l'objectif de **diffuser des contenus promotionnels ciblés aux visiteurs (clients ou prospect) des sites et applications SG.**

Deux objectifs principaux :

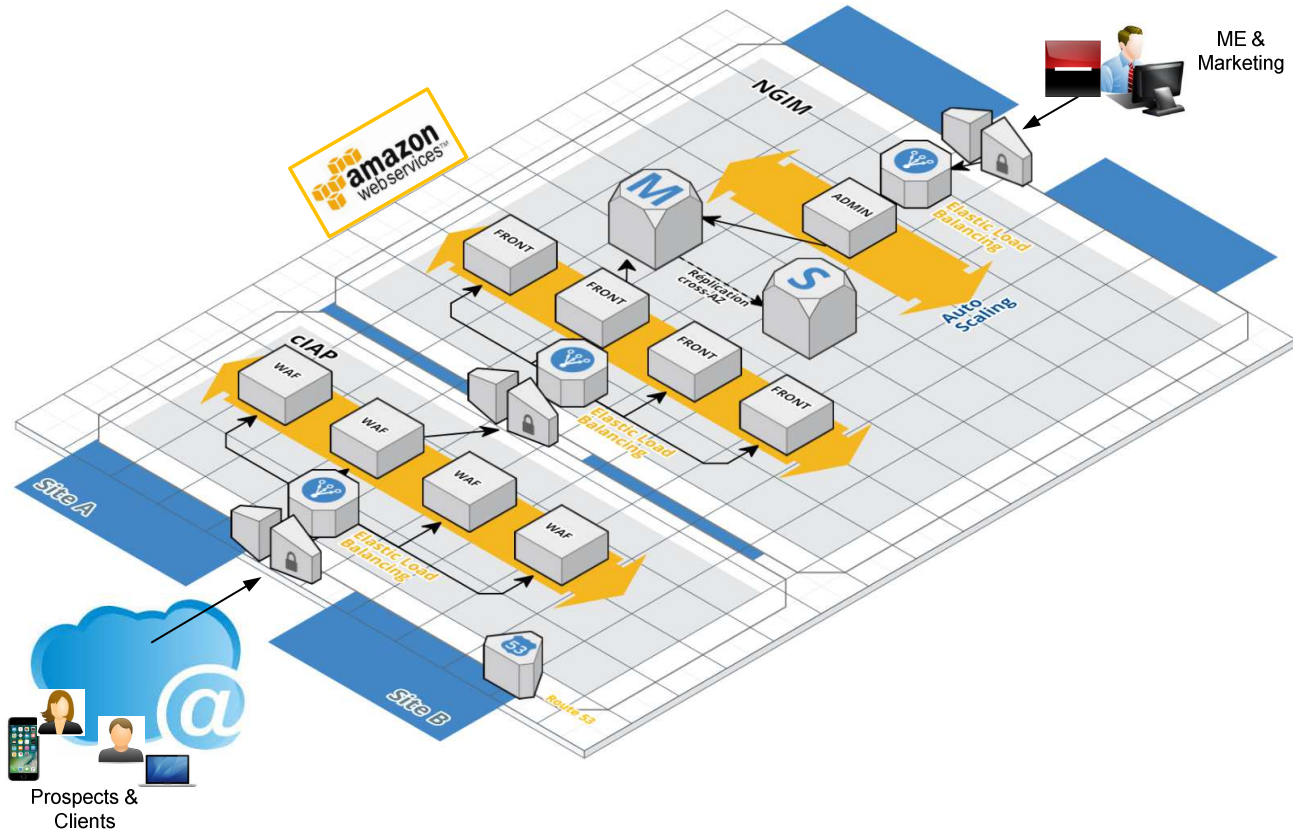
- ✓ **Valoriser le trafic sur les sites et applications Société Générale** en proposant aux visiteurs (prospects et clients) des contenus personnalisés permettant de promouvoir les produits, offres et services Société Générale.
- ✓ **Laisser directement la main au marketing** pour leur permettre dans une échelle de temps réduite de déployer de nouveaux bandeaux publicitaires multi-devices avec comme impact une charge non prévisible sur l'application (**1,5 millions de requêtes par bandeau**)

L'Ad-Server sera construit à partir du progiciel open-source Revive développé en php. Des customisations doivent être apportées à l'application afin qu'elle réponde entièrement aux besoins de Société Générale (sécurisation du processus de publication d'un contenu – invisibilité par rapport aux ad-blockers...).

L'hébergement dans le cloud public AWS de l'outil d'Ad-Server a été privilégié pour les raisons suivantes :



## 1.2 Vue macro de la solution sur AWS



**En termes d'architecture, le principal défi du projet consiste à déployer une solution « infra-aware »,** i.e. une application consciente de son infrastructure et capable de l'adapter en fonction de ses besoins et/ou d'événements (mise à l'échelle, remédiation automatique).

## 1.3 Périmètre

Le périmètre couvert par le lot de 09/2015 est le suivant : diffusion de l'auto-promotion sur le site internet Société Générale ainsi que sur des webviews de l'application mobile.

Un lot ultérieur adressera la diffusion dans des pages natives de l'application (instruction en cours, pas de date de MEP planifiée)

## 2 ARCHITECTURE APPLICATIVE NGIM

L'application NGIM Ad Server est basée sur les briques applicatives suivantes :

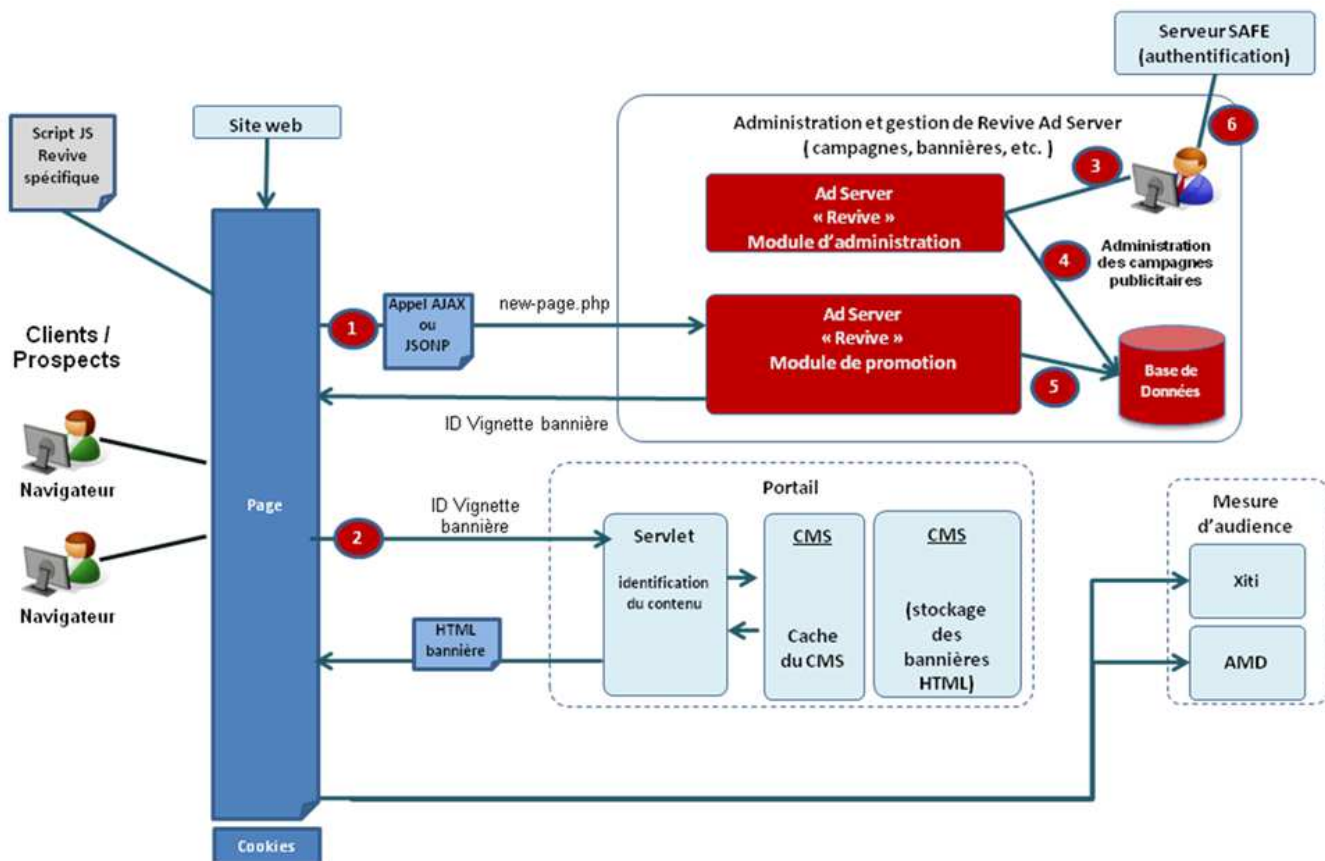
### Nouvelles briques

- ✓ Ad Server – Module promotion
- ✓ Ad Server – Module d'administration
- ✓ Bases de données

### Briques existantes

- ✓ Service d'authentification SAFE
- ✓ Gestion de contenu (bannières publicitaire) de la B@D

### 2.1 Schéma d'architecture applicative



### 2.2 Description des composants applicatifs de NGIM Lot 3

#### 2.2.1 AD Server – Module promotion

Développements internes SG basés sur la solution Open Source Revive AdServer (Apache/PHP)

#### 2.2.2 AD Server – Module Administration

Développements internes SG basés sur la solution Open Source Revive AdServer (Apache/PHP)

#### 2.2.3 Base de données PostgreSQL

La ME a choisi le SGBD PostgreSQL pour héberger les données liées aux campagnes de publicité.



### 2.3 Matrice des flux applicatifs

Flux	Source	Destination	Port	Protocole
1	Navigateur client	Serveur Revive Promotion	443	HTTPS
2	Navigateur client	CMS	443	HTTPS
3	Poste client SG	Serveur Revive Administration	443	HTTPS
4	Serveur Revive Administration	Base PostgreSQL	5432	TCP
5	Serveur Revive Promotion	Base PostgreSQL	5432	TCP
6	Poste client SG	SAFE (Via le SIPO)	443	HTTPS

Note : Les flux 1,2,3,5,6, 9 (Flux HTTPS) bénéficient d'une rupture de protocole (exigences sécurité ITIM/SRO)

### 2.4 Volumétries

Flux	Source	Destination	Fréquence	Poids
1	Navigateur client	Serveur Revive Promotion	1000 hits/sec	< 1ko
2	Navigateur client	CMS NGC	Faible Les bannières sont en cache sur HELIOS	
3	Poste client SG	Serveur Revive Administration	< 30 utilisateurs	faible
4	Serveur Revive Administration	Base PostgreSQL	faible	faible
5	Serveur Revive Promotion	Base PostgreSQL	1000 hits/sec (Read Only)	< 1ko
6	Poste client SG	SAFE (Via le SIPO)	faible	faible

## 3 CONTEXTE AMAZON WEB SERVICES (AWS)

### 3.1 Comptes AWS

#### 3.1.1 Définition

La création d'un nouveau compte AWS se fait avec un login / mot de passe initial. Ce mot de passe donne accès au compte dit « racine » qui a tous les droits sur le compte, y compris celui de le clore définitivement. L'utilisation du compte racine doit donc rester exceptionnelle afin d'éviter les manipulations hasardeuses qui peuvent impacter tous les accès liés à ce compte.

#### 3.1.2 Choix pour NGIM

Un compte AWS gère les accès depuis et vers Internet (cIAP)

En cible, la structuration des comptes AWS évoluera mais un choix a été arrêté pour NGIM lot 3 Ad-Server : 1 compte par environnement sera créé (DEV, HML et PROD).

Chaque compte NGIM respectera l'urbanisation VPC (Virtual Private Cloud) suivante :

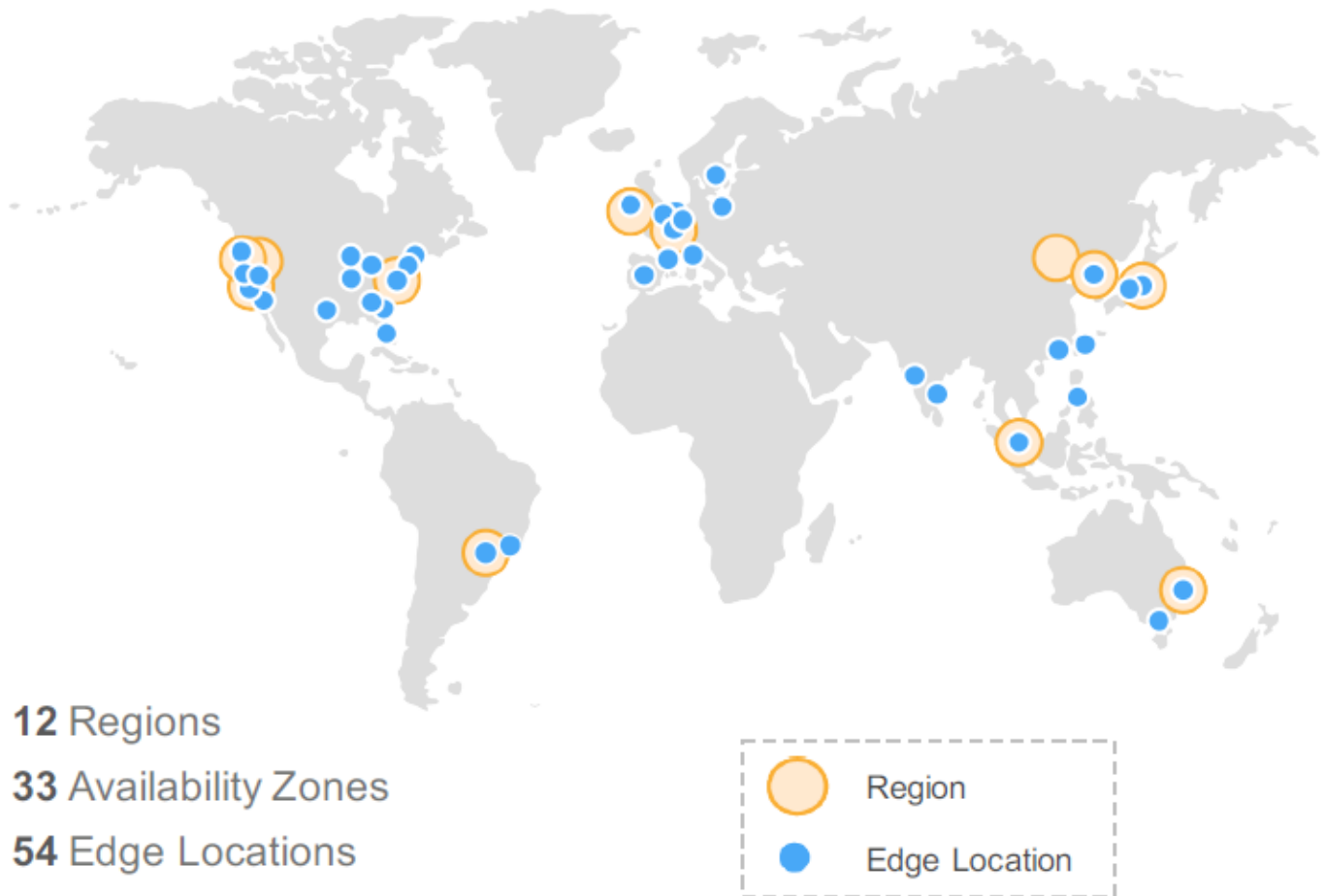
- ✓ VPC Web: Zone d'hébergement de l'infrastructure applicative NGIM
- ✓ VPC Admin: Hébergement du nœud de contrôle et des composants d'administration de l'infrastructure
- ✓ VPC Technique: Hébergement des images OS et packages logiciels

D'autre part, les composants techniques hébergés dans les VPC Technique et Admin sont ici dédiés à un environnement de NGIM, à la cible elles seront mutualisées. Le niveau de mutualisation reste à être étudié.



### 3.2 Infrastructure d'hébergement AWS

Ci-dessous la cartographie des infrastructures AWS :



Principes d'une région AWS :

- ✓ Chaque région chez AWS se situe dans une zone géographique totalement indépendante et isolée des autres. Des flux entre région doivent être véhiculés via Internet et seront considérés par la région destinatrice comme des flux externes.
- ✓ Chaque région dispose de plusieurs zones de disponibilité (Availability Zone - AZ) avec des profils de risques complémentaires. Il est possible d'héberger une application sur 1, 2 voir 3 AZ, AWS s'engage à ce qu'un hébergement sur 3 AZ propose une couverture de risque complète. (problématique télécom ou électrique, crue, explosion, etc)

La Société Générale a choisi d'héberger ses applications en Europe de l'Ouest dans la **région AWS d'Irlande et de Francfort.**

AWS Francfort peut-être utilisée comme région de secours à froid en cas de perte de toute la région Irlande (SLA de plusieurs jours), mais ce ne sera pas le cas pour NGIM lot 3 qui n'a pas ce niveau d'exigences.

### 3.3 Zone de disponibilité (AZ)

Principes d'une AZ :

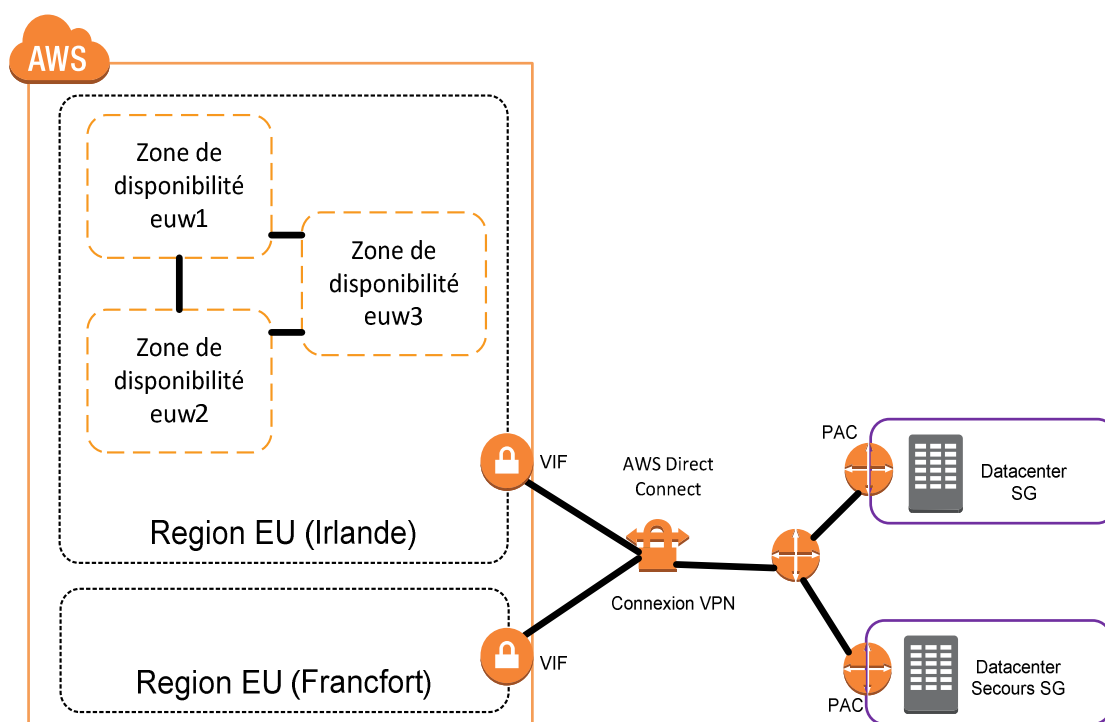
- ✓ Physiquement isolée des autres AZ
- ✓ Séparée géographiquement (profil de risques différents)
- ✓ Interconnectée aux autres AZ via des liens privés à faible latence.

Dans le cadre du projet NGIM lot 3 Ad Server, l'application sera déployée en nominal sur deux AZ en Irlande sans secours à froid.

### 3.4 Connectivité AWS – Société Générale

#### 3.4.1 Vision globale

Les deux régions (Irlande et Francfort) sont reliées aux 2 points d'accès cloud (PAC) Tigery et Seclin 2.



A terme le PAC sera remplacé par une solution CloudBridge/Cloudcell dont le HLD est en cours d'instruction au moment de la rédaction de ce document.

Note : Chaque Virtual Private Gateway repose sur deux VIF chacune rattaché à un port physique d'un équipement d'interconnexion AWS physique distinct garantissant ainsi la robustesse du Direct Connect.

#### 3.4.2 Cloudcell tactique

La Cloudcell cible n'étant pas encore disponible et le planning de mise en œuvre engagé, dans le cadre du projet NGIM lot 3 Ad Server, la Cloudcell utilisée est celle implémentée dans le cadre du POC sogecashweb. Il s'agit d'un cluster ESX hébergé sur deux lames physiques à Tigery sans secours distant.

Cette Cloudcell tactique est raccordée aux infrastructures I2BD d'homologation pour lesquels GTS/TFO/CTY rappelle les SLA qui y sont appliquées :

⇒ **Infrastructure :**

- ✓ Pas de haute disponibilité du fait du simple attachement physique
- ✓ Aucun SLA de rétablissement en cas d'indisponibilité (best effort),

⇒ **Change management :**

- ✓ Les changes sur cette infrastructure peuvent être réalisés entre 12h et 14h tous les jours de la semaine d'où un risque d'indisponibilité accru en HO,
- ✓ Les changes sont classifiés en « mineur », ils sont donc exécutés avec une visibilité et un niveau de contrôle moindre sur les opérations réalisées => risque d'indisponibilité accru



**Point d'attention :** L'ensemble de ces éléments impliquent un niveau de risque d'indisponibilité accru et renforce le caractère « tactique » de cette solution en attendant la mise à disposition de la Cloudcell cible.

### 3.4.3 Direct Connect

Le service AWS Direct Connect permet d'établir une connexion privée entre AWS et les DataCenters de ses clients.

Dans le cadre du POC sogecashweb, une liaison via le partenaire InterCloud a été mise en place avec une bande passante 100Mbps. Afin de permettre un démarrage rapide, il a été décidé de réutiliser cette liaison et le Direct Connect associé.

A noter la nécessité de porter via l'opérateur InterCloud le nombre de Virtual Private Gateway de 1 à 5 (3 pour NGIM et 2 pour le VIAP cf §2.5.3).

## 3.5 Virtual Private Cloud (VPC)

### 3.5.1 Description

#### A) Généralités

Un VPC correspond à une zone d'hébergement logique isolée dans laquelle le client (Société Générale) peut instancier ses ressources AWS au sein d'un réseau virtuel dédié.

Le client a la maîtrise complète de ce réseau virtuel : sélection de la plage d'adresse IP, création des sous-réseaux, configuration de la table de routage et des passerelles réseau.

Le réseau du VPC peut-être segmenté en sous-réseau, chacun d'entre eux attachés à une fonction.

Par exemple, un sous-réseau public pour héberger les composants Web accédés depuis internet, un sous-réseau privé non accessible directement depuis Internet, etc.

Plusieurs couches de sécurité (Security Groups et Network ACL) permettent de sécuriser les échanges entre subnets et entre instances.

Le VPC peut-être connecté :

- ✓ à Internet (via le cIAP),

- ✓ à un DataCenter (Direct Connect)
- ✓ ou à d'autres VPC (VPC Peering)

Un VPC au sein d'un compte AWS se caractérise par :

- ✓ 1 Région
- ✓ 1 bloc CIDR
- ✓ Un ensemble de subnets

## B) NGIM lot 3 – Ad Server

Dans chaque environnement, 4 VPC entreront en jeu pour permettre de fournir le service attendu :

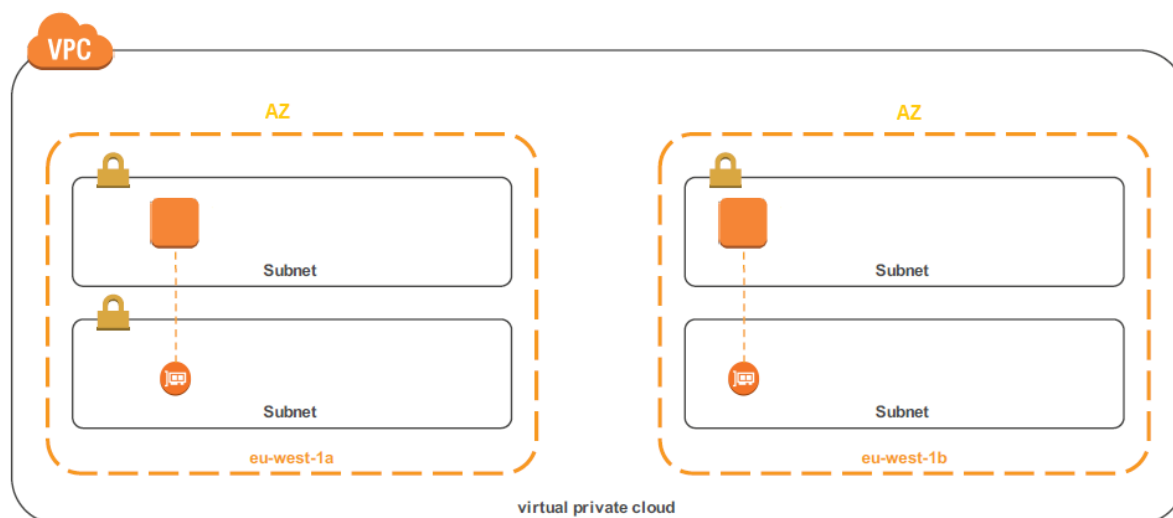
- ✓ VPC cIAP (Compte AWS - GTS/TFO) : Zone exposée mutualisée permettant de sécuriser les flux entrants depuis Internet à destination des applications Société Générale hébergées chez AWS
- ✓ VPC WEB (Compte AWS – NGIM) : Zone hébergeant l'application et séparée en 2 sous-réseaux
  - ✓ Un sous-réseau public hébergeant les capacités de répartition de charge et les instances NGIM ad Server (module promotion)
  - ✓ Un sous-réseau privé hébergeant la base de données NGIM (Service RDS PostgreSQL) et l'instance NGIM Ad Server (module administration)
- ✓ VPC TECHNIQUE (Compte AWS – NGIM) : Zone privée technique contenant le repository OS
- ✓ VPC ADMIN (Compte AWS – NGIM) : Zone privée d'administration contenant les servitudes suivantes
  - ✓ ProtectV Manager
  - ✓ Nœud de contrôle
  - ✓ Bastion AWS (Rebond SSH ou Jump Host)
  - ✓ Proxy HTTP
  - ✓ Relais NTP (Synchronisation avec les serveurs NTP Internes Société Générale)
  - ✓ Relais syslog (collecte des logs systèmes)
  - ✓ Les AMI

### 3.5.2 VPC Mutli-AZ et subnets

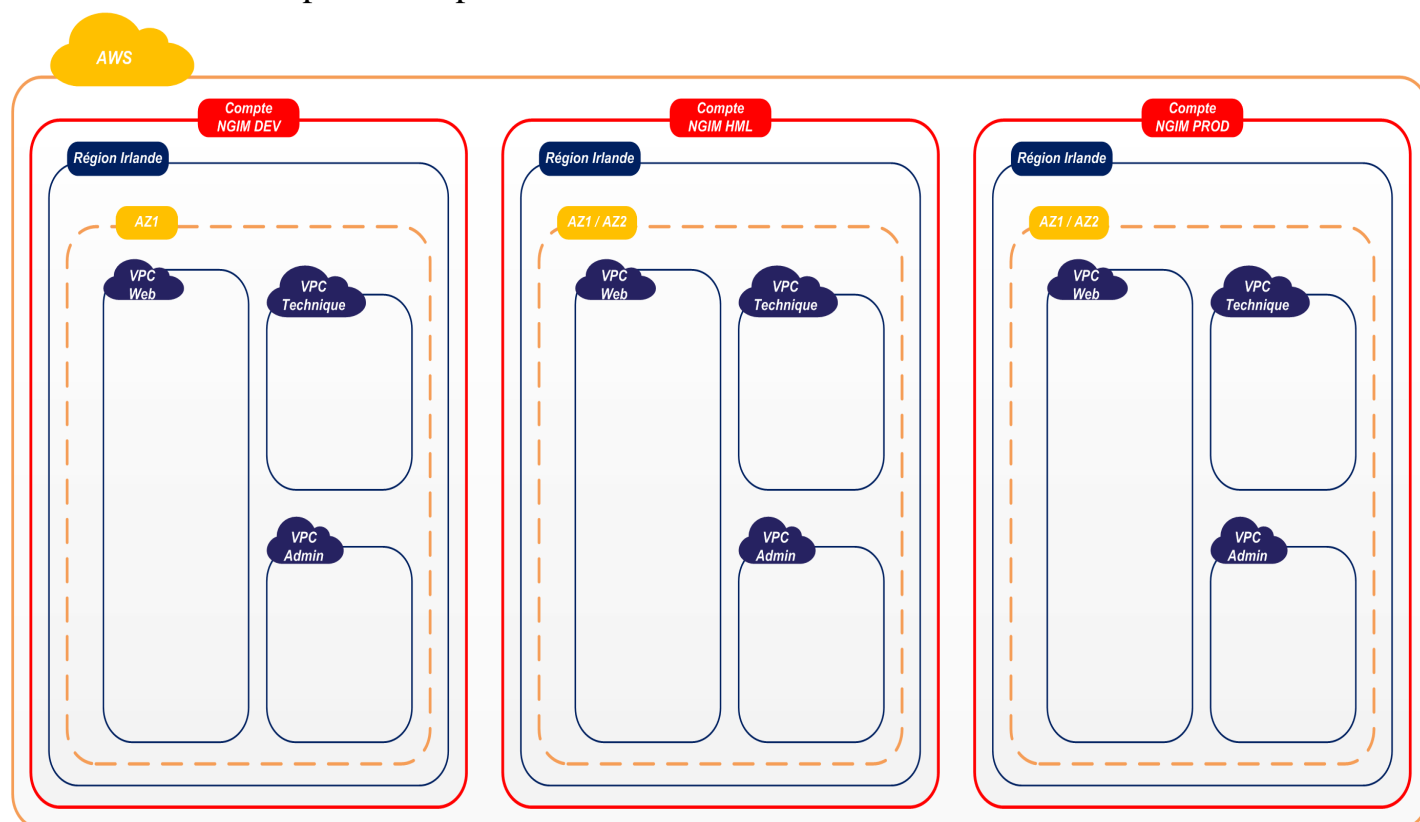
Afin de répondre aux besoins de haute disponibilité, un VPC peut être étendu sur 2 ou trois AZ.

Comme décrit au §2.4.1, un VPC est composé de subnets, les subnets ne sont pas étendus entre AZ, de ce fait pour un tiers de l'application, un subnet par AZ sera créé.

Ci-dessous, la représentation logique d'un VPC déployé sur deux AZ :

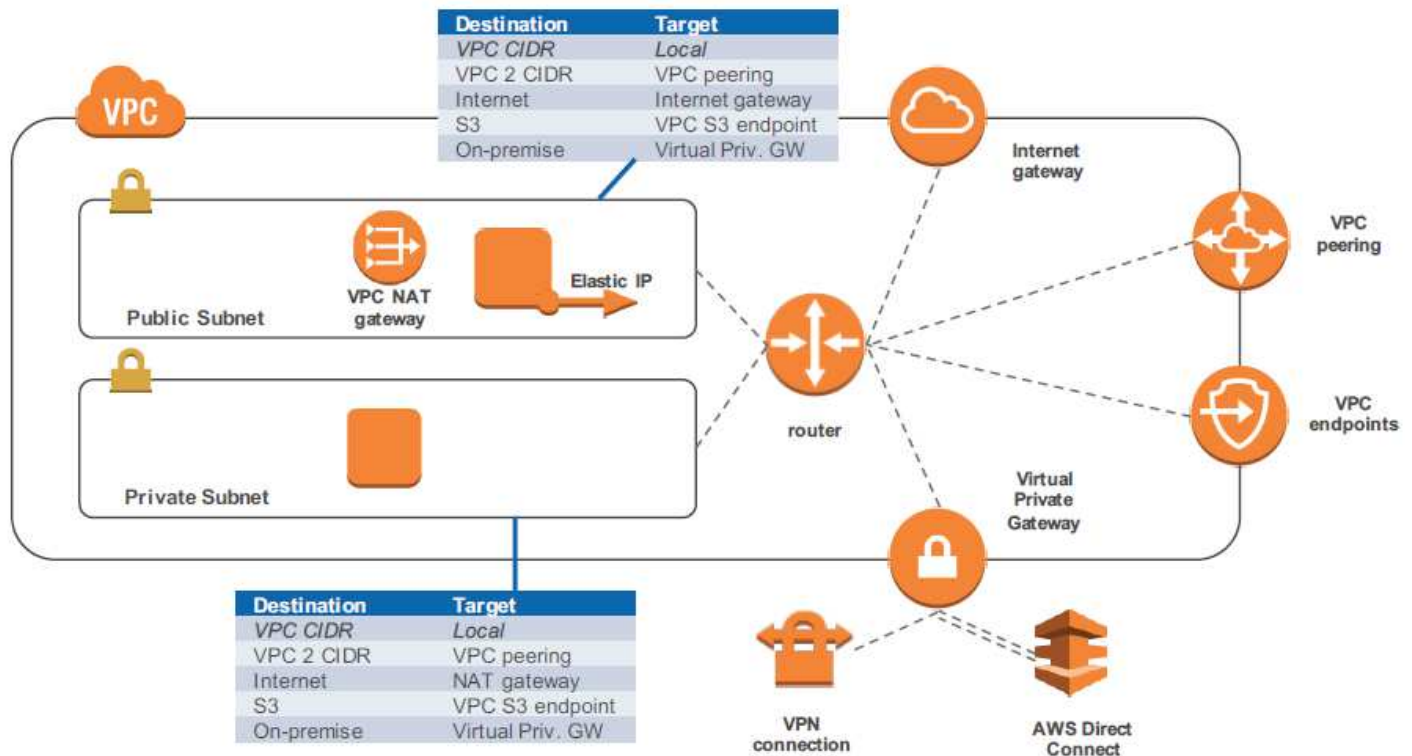


### 3.5.3 Schéma Comptes/VPC pour NGIM



### 3.5.4 Connectivités du VPC

Tous les types de connectivités du VPC sont représentés dans le schéma ci-dessous :



### A) Virtual Private Gateway : Connectivité avec les DataCenters Société Générale

Nous reviendrons sur la connectivité réseau entre AWS et la Société Générale au §4.2, mais une fois cette connectivité fonctionnelle, par défaut, les instances démarrées au sein d'un VPC ne peuvent pas communiquer avec le réseau Société Générale.

Nous pouvons activer cette communication en attachant au VPC une « Virtual Private Gateway » et en adaptant la table de routage. Cette action est à mener pour chaque VPC ayant besoin de communiquer avec le réseau interne sans passer par Internet.

Dans le cadre de NGIM lot 3 Ad server, une Virtual Private Gateway sera attachée aux VPC Admin de chaque compte (3 Virtual Private Gateway au total pour NGIM)

### B) VPC Endpoint

Un VPC Endpoint permet de créer une connexion privée entre un VPC et d'autres services AWS uniquement accessibles par Internet (pour le moment seul le service S3 est concerné, les autres services AWS sont accessibles nativement).

Il s'agit d'un dispositif virtuel robuste, disposant d'une mise à l'échelle horizontale et hautement disponible permettant aux instances au sein d'un VPC de disposer d'un accès pérenne aux services AWS sans contraintes de bande passante ou de disponibilité.

Les instances sont ainsi en mesure de joindre les services AWS avec leur adresse privée et les échanges restent internes au réseau AWS.

Dans le cadre de NGIM Lot 3 Ad Server, cette fonctionnalité ne sera pas utilisée car limitée.

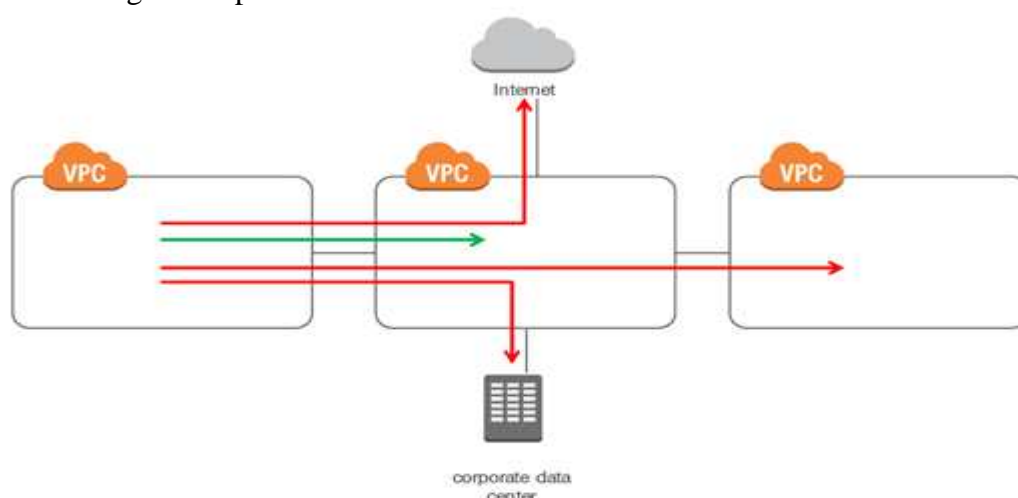
## C) VPC Peering

### 3.5.4.C.1 Généralités

Par défaut, le VPC d'un compte AWS est isolé et ne peut communiquer avec les autres VPC du même compte ou d'un autre compte AWS.

Le VPC Peering est une fonctionnalité AWS permettant d'autoriser les échanges entre deux VPC d'un même compte ou entre deux VPC de comptes AWS différents.

Les instances peuvent ainsi discuter entre différents VPC en utilisant leur adresse IP privée, mais cette fonctionnalité de routage n'est pas transitive.



Une limite est fixée par AWS : un VPC peut détenir au maximum 50 VPC Peered (il est possible en négociant avec AWS d'aller jusqu'à 125 VPC mais cette dernière est une limite technique)

### 3.5.4.C.2 NGIM Lot 3 Ad Server

Dans le cadre du projet NGIM lot 3 Ad-Server, les VPC Peering suivants seront mis en place pour chaque compte AWS :

VPC #1	VPC #2
VIAP	VPC WEB
VIAP	VPC TECHNIQUE
VPC WEB	VPC TECHNIQUE
VPC WEB	VPC ADMIN
VPC TECHNIQUE	VPC ADMIN

## D) Internet Gateway

**Sans objet dans le cadre de ce document** pour NGIM lot 3 Ad Server, les accès depuis et vers Internet sont assurés par le cIAP, composant transverse dont le HLD est en cours d'instruction par GTS/TFO

## E) VPC NAT Gateway

**Sans objet dans le cadre de ce document** pour NGIM lot 3 Ad Server, les accès depuis et vers Internet sont assurés par le VPC VIAP dont le HLD est en cours d'instruction par GTS/TFO

## F) Elastic IP

**Sans objet dans le cadre de ce document** pour NGIM lot 3 Ad Server, les accès depuis et vers Internet sont assurés par le VPC VIAP dont le HLD est en cours d'instruction par GTS/TFO8



### 3.6 *Sécurisation des échanges (NACL et Security Groups)*

#### 3.6.1 Network Access Control List (NACL)

Une NACL une option de sécurité du VPC qui agit comme un firewall permettant de contrôler les flux entrants et sortants de un ou plusieurs sous-réseaux.

Lors de sa création, un VPC vient automatiquement avec une NACL qui par défaut autorise tous les flux entrants et sortants des sous-réseaux du VPC. Cette NACL est modifiable.

Il est possible de créer une Custom NACL et de l'attacher à un subnet, par défaut, toutes les Custom NACL comportent une règle par défaut non modifiable qui interdit tous les flux entrants et sortants. Il est nécessaire ensuite d'ajouter des règles « ALLOW ».

Dans un VPC, chaque sous-réseau doit être muni d'une NACL, s'il n'en dispose pas, il se voit automatiquement attribuée le NACL par défaut.

Un NACL peut être associé à plusieurs sous-réseaux, cependant un sous-réseau ne peut avoir qu'une seule et unique NACL.

Un NACL est une liste de règles numérotées ALLOW ou DENY qui sont appliqués dans l'ordre, le numéro maximum pour une règle est 32766.

Une règle NACL concerne soit les flux entrants (inbound) soit sortant (outbound), elle comprend le protocole, la source, la destination, un port ou une plage de ports.

**Les NACL sont stateless, ce qui implique que le trafic lié aux réponses à une requête ne sera véhiculé que si une règle NACL en sortie l'autorise.**

#### 3.6.2 Security Group

Un Security group agit comme un firewall qui permet de contrôler le trafic au niveau d'une ou plusieurs instances. Lorsqu'une instance est démarrée, il est possible de lui associer jusqu'à 5 security groups par interface réseau.

Si l'instance n'est associée à aucun Security group, lui sera attaché le Security Group par défaut. Ce dernier comporte une règle par défaut modifiable qui autorise tous les flux sortants et interdit tous les flux entrants sur l'instance.

Un security group ne peut contenir que des règles de type « ALLOW », la mise à jour d'un security group est appliquée dynamiquement à toutes les instances associées.

Il est possible de créer jusqu'à 500 Security groups par VPC, 50 règles par Security Group et 5 Security Group par interface réseau d'une instance.

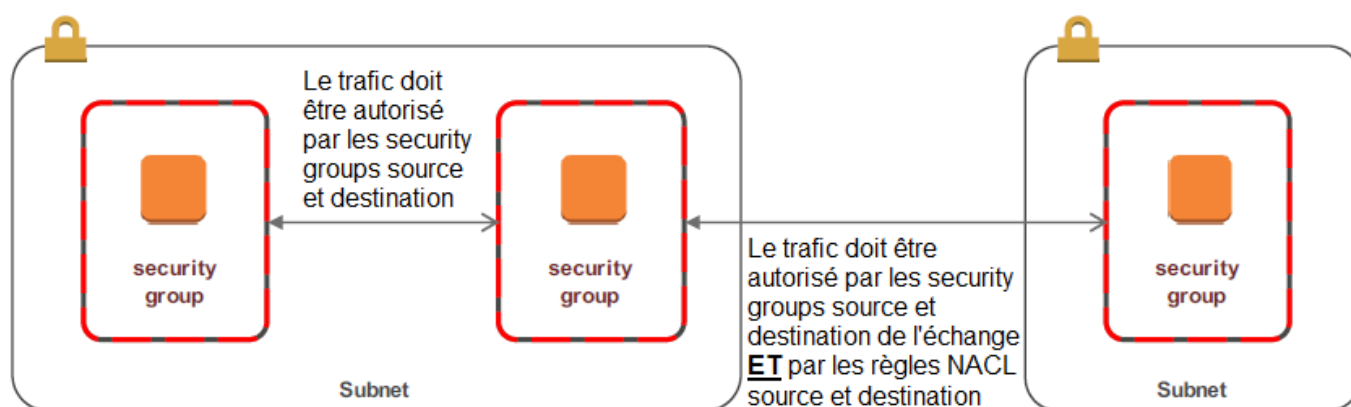
Le Security Group est stateful, le trafic correspondant aux réponses à une requête est nativement autorisé contrairement aux NACLs.

Ce mécanisme de sécurité vient en complément des NACLs.



### 3.6.3 NACL vs Security Group

	Network ACL (NACL)	Security Group
Niveau d'application de la règle	sous-réseau	instance
Supporte des règles de type	ALLOW & DENY	ALLOW uniquement
Les règles s'appliquent	en respectant l'ordre de la liste	dans leur ensemble
Stateful	Non	Oui
Identification de la source	plage d'adresse IP	plage d'adresse IP security group prefixes IP



### 3.6.4 Flow Logs

Cette fonctionnalité AWS permet de collecter toutes les informations nécessaires à l'audit du trafic IP entrant et sortant des VPC.

La fonctionnalité n'est pas activée par défaut, les logs générés sont stockés dans un bucket S3.

Cette fonctionnalité n'est pas un pré-requis à la mise en production de NGIM lot 3 Ad Server mais pourra être utilisée ultérieurement.

Possibilité de l'activer à étudier dans le cadre de NGIM pour tester la fonctionnalité :

- Durée de rétention de 14j
- Conservation des logs dans CloudWatch
- Utilisation des logs lors d'un troubleshooting en se connectant directement sur la Console AWS

### 3.6.5 Règles mises en place pour NGIM lot 3 Ad – server

#### A) Règles NACL

Les règles proposées ci-dessous pourront évoluer. Elles sont identiques pour tous les environnements sauf concernant les échanges avec le cIAP (pas d'interconnexion avec le cIAP en DEV).

REGLES NACL								
Nom NACL	Subnet	Règle n°	Type	Protocole		Ports	CIDR	ALLOW/DENY
ElbFrontPrv_NACL	ElbFrontPrv	100	Inbound	TCP	HTTPS	443	cIAPIn	ALLOW
ElbFrontPrv_NACL	ElbFrontPrv	110	Inbound	TCP	HTTPS	443	AdminPrv	ALLOW
ElbFrontPrv_NACL	ElbFrontPrv	120	Inbound	TCP	HTTPS	1024-65535	subnet FRONT	ALLOW
ElbFrontPrv_NACL	ElbFrontPrv	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
ElbFrontPrv_NACL	ElbFrontPrv	100	Outbound	TCP	HTTPS	443	subnet FRONT	ALLOW
ElbFrontPrv_NACL	ElbFrontPrv	110	Outbound	TCP	HTTPS	1024-65535	cIAPIn	ALLOW
ElbFrontPrv_NACL	ElbFrontPrv	120	Outbound	TCP	HTTPS	1024-65535	AdminPrv	ALLOW
ElbFrontPrv_NACL	ElbFrontPrv	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY
FrontPrv_NACL	FrontPrv	100	Inbound	ALL	ALL	ALL	AdminPrv	ALLOW
FrontPrv_NACL	FrontPrv	110	Inbound	TCP	HTTPS	443	ElbFrontPrv	ALLOW
FrontPrv_NACL	FrontPrv	120	Inbound	ALL	ALL	ALL	BackendPrv	ALLOW
FrontPrv_NACL	FrontPrv	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
FrontPrv_NACL	FrontPrv	100	Outbound	ALL	ALL	ALL	AdminPrv	ALLOW
FrontPrv_NACL	FrontPrv	110	Outbound	TCP	HTTPS	1024-65535	ElbFrontPrv	ALLOW
FrontPrv_NACL	FrontPrv	120	Outbound	ALL	ALL	ALL	BackendPrv	ALLOW
FrontPrv_NACL	FrontPrv	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY
BackendPrv_NACL	BackendPrv	100	Inbound	ALL	ALL	ALL	AdminPrv	ALLOW
BackendPrv_NACL	BackendPrv	110	Inbound	ALL	ALL	ALL	FrontPrv	ALLOW
BackendPrv_NACL	BackendPrv	120	Inbound	ALL	ALL	ALL	ElbBackendPrv	ALLOW
BackendPrv_NACL	BackendPrv	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
BackendPrv_NACL	BackendPrv	100	Outbound	ALL	ALL	ALL	AdminPrv	ALLOW
BackendPrv_NACL	BackendPrv	110	Outbound	ALL	ALL	ALL	FrontPrv	ALLOW
BackendPrv_NACL	BackendPrv	120	Outbound	ALL	ALL	ALL	ElbBackendPrv	ALLOW
BackendPrv_NACL	BackendPrv	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY
ELBBackendPrv_NACL	ELBBackendPrv	100	Inbound	ALL	ALL	ALL	AdminPrv	ALLOW
ELBBackendPrv_NACL	ELBBackendPrv	110	Inbound	ALL	ALL	ALL	BackendPrv	ALLOW
ELBBackendPrv_NACL	ELBBackendPrv	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
ELBBackendPrv_NACL	ELBBackendPrv	100	Outbound	ALL	ALL	ALL	AdminPrv	ALLOW
ELBBackendPrv_NACL	ELBBackendPrv	110	Outbound	ALL	ALL	ALL	BackendPrv	ALLOW
ELBBackendPrv_NACL	ELBBackendPrv	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY
AdminPrv_NACL	AdminPrv	100	Inbound	ALL	ALL	ALL	ElbFrontPrv	ALLOW
AdminPrv_NACL	AdminPrv	110	Inbound	ALL	ALL	ALL	FrontPrv	ALLOW
AdminPrv_NACL	AdminPrv	120	Inbound	ALL	ALL	ALL	BackendPrv	ALLOW
AdminPrv_NACL	AdminPrv	130	Inbound	ALL	ALL	ALL	ElbBackendPrv	ALLOW
AdminPrv_NACL	AdminPrv	140	Inbound	ALL	ALL	ALL	TechPrv	ALLOW
AdminPrv_NACL	AdminPrv	150	Inbound	ALL	ALL	ALL	TechOutPrv	ALLOW
AdminPrv_NACL	AdminPrv	160	Inbound	TCP	SSH	22	EmergencyAdminPub	ALLOW
AdminPrv_NACL	AdminPrv	170	Inbound	ALL	ALL	ALL	CloudCell NGIM	ALLOW
AdminPrv_NACL	AdminPrv	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
AdminPrv_NACL	AdminPrv	100	Outbound	ALL	ALL	ALL	ElbFrontPrv	ALLOW
AdminPrv_NACL	AdminPrv	110	Outbound	ALL	ALL	ALL	FrontPrv	ALLOW
AdminPrv_NACL	AdminPrv	120	Outbound	ALL	ALL	ALL	BackendPrv	ALLOW

AdminPrv_NACL	AdminPrv	130	Outbound	ALL	ALL	ALL	ElbBackendPrv	ALLOW
AdminPrv_NACL	AdminPrv	140	Outbound	ALL	ALL	ALL	TechPrv	ALLOW
AdminPrv_NACL	AdminPrv	150	Outbound	ALL	ALL	ALL	TechOutPrv	ALLOW
AdminPrv_NACL	AdminPrv	160	Outbound	TCP	SSH	1024-65535	EmergencyAdminPub	ALLOW
AdminPrv_NACL	AdminPrv	170	OutBound	ALL	ALL	ALL	CloudCell NGIM	ALLOW
AdminPrv_NACL	AdminPrv	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY
TechPrv_NACL	TechPrv	100	Inbound	TCP	ALL	ALL	AdminPrv	ALLOW
TechPrv_NACL	TechPrv	110	Inbound	TCP	HTTPS	1024-65535	cIAPOut	ALLOW
TechPrv_NACL	TechPrv	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
TechPrv_NACL	TechPrv	100	Outbound	TCP	ALL	ALL	AdminPrv	ALLOW
TechPrv_NACL	TechPrv	110	Outbound	TCP	HTTPS	443	cIAPOut	ALLOW
TechPrv_NACL	TechPrv	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY
EmergencyAdminPub_NACL	EmergencyAdminPub	100	Inbound	TCP	SSH	22	0.0.0.0/0	ALLOW
EmergencyAdminPub_NACL	EmergencyAdminPub	*	Inbound	ALL	ALL	ALL	0.0.0.0/0	DENY
EmergencyAdminPub_NACL	EmergencyAdminPub	100	Outbound	TCP	SSH	1024-65535	0.0.0.0/0	ALLOW
EmergencyAdminPub_NACL	EmergencyAdminPub	*	Outbound	ALL	ALL	ALL	0.0.0.0/0	DENY

## B) Règles Security Groups

Les règles proposées ci-dessous pourront évoluer tout au long de la phase d’homologation. Elles sont identiques pour tous les environnements sauf concernant les échanges avec le cIAP (pas d’interconnexion avec le cIAP en DEV).

REGLES Security Group						
Nom Security Group	VPC	Instance	Protocole		Ports	Source
SecGrp_ELBApCpgn	WEB	ElbAppCpgn	TCP	HTTPS	443	SecGrp_cIAPIn
SecGrp_ELBApCpgn	WEB	ElbAppCpgn	TCP	HTTPS	443	SecGrp_ProxyAWS
SecGrp_AppCpgn	WEB	AppCpgn	TCP	HTTPS	443	SecGrp_ELBApCpgn
SecGrp_AppCpgn	WEB	AppCpgn	TCP	HTTPS	443	SecGrp_ProxyAWS
SecGrp_AppCpgn	WEB	AppCpgn	TCP	SSH	22	SecGrp_JumpHost
SecGrp_AppMng	WEB	AppMng	TCP	HTTPS	443	SecGrp_ProxyAWS
SecGrp_AppMng	WEB	AppMng	TCP	SSH	22	SecGrp_JumpHost
SecGrp_AppMng	WEB	AppMng	TCP	HTTPS	443	SecGrp_ELBApMng
SecGrp_BDDReve	WEB	BDDReve	TCP	PGSQL	5432	SecGrp_AppCpgn
SecGrp_BDDReve	WEB	BDDReve	TCP	PGSQL	5432	SecGrp_AppMng
SecGrp_BDDReve	WEB	BDDReve	TCP	SSH	22	SecGrp_JumpHost
SecGrp_ELBApMng	WEB	ElbAppMng	TCP	HTTPS	443	SecGrp_ProxyAWS
SecGrp_JumpHost	Admin	JumpHost	TCP	SSH	22	<IP host key>
SecGrp_ProxyAWS	Admin	ProxyAWS	TCP	SSH	22	SecGrp_JumpHost
SecGrp_ProxyAWS	Admin	ProxyAWS	TCP	HTTPS	443	192.65.116.0/24
SecGrp_Syslog	Admin	Syslog	TCP	SSH	22	SecGrp_JumpHost
SecGrp_Syslog	Admin	Syslog	TCP	syslog	514	<Cidr Env AWS / 23>
SecGrp_RelaisNTP	Admin	RelaisNTP	TCP	SSH	22	SecGrp_JumpHost
SecGrp_RelaisNTP	Admin	RelaisNTP	UDP	NTP	123	<Cidr Env AWS / 23>

SecGrp_RepoOS	Tech	RepoOS	TCP	SSH	22	SecGrp_JumpHost
SecGrp_RepoOS	Tech	RepoOS	TCP	HTTPS	443	<Cidr VPC Admin>

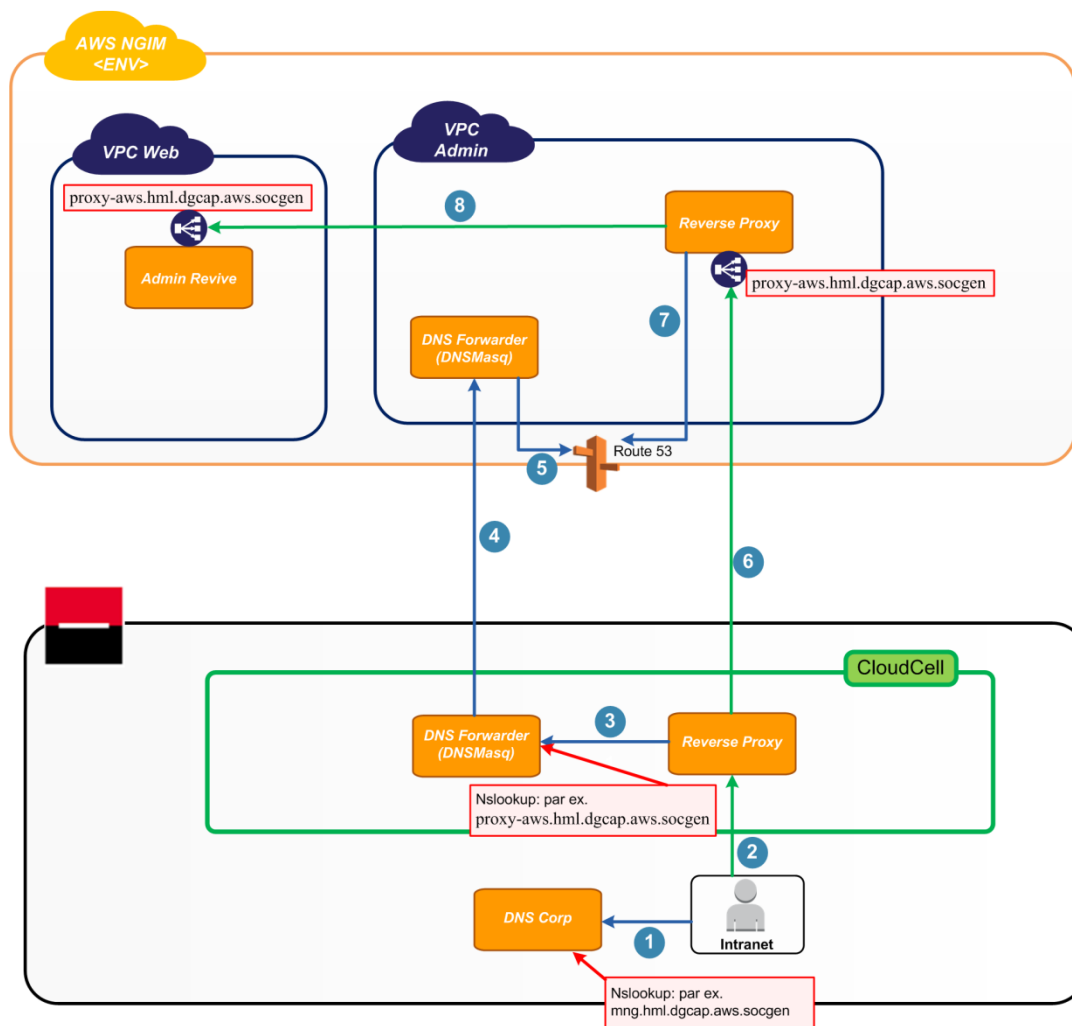
### 3.7 Résolution des noms de domaines

#### 3.7.1 Résolution SI SG – AWS

Dans le cadre du projet NGIM Ad Server, le besoin de résolution DNS depuis le SI SG interne est décrit par les 2 cas d'usages suivants :

- 1- Résolution DNS depuis le PDT SG vers un service applicatif chez AWS :  
dans ce cas, le DNS Corp renvoie toutes les requêtes en \*.dgcaw.ams.socgen vers le Reverse Proxy de la Cloudcell. Le Reverse Proxy utilisera alors le DNS forwarder pour résoudre les adresses des ressources AWS.
- 2- Résolution DNS d'une ressource AWS depuis la Cloudcell : Les servitudes de la Cloudcell s'adressent au DNS forwarder de la cloudcell qui transfère la requête de résolution vers le DNS forwarder du VPC d'admin chez AWS qui interroge à son tour Route53 (DNS AWS).

Le schéma suivant illustre les 2 cas d'usage décrits ci-dessus



Flux	Description
1	Le PDT SG interne exécute une requête de résolution au DNS Corp (SG interne) : → Nslookup : « mng.hml.dgcap.aws.socgen » → Réponse : @IP du Reverse Proxy de la Cloudcell
2	Connexion du PDT de l'utilisateur au Reverse Proxy de la CloudCell
3	Le Reverse Proxy exécute selon sa configuration, une requête de résolution au DNS Forwarder de la Cloudcell : →Nslookup : « proxy-aws.hml.dgcap.aws.socgen »
4	Le DNS Forwarder de la Cloudcell transmet la requête vers le DNS forwarder AWS →Nslookup : « proxy-aws.hml.dgcap.aws.socgen »
5	Le DNS Forwarder AWS transmet à son tour la requête au DNS Route53 d'Amazon →Nslookup : « proxy-aws.hml.dgcap.aws.socgen » → Réponse : @IP de l'ELB du Reverse Proxy
6	Le Reverse Proxy de la Cloudcell se connecte à l'ELB du Reverse Proxy AWS puis à l'instance associée chez AWS
7	Le Reverse Proxy AWS exécute selon sa configuration, une requête de résolution au DNS Route53 d'Amazon : →Nslookup : « mng.hml.dgcap.aws.socgen » → Réponse : @IP de l'ELB du service Revive Administration
8	Le Reverse Proxy AWS se connecte à l'ELB du module Revive Administration puis à l'instance associée chez AWS

### 3.7.2 Route53 : Résolution chez AWS

Route53 est le service de résolution de noms AWS.

Dans le cadre de NGIM lot 3, un domaine privé par environnement est créé sur AWS :

Environnement	Domaine Route 53 Privée de NGIM
DEV	dev.dgcap.aws.socgen
HML	hml.dgcap.aws.socgen
PRD	prd.dgcap.aws.socgen

Actuellement, il n'y a pas de mécanique de diffusion de la zone DNS privée entre le compte NGIM et celui de GTS/TFO ayant servi à construire le cIAP. De ce fait, à la création de l'ELB dans le VPC Web de la partie front de NGIM (module de promotion), AWS fournit une adresse DNS permettant de gérer la résilience entre AZ.

Environnement	Adresse interne Route 53 de l'ELB NGIM Front
DEV	A récupérer en post installation.
HML	internal-proxy-awshml-2090932731.eu-west-1.elb.amazonaws.com
PRD	A récupérer en post installation.

Cette adresse est à fournir à GTS/TFO pour leur permettre de router les flux depuis le cIAP vers l'ELB Front de NGIM.

### 3.8 Outils d'administration

#### 3.8.1 CloudWatch

##### A) Description générale


















Service de surveillance pour les ressources du cloud AWS et les applications qui y sont hébergées, Amazon CloudWatch permet de collecter, de suivre les métriques afin de superviser la disponibilité des services.

Le service permettra de superviser :

- ✓ Les instances Amazon EC2
- ✓ Les instances Amazon RDS PostgreSQL
- ✓ Les ELB
- ✓ Les mesures personnalisées générées par l'application NGIM Lot 3 Ad Server

##### B) Métriques

Le service se présente sous la forme d'une API et permet de collecter nativement :

- ✓ Instance EC2 :
  -  L'utilisation CPU
  -  Crédits CPU utilisés (capacité de « burst »)
  -  I/O Disques
  -  I/O réseaux
  -  Statut de l'instance
  -  Statut de l'OS
- ✓ Instance ELB :
  -  Connexion en erreur vers l'application
  -  Nombre de requêtes exécutées
  -  Nombre d'instances rattachées à l'ELB
  -  Nombre d'instances défaillantes rattachées à l'ELB
  -  Nombre de requêtes en attente d'exécution
  -  La latence (ELB uniquement)
- ✓ Instance RDS PostgreSQL :
  -  Utilisation CPU
  -  Nombre de connexions à la base de données
  -  Mémoire disponible
  -  I/O Disques
  -  Etc.

La liste exhaustive des métriques qui seront remontées sera définie au cours de la phase d'homologation de NGIM Lot 3 Ad Server.

A noter qu'à ce jour le service AWS CloudWatch n'a pas le niveau de certification attendu par le groupe Société Générale (SOC1/SOC2), une étude avec les équipes en charge de la conformité est en cours.

##### C) Fréquence de surveillance et durée de rétention

Les métriques sont conservées deux semaines.

- ✓ Auto Scaling Group : 7 mesures présélectionnées remontées toutes les minutes

- ✓ ELB : 13 mesures présélectionnées remontées toutes les minutes
- ✓ Route 53 : 1 mesure présélectionnée remontées toutes les minutes
- ✓ Instance RDS PostgreSQL : 14 mesures présélectionnées remontées toutes les minutes

### 3.8.2 CloudTrail

AWS CloudTrail est un service Web qui enregistre les appels d'API AWS pour les comptes AWS et les présente sous forme de fichier journal. Les informations enregistrées incluent l'identité de l'utilisateur à l'origine de l'appel d'API, l'heure de l'appel d'API, l'adresse IP source de l'utilisateur ayant effectué l'appel d'API, les paramètres de demande, ainsi que les éléments de réponse renvoyés par le service AWS.

L'historique des appels d'API AWS généré par CloudTrail permet de réaliser une analyse de sécurité, le suivi des modifications au niveau des ressources, ainsi que l'audit de conformité.

Dans le cadre de NGIM Lot 3 Ad Server, le service est activé et la collecte est effectuée dans un bucket S3. Les bonnes pratiques impliquent la mise en place d'un compte AWS et d'un bucket S3 dédié pour ce besoin. Cela pourra être effectué pour NGIM dans un second temps, pour le moment tout est effectué au sein du même compte.

### 3.8.3 CloudFormation

Le projet fait le choix d'utiliser CloudFormation pour une implémentation « Infrastructure as a code » de la couche bas niveau et ansible pour les composants supérieurs.

A noter, par exemple, que des scripts CloudFormation seront utilisés pour la création des buckets S3 du projet et la mise en place des buckets policy.

Concernant la partie bas niveau, ITIM a développé un outil (Stratosphère) permettant d'automatiser au format YAML la génération d'appel au service CloudFormation AWS pour la construction de l'infrastructure d'un projet.

« Stratosphère » est un outil développé en python (python 2.7.6) se basant sur le kit SDK AWS Boto3 et couvrant le périmètre suivant :

- ✓ Réseaux et sous-réseaux virtuels, Tables de routage réseaux, Passerelle Internet [VPC, Subnets, RouteTables, Internet Gateway]
- ✓ Interconnexion Réseaux, Liste de contrôle d'accès réseaux [VPC Peering, NACL]
- ✓ Groupe de règles de sécurité [Security Group]
- ✓ Zones privées et publiques DNS [Route53]



## 4 ARCHITECTURE RESEAU

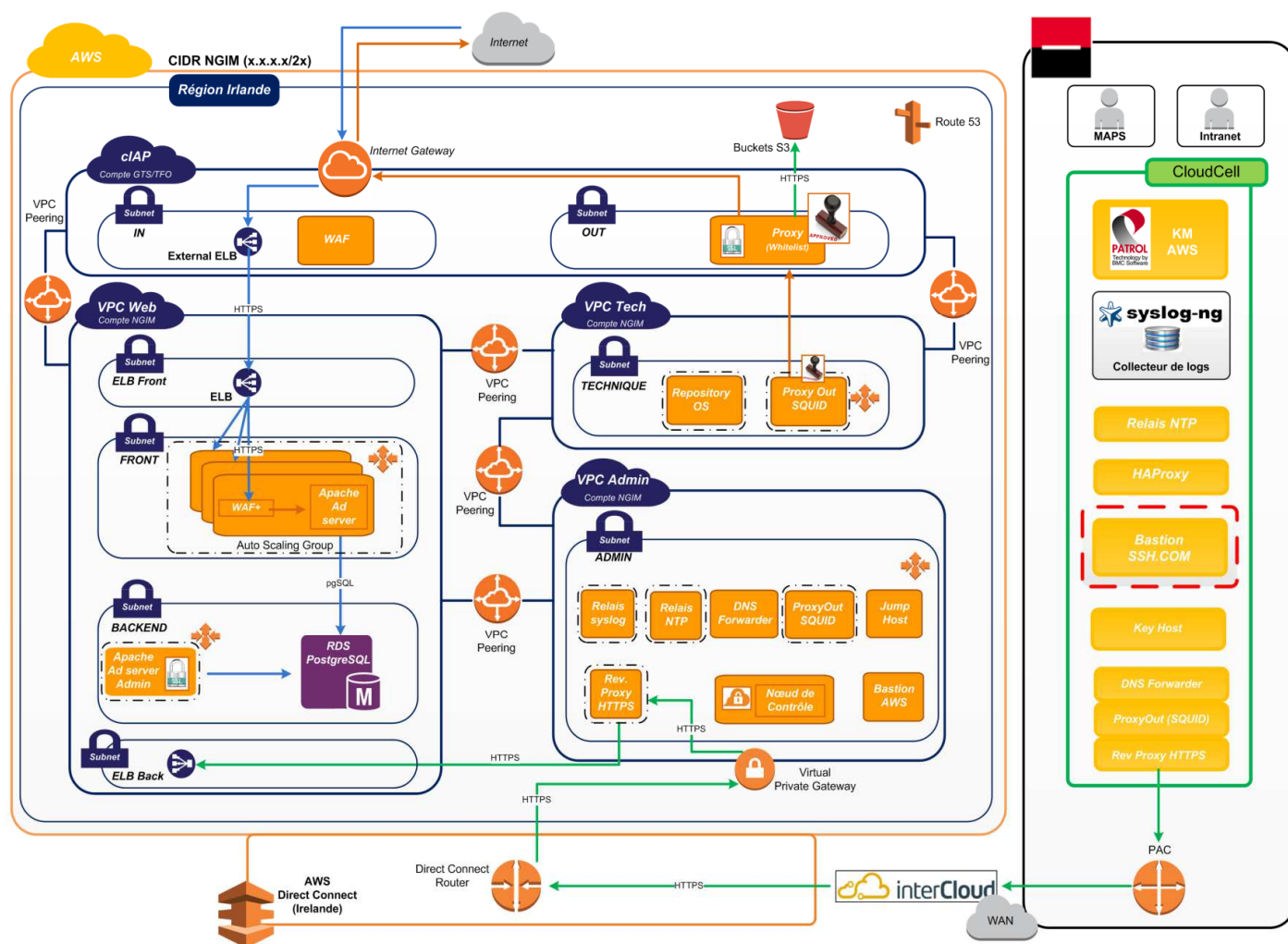
### 4.1 Description générale

Ci-dessous un schéma représentant l'architecture réseau logique appliquée en production pour l'application NGIM lot 3 Ad Server.

Elle sera reproduite dans les environnements HML et DEV.

On y retrouve :

- ✓ La Cloudcell et ses différentes servitudes techniques
- ✓ L'interconnexion AWS – SG basée sur le Direct Connect et le PAC
- ✓ Les différents VPC et les composants qui y sont hébergés.
- ✓ Les principes de peering entre VPC
- ✓ Les Virtual Interface Gateway montées sur les VPC qui le nécessitent
- ✓ L'Internet Gateway sur le cIAP



## 4.2 Matrice de flux applicatifs avec une vision infrastructure

Ref Flux *	Source	Localisation	Destination	Localisation	Port	Protocole
Flux : 1 Clients internet vers Revive promotion	Navigateur client	Internet	ELB public	VPC cIAP	443	HTTPS
	Subnet Privé cIAP	VPC cIAP	ELB Front	VPC Web / Subnet ELB Front	443	HTTPS
	ELB Front	VPC Web / Subnet ELB Front	Instances EC2 Front (Revive promotion)	VPC Web / Subnet Front	443	HTTPS
Flux : 5 Accès BDD serveurs Revive promotion	Instances EC2 Front (Revive promotion)	VPC Web / Subnet Front	Instance RDS Revive	VPC Web / Subnet Backend	5432	TCP
Flux : 3 Clients SG (ME, Marketing) vers Revive Administration	PDT SG	Any RDS	Reverse Proxy Apache (PAWSLX01)	CloudCell	443	HTTPS
	Reverse Proxy Apache (PAWSLX01)	CloudCell	ELB Rev Prox AWS	VPC Admin / Subnet Admin ELB priv	443	HTTPS
	ELB Rev Prox AWS	VPC Admin / Subnet ELB priv	Instance EC2 Rev Prox AWS	VPC Admin / Subnet Admin priv	443	HTTPS
	Instance EC2 Rev Prox AWS	VPC Admin / Subnet Admin priv	ELB Revive Admin	VPC Web / Subnet ELB Backend	443	HTTPS
	ELB Revive Admin	VPC Web / Subnet ELB Backend	Instance EC2 Revive Admin	VPC Web / Subnet ELB Backend	443	HTTPS
	PDT SG	Any RDS	Plateforme SAFE via le SIPO (SAML v2)	CITSv2 (TIG/MCS/SEC)	443	HTTPS
Flux : 4 Accès BDD serveurs Revive Administration	Instances EC2 Backend Revive Administration	VPC Web / Subnet Backend	Instance RDS Revive	VPC Web / Subnet Backend	5432	TCP

(\*) : Référence du flux correspondant à la matrice applicative de la section **Erreur ! Source du renvoi introuvable.**

### 4.3 Matrice de flux techniques

Flux	Source	Localisation	Destination	Localisation	Port	Protocole
NTP	ALL EC2	ALL VPC	Relais NTP	VPC Admin	123	UDP
	Relais NTP	VPC Admin	Relais NTP	CloudCell	123	UDP
	Relais NTP	CloudCell	Serveur NTP Interne	Intranet CITS	123	UDP
Logs systèmes	ALL EC2	ALL VPC	Relais syslog-ng	VPC Admin	514	TCP
	Relais syslog-ng	VPC Admin	Relais syslog-ng	CloudCell	514	TCP
	Relais syslog-ng	CloudCell	Log4ALL	Intranet CITS	514	TCP
Key Secure	ProtectV Manager	VPC Admin	HAProxy	VPC Admin	443	HTTPS
	HAProxy	VPC Admin	HAProxy	CloudCell	443	HTTPS
	HAProxy	CloudCell	Boitiers HSM	DMZ L3	443	HTTPS
Accès SSH	Jump Host	VPC Admin	ALL EC2	ALL VPC	22	SSH
	Key Host	CloudCell	Jump Host	VPC Admin	22	SSH
	Bastion SSH.COM	CloudCell	Key Host	CloudCell	22	SSH
	Rebond MAPS	Zone MAPS	Bastion SSH.COM	CloudCell	22	SSH
	PDT SG	NDG VDF Les Dunes, Delta, Julia, Borea	Bastion SSH.COM	CloudCell	22	SSH
DNS (SI SG vers AWS)	DNS Interne SG	RDS	DNS Forwarder	CloudCell	53	UDP
Accès aux API AWS *	PDT SG	Any RDS	Proxy Squid (PAWSLX01)	CloudCell	3128	HTTPS
	Proxy Squid	CloudCell	Proxy Squid	VPC Admin	443	HTTPS
	Proxy Squid	VPC Admin	Proxy Squid	VPC Tech	443	HTTPS
	Proxy Squid	VPC Tech	Proxy Squid	cIAP	443	HTTPS
	Proxy Squid	cIAP	API AWS	AWS (Internet)	443	HTTPS
Supervision	Agent Patrol AWS	CloudCell	Proxy Squid	CloudCell	3128	HTTPS
	Proxy Squid	CloudCell	API CloudWatch (via chaîne accès aux API AWS)	AWS	443	HTTPS

(\*) : whitelist des API AWS et endpoint S3 gérée au niveau du proxy Squid Tech et proxy Squid cIAP

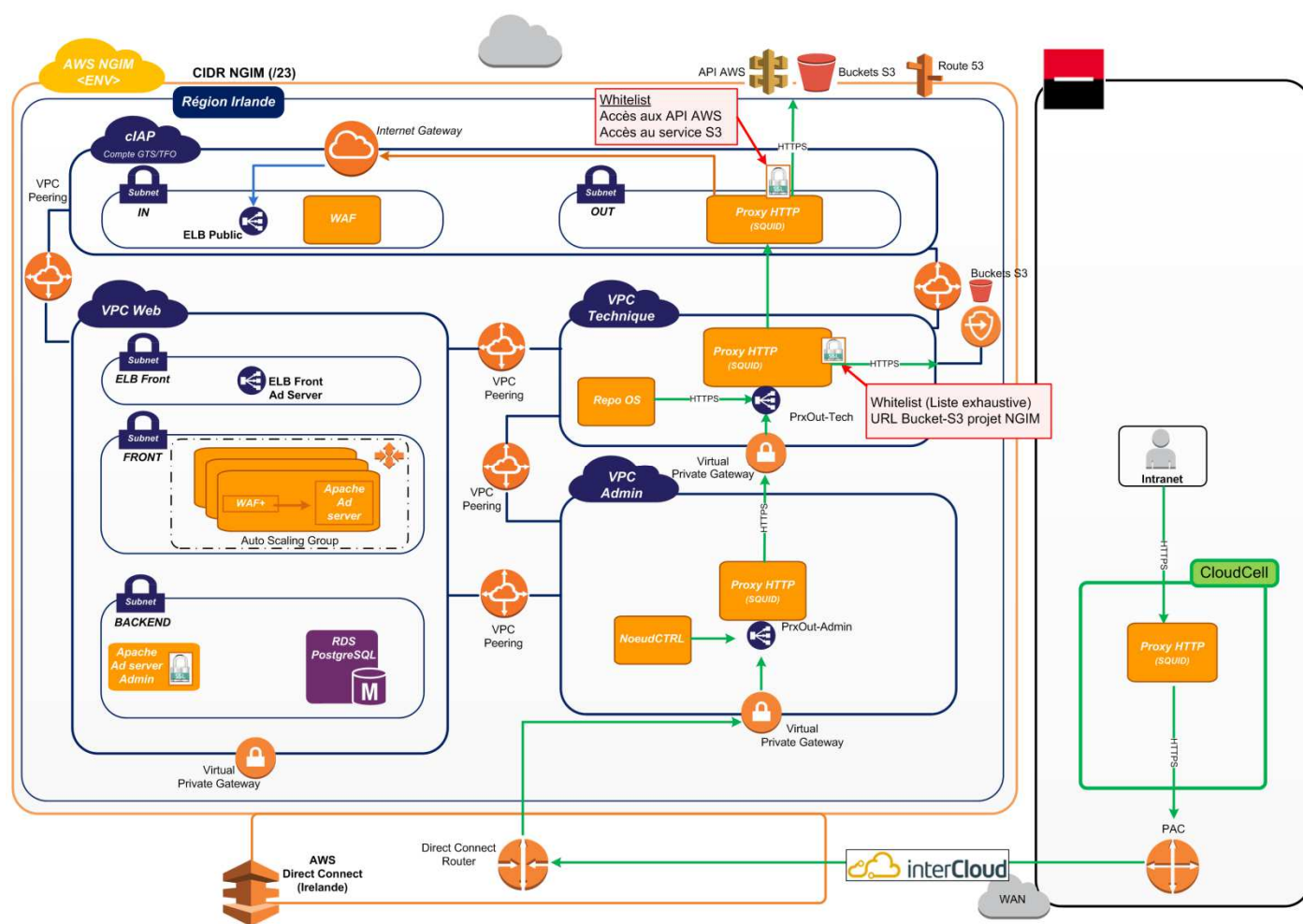
Note : cette matrice devra se voir ajouter les flux techniques qui rentrent en jeu dans la mécanique de chiffrement de l'OS NTSS.

#### 4.4 Cinématique d'accès aux API AWS

La solution identifiée à ce jour se base sur un chainage de proxy Squid ayant pour objectifs

- 1- L'accès aux buckets S3 du projet via le endpoint S3 connecté au VPC Tech. Ce flux est routé vers le endpoint S3 en sortie du proxy Squid du VPC Tech. Celui-ci est autorisé sur la base d'un filtrage d'URL exhaustives des buckets S3 du projet (whitelist). La whitelist est à la main du projet
- 2- Autoriser l'accès aux API AWS via le proxy Squid du cIAP

La cinématique est décrite par le schéma ci-dessous :



 <p>BUILDING TOGETHER TEAM SPIRIT SOCIÉTÉ GÉNÉRALE ITIM – GTS/RET</p>	<p>Projet NGIM lot 3 Ad Server</p> <p>Dossier Architecture Hébergement</p>	 <p>Diffusion interne SG</p>
--	--	--

## 4.5 Cloudcell

La Cloudcell est une DMZ du SI SG reliée au PAC et permettant de proxifier tous les échanges avec les services AWS.

Pour les besoins de NGIM, la Cloudcell hébergera les servitudes suivantes :

- ✓ Proxification des flux HTTPS entre AWS et Société Générale
- ✓ Collecte des logs systèmes
- ✓ Redirection des flux à destination des boîtiers HSM pour le chiffrement des instances EC2
- ✓ Rebond SSH du SI interne SG vers AWS
- ✓ Gestionnaire de clés SSH (basée sur l'agent SSH)
- ✓ Supervision et Métrologie
- ✓ Synchronisation NTP des instances AWS avec l'horloge du SI Interne SG

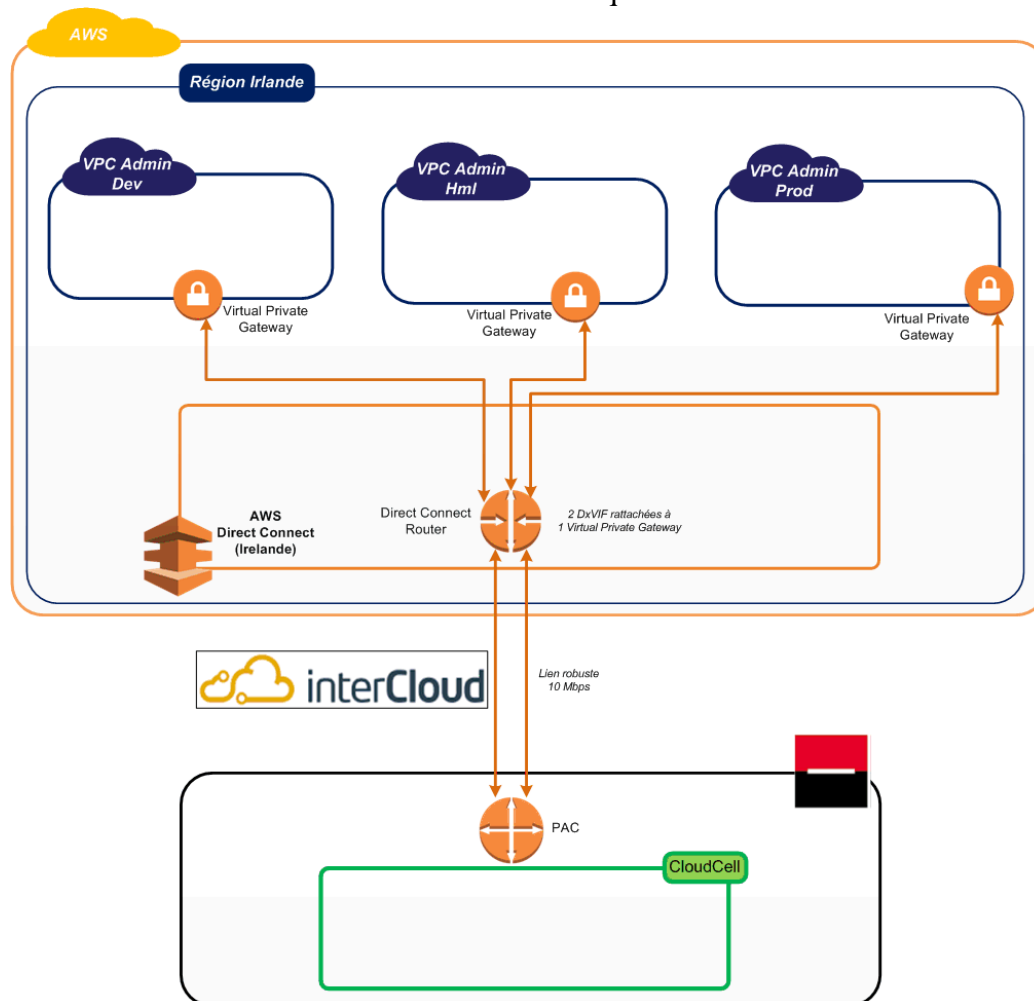
### Note :

*Le projet NGIM utilisera en tactique la Cloudcell ayant servi pour le POC AWS. Les servitudes NGIM devront migrer vers la Cloudcell cible qui sera hébergée dans le Cloud GTS.*

#### 4.6 Interconnexion Société Générale – AWS

Le SI SG est interconnecté avec le Cloud Amazon via le PAC, cette interconnexion est opérée par InterCloud. Le PAC est déployé en Geocluster sur deux sites (Tigery et Seclin2).

Côté Amazon Web Services, c'est le DirectConnect qui permettra le routage des flux d'échange entre les VPC d'admin et le SI SG. Pour NGIM, 3 DxVIF (Virtual Private Gateway) seront utilisées pour le routage des flux vers les 3 VPC d'admin Dev/Hml/Prod comme indiqué dans le schéma suivant :

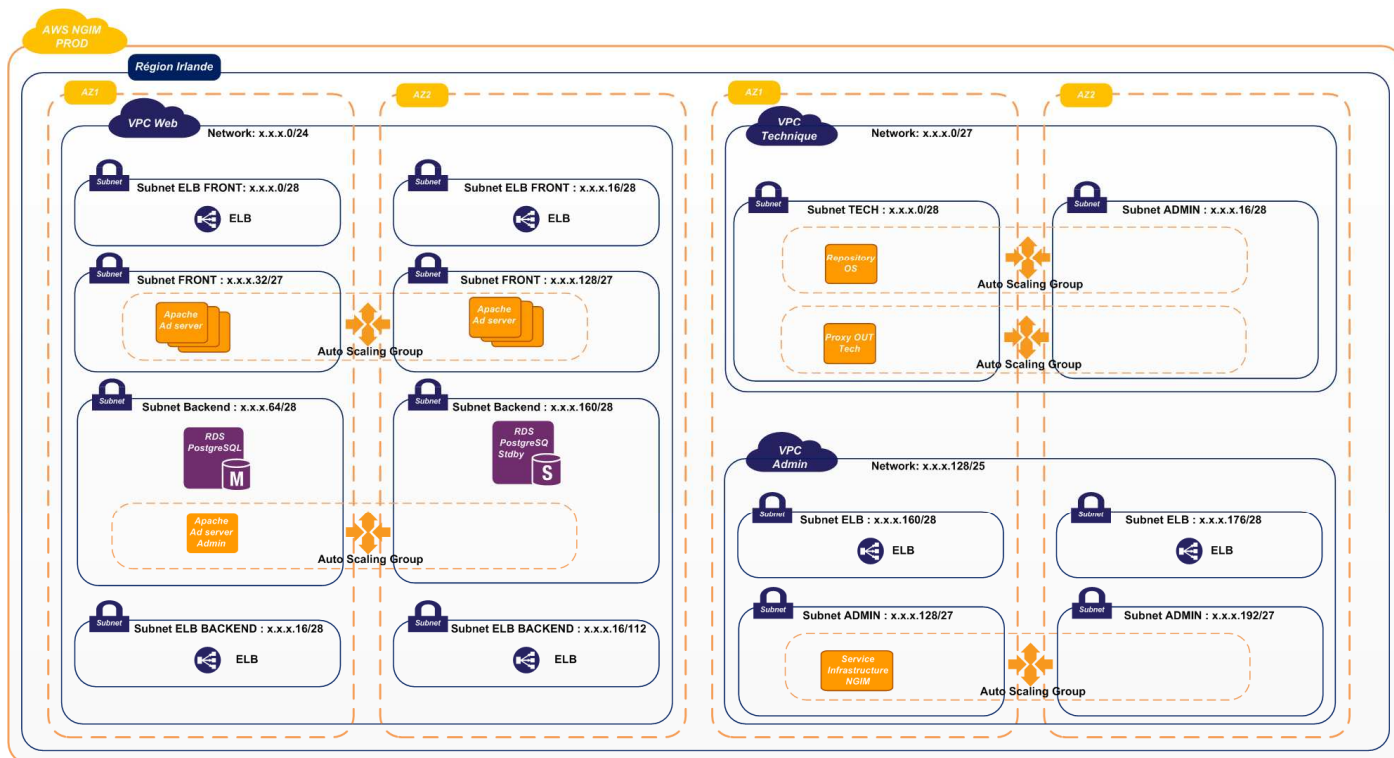


#### Notes :

- 1- L'adressage utilisé chez Amazon sera de type SGNA
- 2- Les flux SG → AWS ne seront pas NATés
- 3- Les flux AWS → SG seront NATés en 1:1 au niveau du PAC

## 4.7 Urbanisation réseau chez AWS

Le schéma suivant décrit la répartition des subnets par VPC et par zone de disponibilité pour les environnements HML/PROD de NGIM :



### Note :

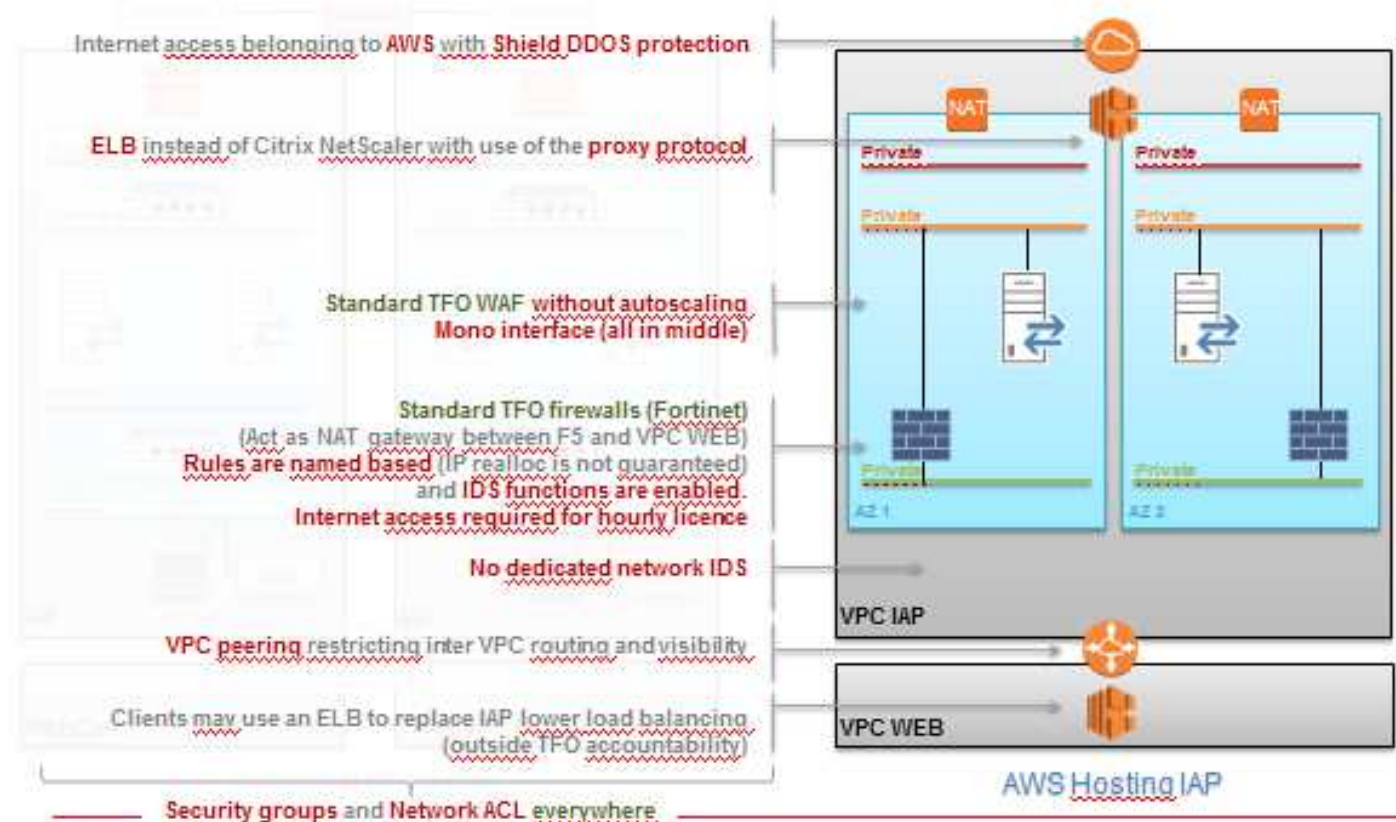
- 1- le même découpage réseau sera appliqué à l'environnement de développement mais sur une seule AZ.
- 2- Le cIAP est lui aussi étendu sur 2 AZ avec un plan d'adressage global de taille /20.



#### 4.8 Interconnexion Internet – NGIM

Les échanges entre les VPC NGIM et Internet se feront via le VPC cIAP. Celui-ci est construit avec un compte AWS de GTS/TFO et sera mutualisé entre plusieurs projets.

Ci-dessous le HLD du cIAP déployé en production :



L'application NGIM bénéficie par défaut de la protection anti-DDoS [AWS Shield Standard](#). Des études sont en cours pour l'implémentation de la version avancée.



## 5 ARCHITECTURE D'HEBERGEMENT DES SERVITUDES POUR AWS

### 5.1 Description générale des servitudes techniques

Afin d'interconnecter les ressources instanciées chez AWS au réseau interne, un ensemble de servitudes techniques doivent être mises en œuvre dans la Cloudcell, zone d'interconnexion entre les Cloud Providers et la Société Générale.

Cette Cloudcell (tactique et/ou cible) devra permettre d'adresser les besoins suivants :

- ✓ Proxyfication des flux HTTPS entre AWS et Société Générale
- ✓ Collecte des logs systèmes
- ✓ Redirection des flux à destination des boîtiers HSM pour le chiffrement du nœud de contrôle (NTSS)
- ✓ Rebond SSH du SI interne SG vers AWS
- ✓ Supervision et Métrologie
- ✓ Synchronisation NTP des instances AWS avec l'horloge du SI Interne SG
- ✓ Résolution DNS des ressources AWS à partir du SI SG

Pour NGIM lot 3 Ad server, chacun de ces services sera hébergé dans une VM technique dédiée déployée au sein de l'ESX rattaché à la Cloudcell tactique (DMZ I2BD)

Pour la matrice des flux cf [§4.3](#)

### 5.2 Servitude « Reverse Proxy »

La solution se base sur une VM hébergeant un serveur Apache installé selon les normes GTS/RET sous le trigramme « AWS ».

Le reverse proxy des URL est configuré dans le fichier de configuration situé sous conf/extra/httpd-proxy.conf

### 5.3 Servitude « Proxy »

Elle permet de proxifier les flux HTTPS vers les API AWS et les buckets S3 du projet. La solution se base sur un Squid déployé sur la même VM que la servitude « Reverse Proxy ». La chaîne proxy et toute la cinématique associée sont détaillés au [§4.4](#).

### 5.4 Servitude « DNS Forwarder »

La solution repose sur l'installation du composant dnsmasq sur la VM qui héberge déjà les servitudes « Reverse Proxy » et « Proxy ». Cette servitude permet la résolution DNS des ressources AWS à partir de la CloudCell.

### 5.5 Servitude « Collecte des logs systèmes »

La solution est déployée au sein d'une VM dédiée instanciée sur la Cloudcell.

Les pré-requis, binaires ainsi que la configuration associée de la servitude doit être instruite avec GTS/STP/OSM.

## 5.6 Servitude « Redirection des flux Keystores »

Pour récupérer les clés de chiffrement utilisé pour sécuriser les credentials sur le nœud de contrôle, la solution repose sur une VM dédiée hébergeant un HAProxy et redirigeant les flux vers les Keystores GTS/RET.

En production, il y a deux keystores, le mode de répartition de charge choisi entre les keystores est actif/actif

## 5.7 Servitude « Bastion SSH »

### 5.7.1 Généralités

Les exigences de sécurité nécessitent le déploiement d'une solution de bastion permettant de tracer tous les flux d'administration entre AWS et Société Générale, l'objectif étant d'implémenter une politique renforcée de gestion d'identifications et d'habilitations.

En cible, le programme SIGMA a identifié le produit CyberArk pour répondre à ce besoin, cependant cette solution n'est pas disponible à ce jour.

Dans le cadre de NGIM lot 3 Ad Server, ITIM et GTS/RET ont choisi d'implémenter la solution CryptoAuditor de la société SSH.COM.

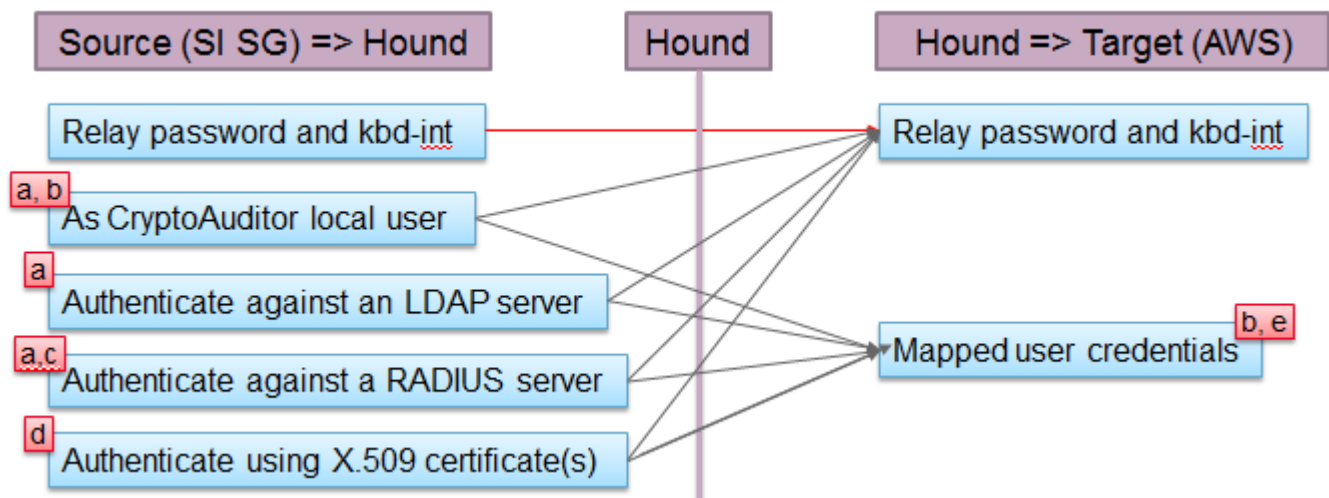
### 5.7.2 CryptoAuditor : protocoles pris en charges et fonctionnalités

CryptoAuditor permet d'auditer les flux SSH, RDP, HTTP en mode « bastion » (coupure) ou « furtif » (router ou bridge).

**Table 3.3. Supported monitored protocols and capabilities**

Capability	SSH	RDP	TCP <sup>a b</sup>	HTTP <sup>c</sup>
Control of subchannels	Yes	Yes	No	N/A <sup>d</sup>
Store data	Yes	Yes	Yes	Yes
Index & Free-text keyword search	Yes	Yes	Yes	Yes
View as text	Yes	Yes <sup>e</sup>	Yes	Yes
Replay as video	Yes	Yes	No	No
Download transferred files	Yes <sup>f</sup>	Yes <sup>g</sup>	No	Yes
Send to DLP/AV via ICAP	Yes	No	Yes	Yes
Send to IDS	Yes	No	Yes	Yes

### 5.7.3 CryptoAuditor : Gestion des authentifications en mode bastion



- ✓ a: La configuration du client SSH doit au moins avoir comme méthode d'authentification favorite "keyboard-interactive".
- ✓ b: l'authentification par clé publique est supportée pour SSH
- ✓ c: Cette option n'est pas disponible dans le mode "FIPS"
- ✓ d: SSH seulement, cette option peut être utilisée si l'utilisateur s'est authentifié à l'aide d'une smart card (PIV/CAC) qui contient un certificat de type X.509.
- ✓ e: Si le mot de passe pour l'utilisateur en question n'est pas spécifié dans le système CryptoAuditor, l'utilisateur doit entrer dans mot de passe.

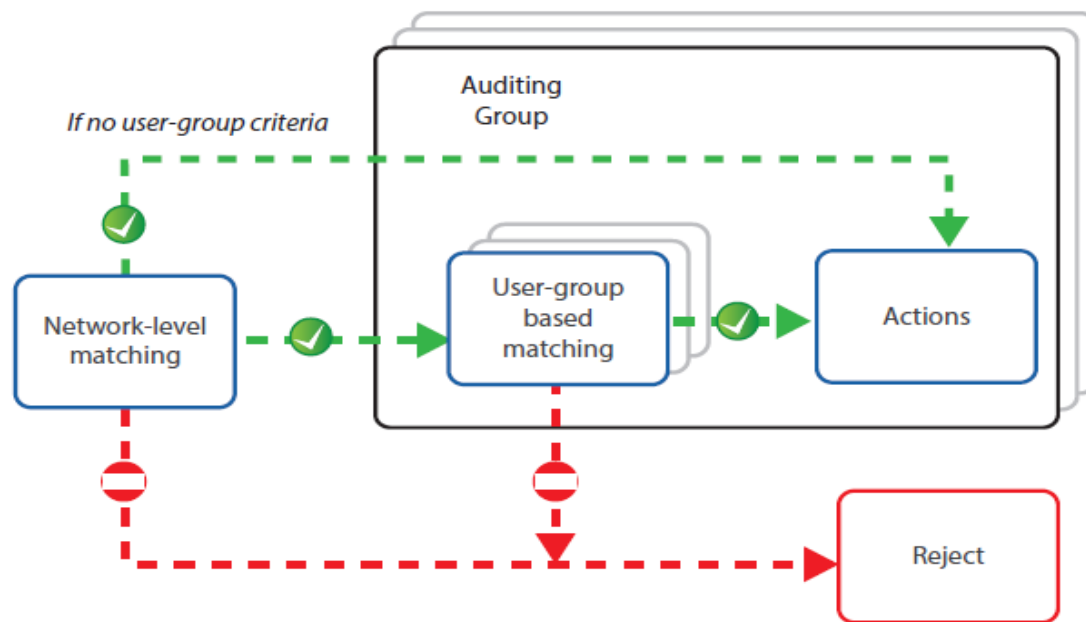
### 5.7.4 CryptoAuditor : Règles pour les utilisateurs et groupes d'utilisateurs

Les règles d'audit peuvent s'appuyer sur deux types de critères :

- ✓ Réseau: IP source, IP destination, Port de destination, VLAN ID, Listener sur le Bastion
- ✓ User Groups: identité de l'utilisateur

L'utilisation de « User Group » permet :

- ✓ D'associer un utilisateur cible distinct de l'utilisateur source
- ✓ Associer un même utilisateur cible à plusieurs utilisateurs source
- ✓ Masquer les informations d'authentification sur le serveur cible
- ✓ Changer le type d'authentification



### 5.7.5 CryptoAuditor : Gestion des utilisateurs

#### ✚ Utilisateurs

- ✓ Les utilisateurs sont définis en local à CryptoAuditor (dans le Vault)

#### ✚ Utilisateurs locaux et groupes

- ✓ On peut affecter une ou plusieurs clefs publiques
- ✓ N'a pas nécessairement un mot de passe si une clef publique est définie
- ✓ Les utilisateurs peuvent être rassemblés dans des « User Groups » sur lesquels seront appliquées des règles

#### ✚ Correspondance utilisateurs source vs utilisateurs cible

- ✓ L'association est faite au niveau du « User Group » via un « User Mapping »
- ✓ Le « User Mapping » permet d'associer à un groupe d'utilisateurs donné un identifiant utilisateur distinct sur un « Host Group » cible
- ✓ L'authentification de l'utilisateur cible sur le serveur cible est réalisée comme suit:
  - Stockage du mot de passe dans le « User Mapping »
  - Relais du mot de passe saisi par l'utilisateur source
  - Clef privée avec ou sans passphrase pour les connexions SSH (passphrase stockée dans le « User Mapping »)

#### ✚ Choix de la destination

- ✓ La règle peut, au choix :
  - Diriger l'utilisateur vers le serveur initial
  - Rediriger l'utilisateur vers un serveur et un port fixe

### 5.7.6 Key Host

#### A) Rôle





La mécanique d'authentification des utilisateurs auprès des serveurs AWS choisie est basée sur une gestion des clefs publiques/privées.

Le Key Host a pour rôle :

- ✓ D'authentifier les utilisateurs (authentification par clé)
- ✓ La gestion du mapping users / profil
- ✓ De limiter l'accès des profils d'utilisateurs aux serveurs sur lesquels les clés publiques sont déployées.

#### B) Mapping des utilisateurs

4 types de comptes utilisateurs ont été créés dans l'environnement AWS :

-  ngim\_automation : compte pour les actions de construction par l'automate
-  ngim\_factotum : compte pour les actions de construction par l'humain
-  ngim\_admin : compte pour les actions d'administration sur les composants sur tous les environnements
-  ngim\_team : compte pour les actions d'administration en DEV et de consultation sur les environnements d'homologation et de production

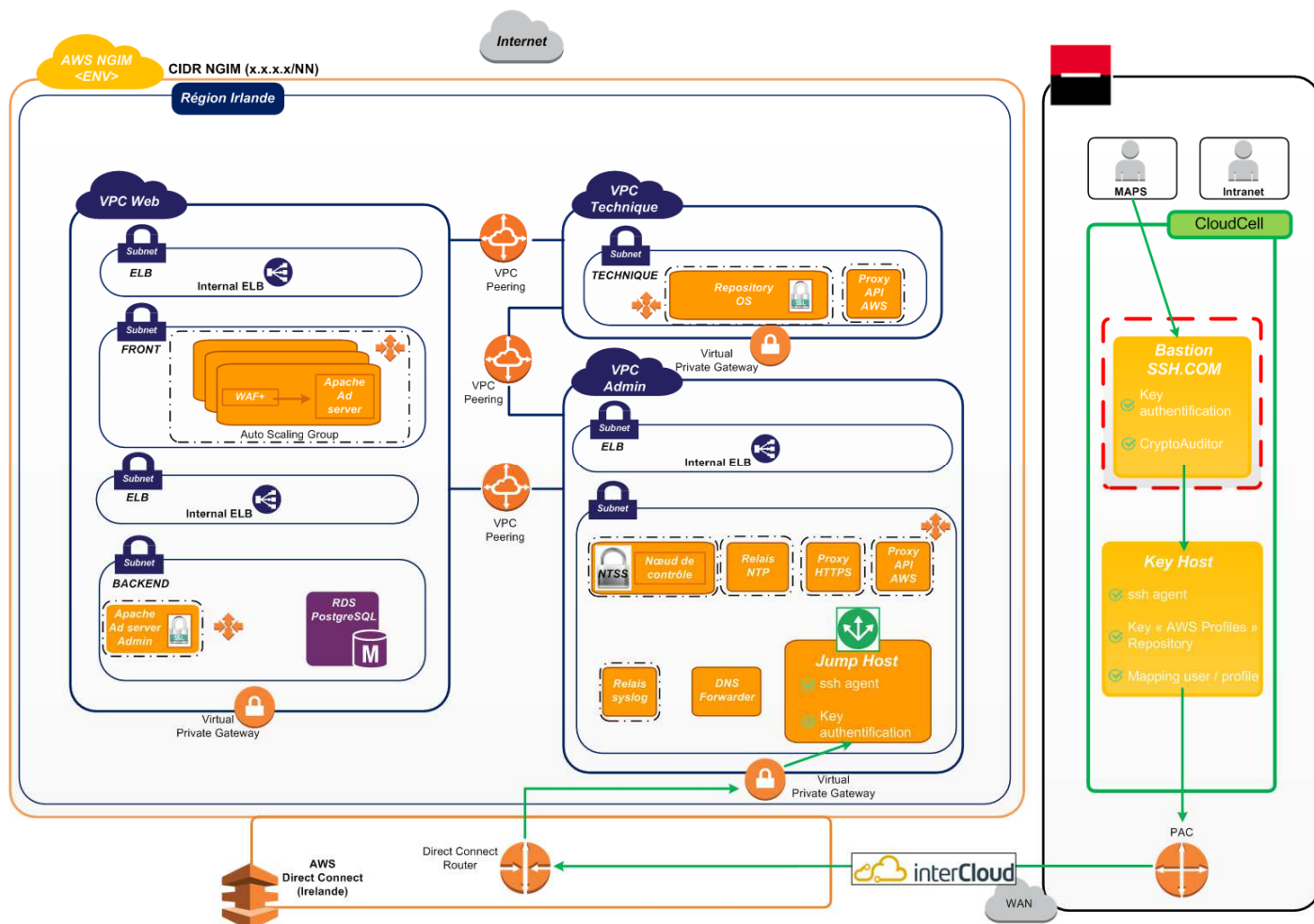
Chaque utilisateur qui se connecte au Bastion avec sa clé privée se retrouve mappé sur le Key Host avec un de ces comptes pour un environnement donné.

### 5.7.7 Jump Host (ou Bastion AWS)

Le « Jump Host » ou « Bastion AWS » est une instance AWS hébergée dans le VPC Admin jouant le rôle de passerelle lors de la connexion SSH depuis le Key Host vers un serveur AWS.

Il véhicule ensuite l'ensemble du trafic entre les deux extrémités dans le cadre de cette connexion.

### 5.7.8 Schéma de la cinématique globale d'accès SSH aux serveurs AWS



## 5.8 *Servitude « Supervision et métrologie »*

### 5.8.1 Principes

AWS propose un service de supervision nommé CloudWatch accessible via API.

La solution de supervision dans le cadre de NGIM lot 3 Ad Server reposera sur une remontée des indicateurs mis à disposition par cette API via la solution GTS/RET BMC Patrol.

### 5.8.2 Solution

Le design de NGIM lot 3 sur AWS propose **une remédiation automatique** pour l'ensemble des composants applicatifs et techniques.

La supervision mise en place consiste à alerter les équipes projet et opérationnelle en cas de :

- ✓ Dysfonctionnement des mécanismes de remédiation automatique
- ✓ Dysfonctionnement applicatif (vue utilisateur)

Synthèse de la solution et cinématique de remontée de la supervision :

- ✓ Un agent de supervision BMC Patrol doté d'un KM AWS (version 1.2.10) sera installé dans la Cloudcell (1 VM dédiée « supervision » contenant 1 agent Patrol par environnement).
- ✓ Celui-ci interrogera régulièrement l'API CloudWatch AWS au travers d'une IAM adéquate et remontera en interne les résultats de la supervision vers PNET
- ✓ Les dysfonctionnements détectés seront remontés en tant que notifications (pas de création de tickets d'incidents automatique auprès des équipes de pilotage de Bangalore)
- ✓ Les dysfonctionnements récurrents (redémarrage en boucle d'une instance) donneront lieu à la création d'une alarme à destination du BT RET/API BAN

### 5.8.3 Cas de dysfonctionnements

#### A) **Dysfonctionnement de l'Autoscaling group**

Il existe plusieurs cas de figure :

- Mauvaise configuration de l'instance qui empêche son démarrage
- Bug applicatif et/ou technique qui fait tomber un composant en erreur de manière récurrente
- Espace de stockage plein qui bloque le système
- Etc ...

Dans tous les cas de figure, le comportement de l'autoscaling group sera le même : il tentera sans limite de redémarrer les instances tant que le nombre minimal d'instance n'est pas atteint.

**Solution** : Un outil développé en python est intégré au KM Commun de l'agent Patrol déployé sur la Cloudcell et aura en charge de superviser la création/suppression des instances d'un autoscaling group. Si le nombre d'évènements dépassent un seuil prédéterminé, une alarme sera générée par l'agent Patrol à destination de Pixel avec création de ticket auprès de l'équipe opérationnelle en charge (RACI à déterminer entre l'équipe projet et RET/API en fonction des composants).



## B) Dysfonctionnement applicatif (vue de l'utilisateur)

Afin de garantir la proactivité des équipes projet et opérationnelle sur un dysfonctionnement du point de vue de l'expérience utilisateur, une supervision applicative basée sur un test de bout en bout de l'application sera déployé.

Cette supervision applicative sera effectuée selon deux axes :

- ✓ Chaîne complète de connexion : Accès depuis Internet à l'URL de test de DCA Revive déployée sur le Front NGIM. Le test sera initié depuis soit :
  - Les sondes Witbe de la B@D
  - L'agent Patrol déployé sur la Cloudcell via la chaîne de Proxy du cIAP Out
  - L'agent Patrol déployé sur la Cloudcell via Sogétoile (routes à ouvrir à date)
- ✓ Chaîne partielle de connexion : Accès depuis l'agent Patrol déployé en Cloudcell à l'URL de test DCA Revive via le Reverse Proxy du VPC Admin. (Permet de valider exclusivement que l'application NGIM est disponible)

### 5.8.4 Flux

L'agent patrol de la Cloudcell doit être en mesure de joindre les adresses AWS suivantes :

Service Amazon	Region Name	Region	Endpoint
Identification	NA	NA	iam.amazonaws.com
Central	NA	NA	monitoring.amazonaws.com <i>Note : Ne correspond a rien côté AWS aujourd'hui</i>
CloudWatch	EU (Ireland)	eu-west-1	monitoring.eu-west-1.amazonaws.com
CloudWatch Events	EU (Ireland)	eu-west-1	events.eu-west-1.amazonaws.com
CloudWatch Logs	EU (Ireland)	eu-west-1	logs.eu-west-1.amazonaws.com
CloudWatch	EU (Frankfurt)	eu-central-1	monitoring.eu-central-1.amazonaws.com
CloudWatch Events	EU (Frankfurt)	eu-central-1	events.eu-central-1.amazonaws.com
CloudWatch Logs	EU (Frankfurt)	eu-central-1	logs.eu-central-1.amazonaws.com

### 5.8.5 Points d'attention

L'agent Patrol AWS se base sur l'appel au service AWS CloudWatch pour la notification et la remontée des alertes vers le pilotage interne SG.

Le service AWS CloudWatch n'a pas à ce jour le niveau de certification attendu par le groupe SG, une étude est en cours avec les équipes de la conformité (cf §3.8.1)

## 5.9 Servitude « Relais NTP »

AWS ne propose pas de service de synchronisation NTP, le fonctionnement de base consiste à se synchroniser avec les sources disponibles sur Internet.

A des fins d'audit, nous devons mettre en place une source de synchronisation NTP fiable et unique pour tous les composants déployés sur AWS.

Les études à ce jour convergent donc vers l'utilisation de sources internes.

Cette servitude se base sur un serveur NTP installé selon les normes GTS/RET/INF ayant pour objectif de relayer vers les instances AWS la synchronisation des horloges depuis les sources interne GTS gérée par GTS/TFO.

### 5.10 Description du socle d'hébergement des servitudes

Le tableau ci-dessous décrit les besoins en termes d'hébergement pour chacune des servitudes dans les différents environnements :

Rôle/Services	Environnement Catégorie	Serveurs	Type	Besoins			Site/CSR	Logiciels installés
				vCPU	RAM	Stockage		
* Rev Proxy HTTPS Flux Sortants SG --> AWS * Proxy Squid Flux Sortants SG --> AWS * DNS Forwarder Flux Sortants SG --> AWS	DEV Servitude applicative	DAWSLX01	VM Factory	1	2	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Apache 2.4.x
Relais HAProxy	DEV Servitude applicative	DAWSLX02	VM Factory	1	2	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits HAProxy
* Rev Proxy HTTPS Flux Sortants SG --> AWS * Proxy Squid Flux Sortants SG --> AWS * DNS Forwarder Flux Sortants SG --> AWS	HOMOL Servitude applicative	HAWSLX01	VM Factory	1	2	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Apache 2.4.x
DNS Masquerade SG --> AWS	HOMOL Servitude applicative	HAWSLX01	VM Factory	1	2	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Apache 2.4.x
Relais HAProxy	HOMOL Servitude applicative	HAWSLX02	VM Factory	1	2	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits HAProxy
* Rev Proxy HTTPS Flux Sortants SG --> AWS * Proxy Squid Flux Sortants SG --> AWS * DNS Forwarder Flux Sortants SG --> AWS	PROD Servitude applicative	PAWSLX01	VM Factory	2	4	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Apache 2.4.x
Relais HAProxy	PROD Servitude applicative	PAWSLX02	VM Factory	2	4	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits HAProxy
Bastion Accès SSH	Servitude Technique	PAWSLX03	VM Factory	2	4	120	Tigery CSR: Cloudcell	OS FreeBSD (appliance) SSH.COM (CryptoAuditor)

BUILDING TOGETHER <b>TEAM SPIRIT</b>  <b>SOCIÉTÉ GÉNÉRALE</b> ITIM – GTS/RET	<b>Projet NGIM lot 3 Ad Server</b> <b>Dossier Architecture Hébergement</b>	 Diffusion interne SG
---	---	---

Relais NTP	Servitude Technique	PAWSLX04	VM Factory	1	2	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Serveur NTP
Concentrateur Syslog-NG	Servitude Technique	PAWSLX05	VM Factory	2	4	150	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Syslog-NG
Key Host	Servitude Technique	PAWSLX06	VM Factory	2	4	150	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Syslog-NG
Supervision AWS	Servitude Technique	PSPVSAAS01	VM Factory	2	16	60	Tigery CSR: Cloudcell	OS Linux RedHat 7.2 64 bits Patrol

## 6 ARCHITECTURE D'HEBERGEMENT DES COMPOSANTS TECHNIQUES

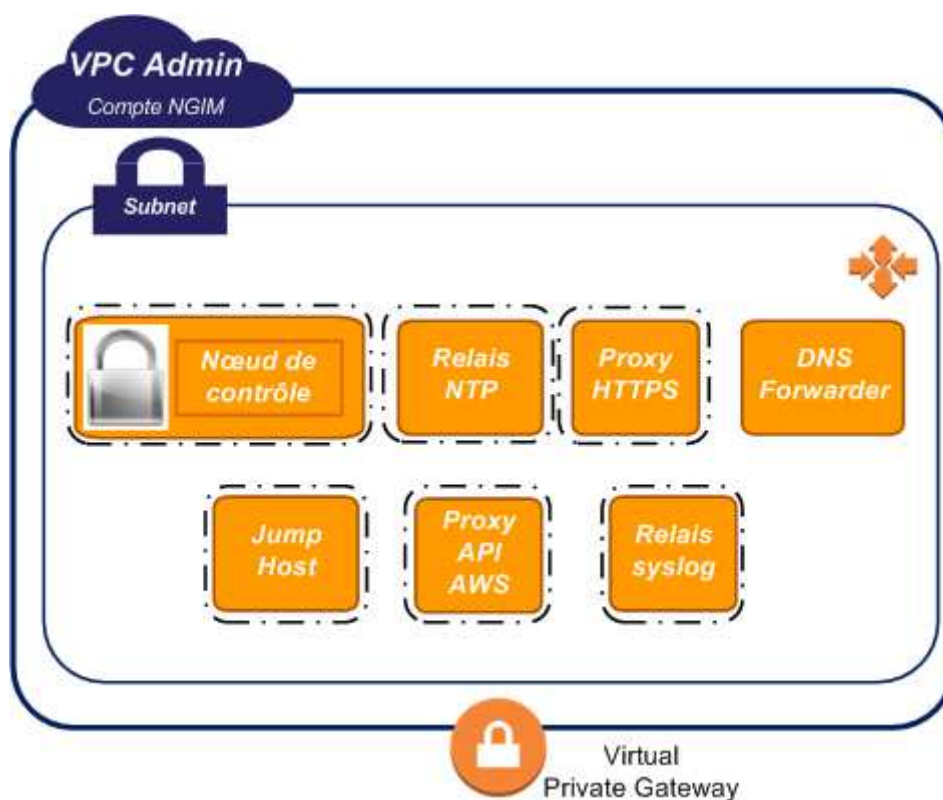
### 6.1 Zone d'hébergement des composants techniques

L'ensemble des composants techniques de NGIM lot 3 Ad Server sont hébergés dans la zone VPC Admin de chacun des comptes AWS (NGIM PROD, NGIM HML, NGIM DEV).

En cible, certains de ces composants pourront être amenés à être hébergés dans des zones transverses.

Afin de permettre à ITIM et GTS/RET d'accomplir leurs missions en phase de construction et en RUN, les composants à mettre en place chez AWS suivants ont été identifiés :

- ✓ Nœud de contrôle
- ✓ Reverse Proxy https
- ✓ Proxy API AWS
- ✓ Jump Host
- ✓ Repository OS
- ✓ Relais NTP
- ✓ Relais syslog



## 6.2 Synthèse des ressources AWS allouées

Composant	Instance AWS	Localisation	Etat	Nom d'instances
Proxy sortant	T2 micro	VPC Technique	Stateless	1
Repository OS	T2 micro	VPC Technique	Stateless	1
Nœud de Contrôle	T2 micro	VPC Admin	Stateless	1
Relais NTP	T2 micro	VPC Admin	Stateless	1
Reverse Proxy https	T2 micro	VPC Admin	Stateless	1
Proxy API AWS	T2 micro	VPC Admin	Stateless	1
DNS Forwarder	T2 micro	VPC Admin	Stateless	2
Jump Host	T2 micro	VPC Admin	Stateless	1
Relais Syslog	T2 micro	VPC Admin	Stateless	1

## 6.3 Résilience des briques techniques

### 6.3.1 Modèle de résilience

Le VPC Admin est étendu sur 2 AZ, les briques sont déployées au sein d'une instance EC2 en A/P sur 2 AZ avec auto-remédiation.

Cela concerne les servitudes AWS suivantes :

- ✓ Nœud de Contrôle,
- ✓ Jump Host,
- ✓ Reverse Proxy HTTP,
- ✓ Proxy API AWS
- ✓ Serveur NTP (Relai vers les serveurs NTP Internes Société Générale),
- ✓ Relais Syslog (collecte des logs systèmes),
- ✓ DNS Forwarder

Le VPC Tech est lui étendu sur 2 AZ, il contient uniquement le référentiel des packages OS et applicatifs déployé au sein d'une instance EC2 en A/P sur 2 AZ avec auto-remédiation.

### 6.3.2 Principes de remédiation

Cf [§9](#)

## 7 ARCHITECTURE D'HEBERGEMENT DE NGIM

### 7.1 Description des socles d'hébergement des composants techniques

#### 7.1.1 Description des types d'instances AWS

Instance AWS	CPU	RAM	Stockage	Bande passante dédiée à EBS (Mbits/s)
t2.micro	1	1	EBS uniquement	Sans objet
t2.large	2	8	EBS Uniquement	Sans objet
m4.large	4	16	EBS uniquement	750

#### 7.1.2 Synthèse des ressources AWS allouées

Composant	Instance AWS	Localisation	Etat	Nombre d'instances	Résilience
Front NGIM (module promotion)	t2.large <sup>(1)</sup>	VPC WEB Subnet Frontend	Stateless	Min=2 <sup>(1)</sup> Max=25 <sup>(1)</sup>	Actif/Actif
Front NGIM (module administration)	t2.micro <sup>(1)</sup>	VPC WEB Subnet Backend	Stateless	1	Standalone
Base de données RDS PostgreSQL	m4.large <sup>(1)</sup>	VPC WEB Subnet Backend	Stateful	2	Actif/Hot Standby







(1) : les benches en homologation ont permis de valider ces valeurs.

### 7.2 Résilience des instances EC2

#### 7.2.1 Solution de remédiation

Cf [§9](#)

#### 7.2.2 Tableau de synthèse de résilience des instances EC2

Instance AWS EC2	Elastic LB	Autoscaling Group	Multi-AZ	Nombre d'AZ	Résilience
Front NGIM (module promotion)				2	Actif/Actif
Front NGIM (module administration)				2	Actif/Passif


### 7.3 *Résilience de la base de données*

#### 7.3.1 Principes

Le service managé RDS PostgreSQL propose le modèle suivant retenu pour ce projet :

- ✓ Deux instances de bases de données (1 sur chaque AZ)
- ✓ Modèle Actif/Hot Standby
- ✓ L'accès à l'instance de base de données s'effectue via un DNS technique en charge de la gestion du failover en cas de défaillance d'une instance
- ✓ Le service managé assure la réplication de données entre les deux instances

#### 7.3.2 Tableau de synthèse

Instance RDS	Multi-AZ	Nombre d'AZ	Résilience	Robustesse
Base PostgreSQL		2	Actif/Hot-Standby	Bascule DNS automatisée

#### 7.3.3 Schéma du modèle de résilience en homologation et production

Cf [4.7](#)



## 7.4 Niveaux de service atteints

Le déploiement des instances EC2 en Multi-AZ permet d'obtenir un taux de disponibilité > 99.95%.

Les services AWS proposent nativement un taux de disponibilité de 99,9999%

Les instances EC2 sont toutes déployées dans un autoscaling group en capacité de les remédier automatiquement.

Le temps de remédiation sera évalué lors des tests de benchs mais nous nous pouvons d'ores et déjà indiquer que les instances peuvent être relancées en cas de défaillance dans un délai de quelques minutes.

Concernant l'instance RDS PostgreSQL, AWS affiche un niveau de disponibilité > 99.95%.

Tableau descriptif des niveaux de services atteintes en fonction des cas de panne :

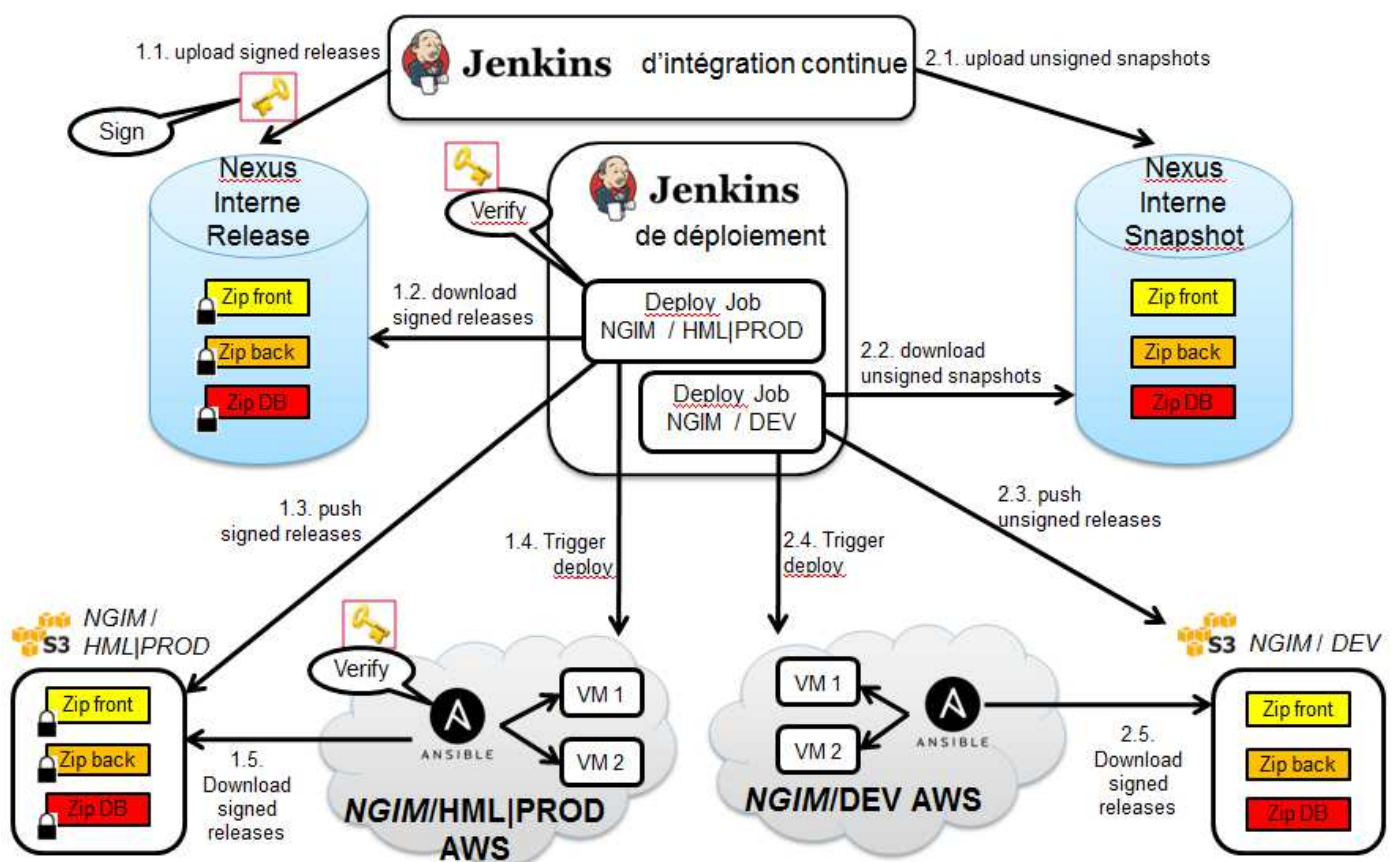
Type de panne	Effet	Mécanismes de robustesse / Actions
Alimentation électrique	Perte d'une ou plusieurs instances	AWS Autoscaling group <ul style="list-style-type: none"> <li>RTO = 0 pour NGIM Front</li> <li>RTO &lt; 1 min pour La base de données, NGIM Admin et les composants techniques</li> </ul>
Perte d'un ou plusieurs disques durs	Perte d'une ou plusieurs instances	AWS Autoscaling group <ul style="list-style-type: none"> <li>RTO = 0 pour NGIM Front</li> <li>RTO &lt; 1 min pour La base de données, NGIM Admin et les composants techniques</li> </ul>
Perte d'un rack de serveurs	Perte d'une ou plusieurs instances	AWS Autoscaling group <ul style="list-style-type: none"> <li>RTO = 0 pour NGIM Front</li> <li>RTO &lt; 1 min pour La base de données, NGIM Admin et les composants techniques</li> </ul>
Perte d'un datacenter ou d'une AZ (ensemble de datacenters)	Perte d'une ou plusieurs instances	AWS Autoscaling group et déploiement sur 2 AZ <ul style="list-style-type: none"> <li>RTO = 0 pour NGIM Front</li> <li>RTO &lt; 1 min pour La base de données, NGIM Admin et les composants techniques</li> </ul>
Perte de la base de données PostgreSQL	Indisponibilité le temps de la bascule (<1min constatée)	Service RDS PostgreSQL déployé sur 2 AZ RTO < 1 min RPO = 0
Détection d'une anomalie au niveau d'un autoscaling group	Dégradation voir arrêt du service concerné	<ul style="list-style-type: none"> <li>Diagnostic à effectuer sur AWS (connexion à la console AWS et/ou au nœud de contrôle chez AWS)</li> <li>Correction d'une configuration applicative et/ou technique</li> <li>Génération d'une nouvelle Image serveur une fois la correction validée</li> <li>Intégration de la nouvelle image dans l'autoscaling group</li> </ul>
Perte de la base de données PostgreSQL et incident lors de la bascule sur le nœud de secours	Arrêt du service NGIM	<ul style="list-style-type: none"> <li>Diagnostic sur la base de données à effectuer sur AWS (connexion à la console AWS et/ou au nœud de contrôle chez AWS)</li> <li>Correction potentielle de la configuration de la base de données (recette Ansible)</li> <li>Réouverture du service</li> </ul>
Corruption de la base de données PostgreSQL	Arrêt du service NGIM	<ul style="list-style-type: none"> <li>Diagnostic sur la base de données à effectuer sur AWS (connexion à la console AWS et/ou au nœud de contrôle chez AWS)</li> <li>Restauration de la base de données à partir du dernier snapshot (RPO=24H)</li> <li>Vérifier la cohérence et l'intégrité de la base de données restaurée</li> <li>Réouverture du service</li> </ul>

## 8 DEPLOIEMENT APPLICATIF

### 8.1 Objectifs

La mécanique de déploiement des applicatifs décrite ci-dessous a pour objectif d'automatiser et de garantir l'origine et l'intégrité des déploiements de NGIM pour environnements d'homologation et de production en signant les packages applicatifs (artéfacts en version release).

### 8.2 Schéma



### 8.3 Cinématique

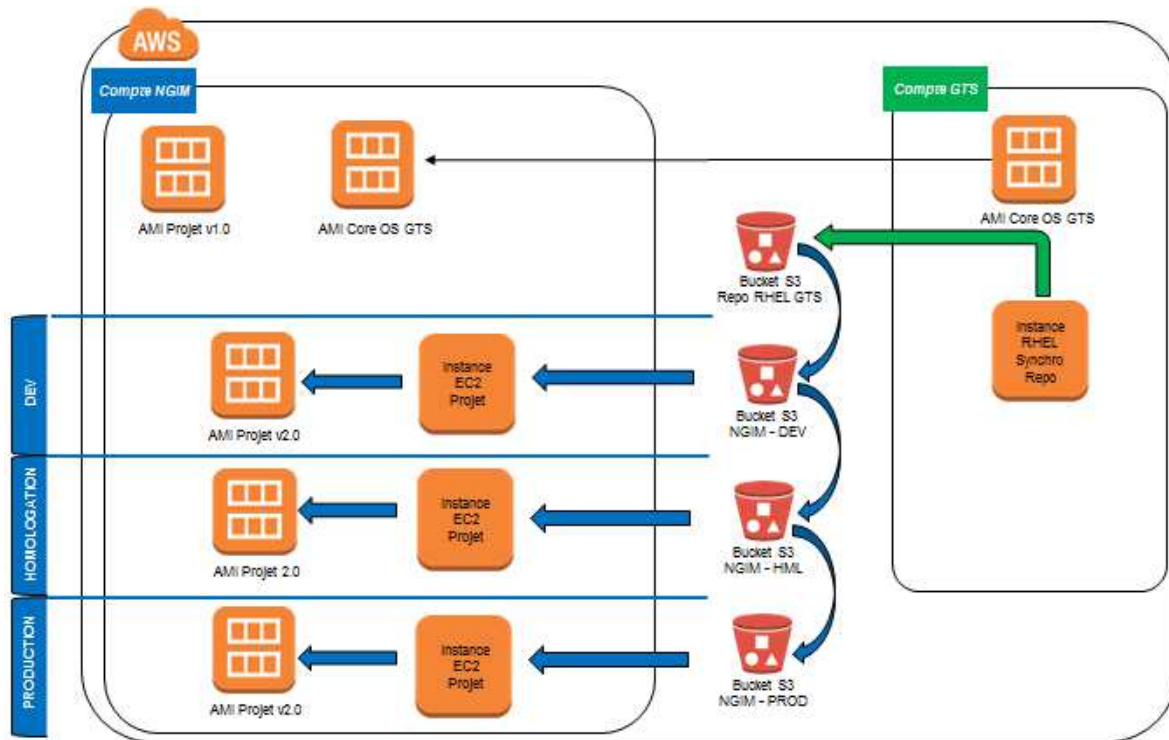
- 1) Jenkins d'intégration continue construit à partir du GIT les packages applicatifs dans le Nexus Interne Release et les signent.
- 2) Jenkins de déploiement pousse dans un bucket S3 les packages applicatifs signés
- 3) Jenkins de déploiement exécute la recette ansible sur le nœud de build associée au package, vérifie sa signature
- 4) Le nœud de build s'appuie sur le Key Store on-premise pour s'authentifier auprès de l'instance destinataire et y déploie le package (ansible mode PUSH)

Note : Des échanges concernant les capacités de remédiation ont lieu au moment de la rédaction de ce document pouvant impacter cette cinématique.

## 8.4 Gestion du changement OS et applicatif

Note : La repository pour NGIM lot 3 n'est à ce jour pas encore déployé dans un bucket S3 (d'où l'instance Repository OS dans le VPC Tech)

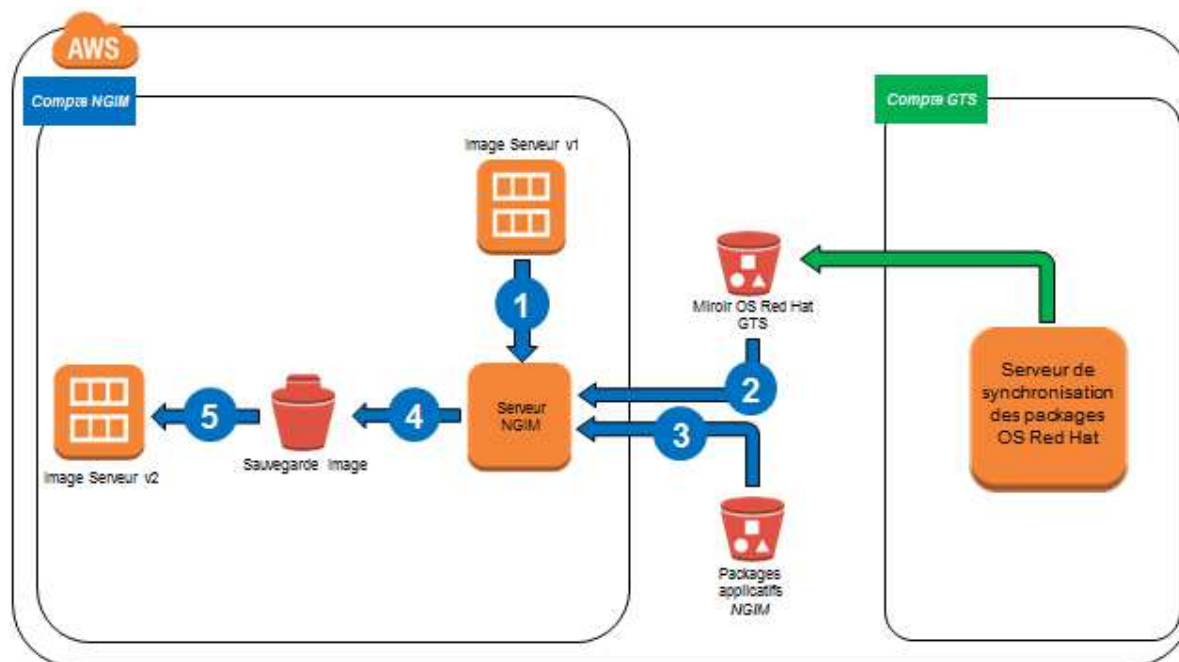
### 8.4.1 AMI Factory (Usine à images)



Flux	Description
1	Création à partir de l'AMI Core OS GTS de l'instance EC2 Projct
2	Configuration OS spécifique au projet et création de l'AMI Core OS Projct
3	Déploiement des packages applicatifs sur l'instance EC2 ou autres composants techniques mis à disposition sur le Repository SocGen
4	Création de l'AMI Projct pour cette instance

- La configuration OS spécifique a pour objectif de mettre en place l'ensemble des spécificités OS pour le projet (comptes, arborescence, etc.)
- Les packages applicatifs comprennent les binaires applicatifs et les fichiers de configurations
- L'AMI projet pour un composant doit être autonome (permet à l'Autoscaling group de remédier de façon autonome une instance à partir de son AMI)
- Le cycle de vie et la gestion des AMI Core OS Projct et des AMI Projct est laissée à la main du projet

## 8.4.2 Cinématique détaillée



Flux	Description
1	Démarrage de l'instance EC2 Projet depuis l'AMI Projet version N
2	Upgrade des packages OS depuis le bucket S3 Repository Red Hat GTS (patches)
3	Upgrade des packages applicatifs depuis le bucket S3 (1 bucket applicatif par environnement)
4	EBS Snapshot de l'instance EC2 Projet
5	Création de l'AMI Projet version N+1 de l'instance EC2 Projet

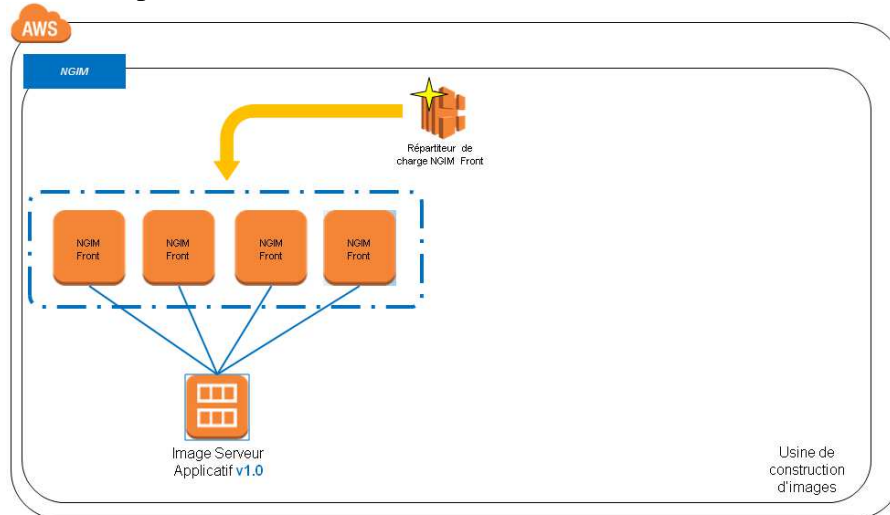
- Le projet est responsable du cycle de vie des AMI Projet de ces instances
- Le Repository Red Hat est rafraîchi automatiquement depuis le compte GTS (Fréquence à définir à date) et contient les derniers patches de sécurité pour la release en question
- Le projet est responsable de l'application des patches de sécurité sur ses AMIs
- Un bucket S3 doit être provisionné par projet et par environnement pour permettre d'appliquer les évolutions/patches selon le circuit recommandé par ITIM/SRO, à savoir DEV => HML => PRD
- La création de l'instance et la génération de l'AMI est exécuté via des recettes Ansible depuis le Nœud de Contrôle

## 8.5 Déploiement blue/green

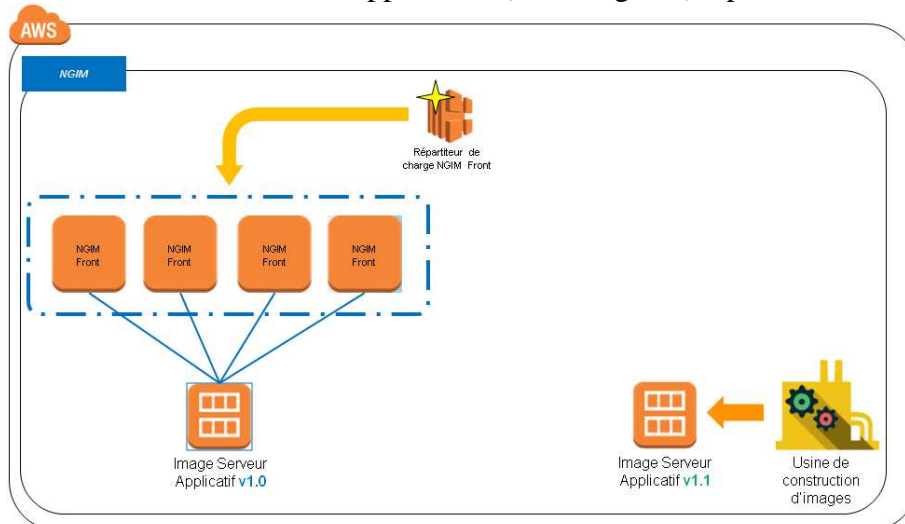
Déploiement de la nouvelle version (green) de l'application en production pendant que la version actuelle (blue) rend le service auprès des utilisateurs.

Une fois la version green validée, l'ELB bascule les requêtes utilisateurs vers la version blue.

Etape 1 : Version actuelle en production (version blue)

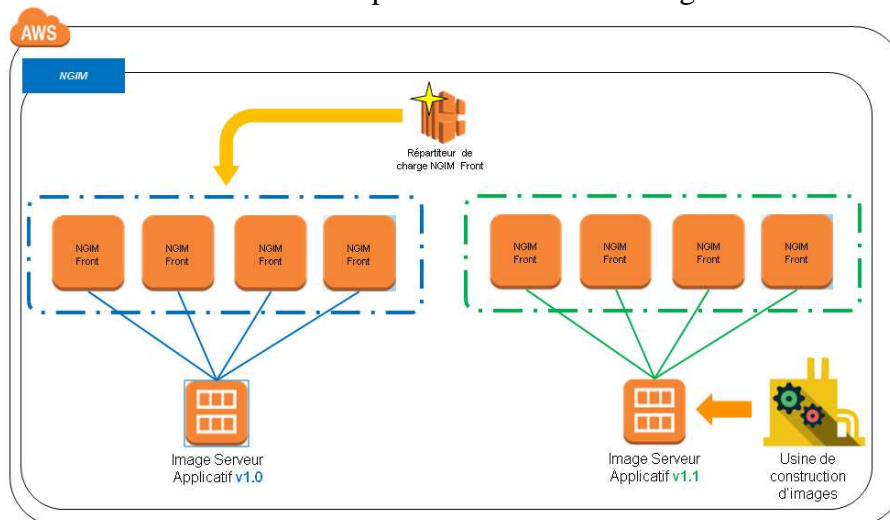


Etape 2 : Construction de la nouvelle version applicative (version green) à partir de l'AMI Factory

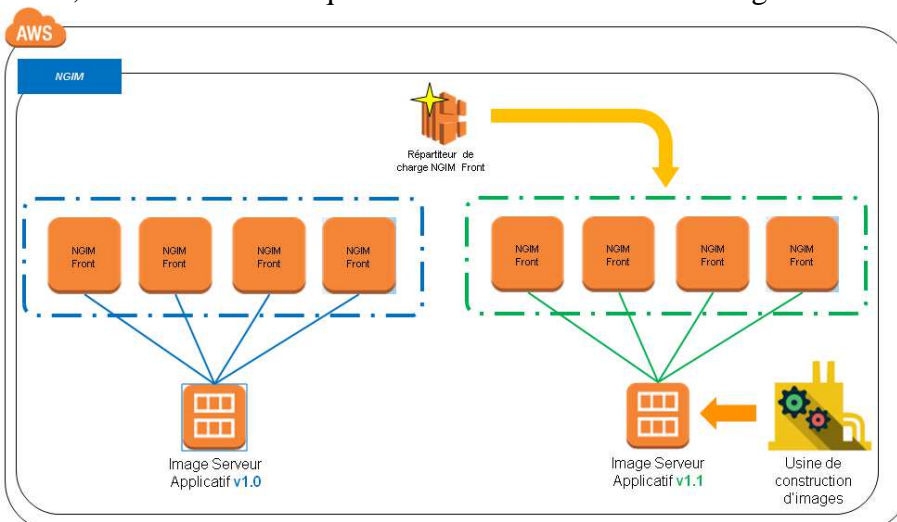




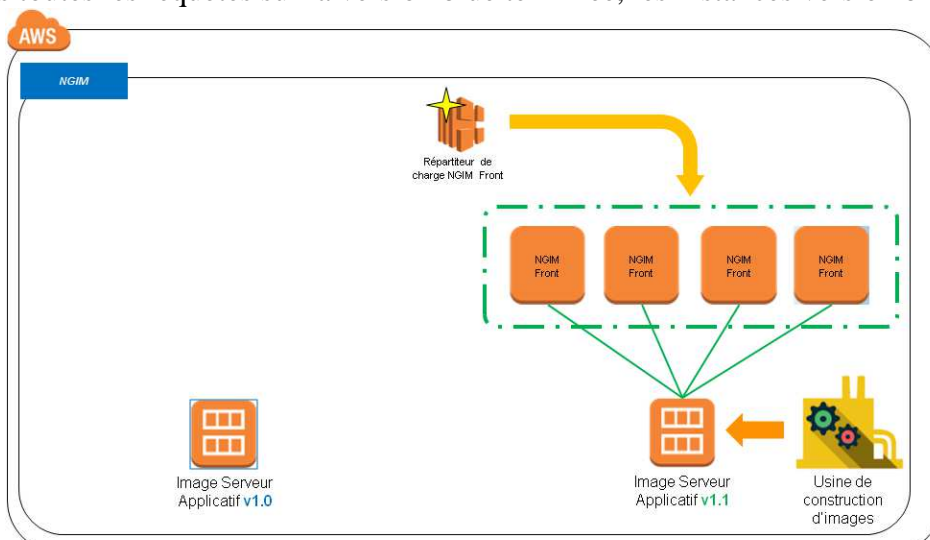
Etape 3 : Construction de nouvelles instances à partir de l'AMI version green



Etape 4 : Une fois testée, l'ELB route les requêtes utilisateurs vers la version green de l'application



Etape 5 : Une fois toutes les requêtes sur la version blue terminée, les instances version blue sont terminées.



## 9 MECANISMES DE REMEDIATION DES INSTANCES EC2

### 9.1.1 Principes

Une AMI projet ici se veut autonome, elle se compose de l'AMI Custom OS du projet et des packages applicatifs nécessaires au fonctionnement d'une brique. Ainsi l'autoscaling group est en mesure de créer de façon complètement autonome une instance à partir de son AMI sans avoir à appeler le Nœud de contrôle pour exécuter les recettes Ansible associées. Ce dernier devient alors un Nœud de « Build » au lieu d'un Nœud de « Contrôle ».

Il est nécessaire de disposer de la dernière version d'AMI pour chaque brique applicative et technique de NGIM. Elles sont construites en phase de BUILD depuis le Nœud de « Build » et ce à chaque évolution qu'elle soit applicative ou technique (release applicative ou technique, patches de sécurité, etc.)

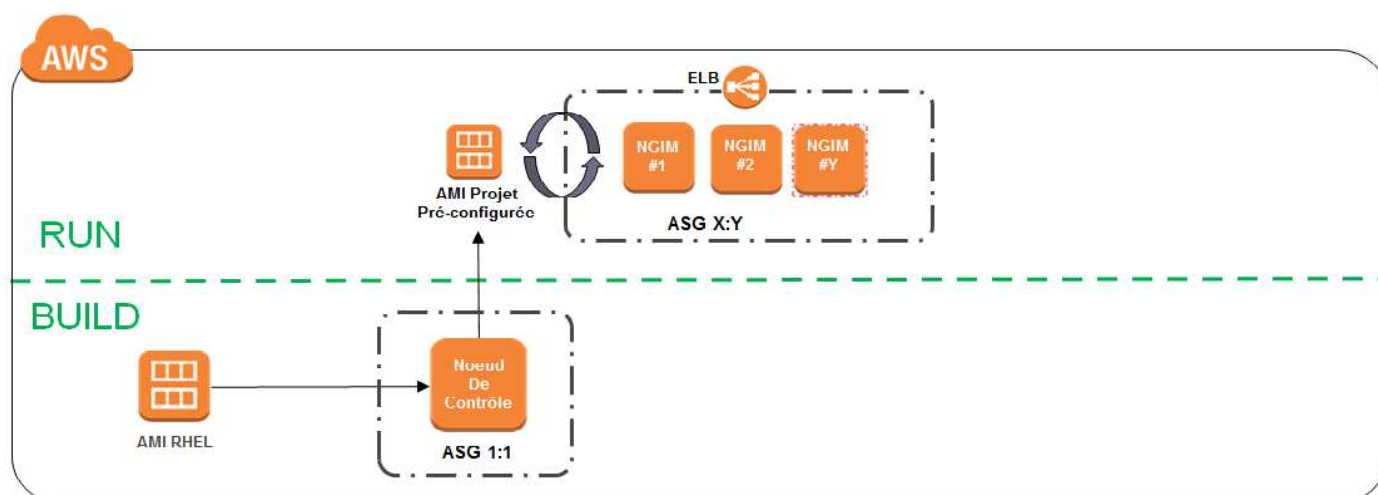
Cette solution concerne toutes les briques sauf le Nœud de « Contrôle » et le DNS Forwarder, ce dernier nécessite une adresse IP fixe, caractère incompatible avec l'autoscaling group.

### 9.1.2 Critères de remédiation

Toutes les briques déployées dans un autoscaling group sont rattachée(\*) à un ELB en amont. Ce dernier effectue un health check à fréquence prédéfinie, au bout de N tentatives échouées, l'ELB considère l'instance comme « malsaine », l'information est automatiquement passée à l'autoscaling group qui démarre une nouvelle instance à partir de la dernière AMI puis détruit l'instance « malsaine ».

(\*) : Sauf le Relais NTP, l'ELB ne prend en charge le protocole UDP pour le health check

### 9.1.3 Cinématique de remédiation



### 9.1.4 Contraintes/Risques Sécurité

Ce scénario requiert l'utilisation des services AWS Autoscaling Group et CloudWatch qui ne sont pas certifiés SOC. Etant donné que NGIM lot 3 n'est pas classifiée PS2E, ces services peuvent être utilisés.



<p>BUILDING TOGETHER</p> <p>TEAM SPIRIT  SOCIÉTÉ GÉNÉRALE</p> <p>ITIM – GTS/RET</p>	<p>Projet NGIM lot 3 Ad Server</p> <p>Dossier Architecture Hébergement</p>	<p></p> <p>Diffusion interne SG</p>
--	--	---

### 9.1.5 Contraintes/Risques Opérationnels

Sans objet

## 10 SECURITE

### *10.1 Gestion des droits et habilitations*

#### 10.1.1 IAM

A compléter

#### 10.1.2 Authentification SAFE sur NGIM Module administration

L'accès au module d'administration de NGIM se fait via une authentification SAFE SAMLV2.

#### 10.1.3 Authentification SAFE sur la console AWS

L'accès à la console AWS se fait via l'API SAMLV2 permettant la fédération avec SAFE.

La mécanique sera décrite plus en détails dans une version ultérieure.

### *10.2 Sécurisation des échanges*

#### 10.2.1 NACL

Cf [§3.6.1.E.1](#)

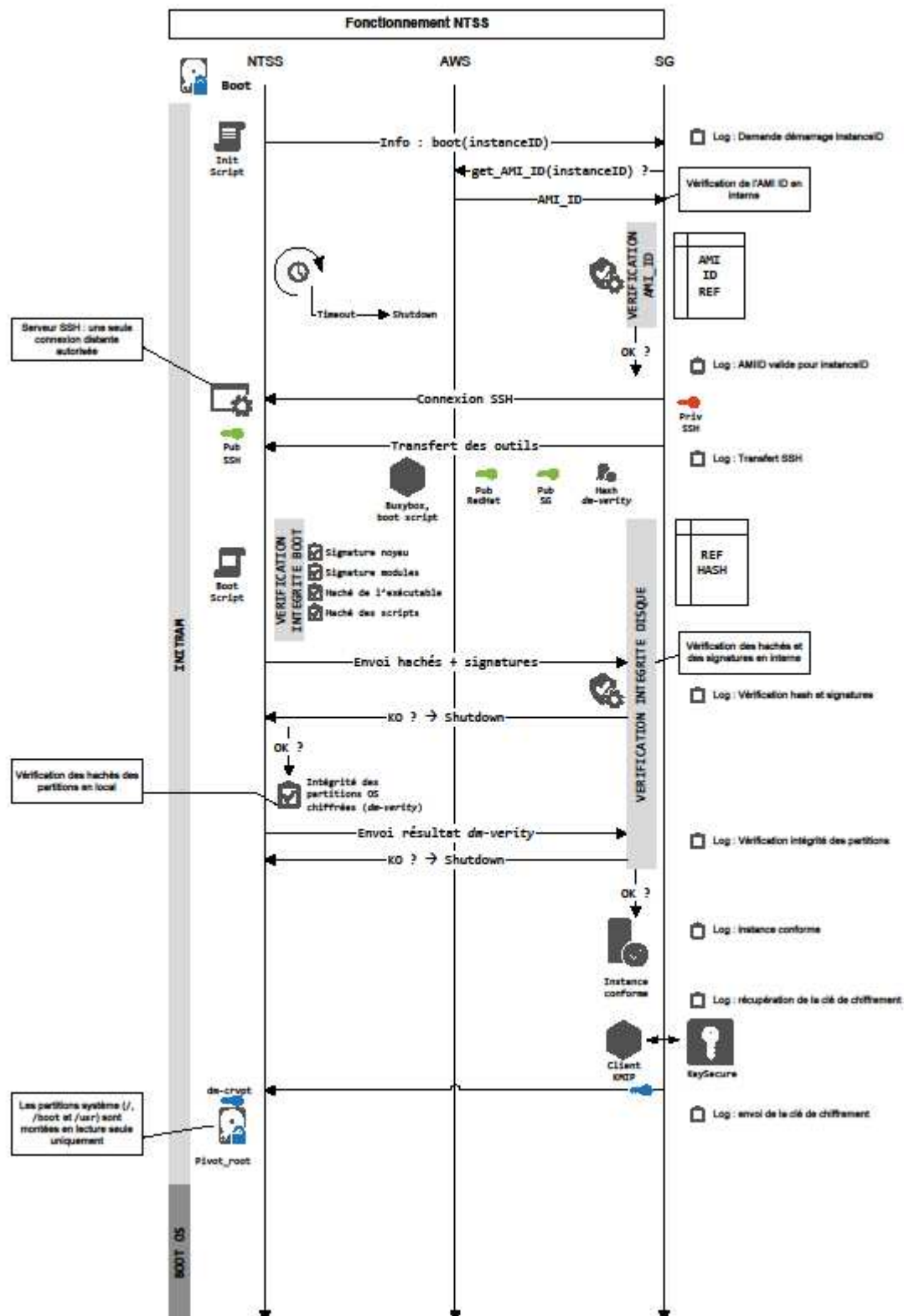
#### 10.2.2 Security Groups

Cf [§3.6.1.E.2](#)

## 10.3 NTSS

Focus sur la cinématique de démarrage d'une instance dont le disque est chiffré par NTSS

V1.0 - 20161202



## 11 EXPLOITABILITE

### *11.1 Cinématique d'accès exploitants et ME aux serveurs AWS*

Les accès SSH aux plateformes AWS seront relayés par le bastion SSH.COM (cf §5.5).

La méthode d'authentification par clef a été retenue, seuls les utilisateurs disposant d'une clef habilité pourront se connecter aux serveurs AWS depuis le Key Host (Cloudcell) et via le Jump Host (Rebond SSH côté AWS).

### *11.2 Supervision*

Cf [5.6](#)

### *11.3 Métrologie*

Cf [5.6](#)

### *11.4 Sauvegarde*

Toutes les instances déployées pour NGIM lot 3 sont stateless à l'exception de la base de données, seule brique à disposer d'une mécanique de sauvegarde basée sur l'exécution de snapshot journalier proposé par le service managé RDS d'AWS.

### *11.5 Collecte des logs*

Toutes les logs systèmes et applicatives sont collectées par syslog et envoyés vers log4all via le Relais Syslog du VPC Admin puis celui de la CloudCell.

### *11.6 Gestion du changement*

Cf [8.4](#)

### *11.7 Gestion des incidents*

Cf [7.4](#)

## 12 ECOLIENCE DE NGIM LOT 3

Une ECOLIENCE est la granularité sur laquelle un exercice de résilience est validé (Robustesse ou Secours). Elle se compose :

- Soit d'un regroupement « d'applications » (ou composants applicatifs) couvrant des fonctions cohérentes pour une activité bancaire donnée,
- Soit d'un ensemble de services techniques transversaux (point d'accès internet, par exemple), eux-mêmes exercisables.

Elle doit pouvoir basculer en toute indépendance pour les composants disposant de solutions de robustesse et/ou de secours.

Elle est conçue avec un découplage sur les flux et a une cohérence garantie des données dans le cadre d'une bascule.

L'écolience des activités de la banque à distance a été définie lors de l'étude « Résilience SDI de la B@ » en 2014 sous la référence E04A.

L'activité métier portée par l'application NGIM Ad server concerne la gestion des campagnes d'auto promotion. Celle-ci est hébergée chez AWS et a été conçue de manière complètement décorrélée des activités de la B@D portées par l'infrastructure on premise. En effet, en cas d'indisponibilité de la plateforme NGIM Ad Server, l'écolience de la B@D E04A continue ses activités sans interruption grâce à un mécanisme de débrayage.

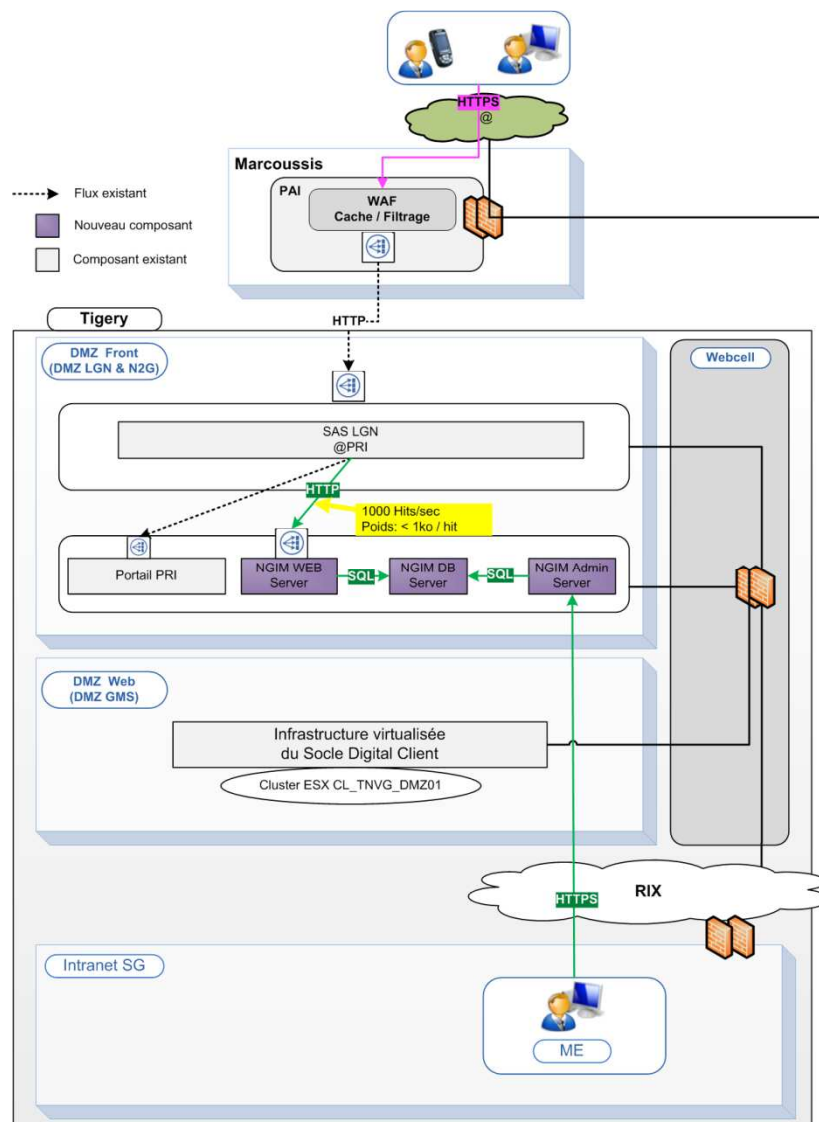
Par ailleurs, l'activité NGIM Ad Server a été évaluée à un niveau de criticité au sens STAMP à secondaire ce qui ne nécessite pas la mise en œuvre d'un secours hors région.

Cependant, l'application NGIM Ad Server est mise en œuvre chez Amazon avec une robustesse multi-AZ décrite dans la section résilience (Cf mécanismes de remédiation [§6](#))

## 13 SOLUTION DE REVERSIBILITE

### 13.1 Description de la solution d'hébergement en interne

La localisation des composants NGIM dans la DMZ LGN de la banque à distance est définie selon les principes d'hébergements établis par le cadre de référence du Socle Digital Client



La solution proposée repose sur une mutualisation du cluster de virtualisation de la DMZ Web, mis en œuvre dans la cadre du Socle Digital Client avec la DMZ Front.

#### Notes:

- ✓ Cette mutualisation servira à créer des VM aussi bien dans les DMZ FRONT (N2G&LGN) et DMZ Web
- ✓ Aucun besoin de pontage (créer des VM multi-zones) => Conservation de l'isolation des zones Front et Web

### ***13.2 Contraintes techniques liées à la solution proposée***

- ✓ Raccordement de la DMZ Front (LGN & N2G) au châssis serveurs de la DMZ Web du Socle Digital Client
- ✓ Utilisation du trunk (standard 802.1Q) pour consolider ce raccordement
- ✓ Mutualisation du cluster de virtualisation VMWare entre les zones Front et Web

### ***13.3 Chemin de migration depuis le Cloud AWS***

Aucune donnée est à récupérer depuis AWS, la base de données Revive peut être reconstruite from scratch.

La migration nécessitera uniquement la redirection des flux utilisateurs vers la nouvelle infrastructure hébergée en interne.

< **Fin du document** >