Architecture AWS d’une application d’appels à projets

SR2I209- Sécurité des données dans le Cloud

EL HAJJAJI Riad

SOMMAIRE:

1/ Sujet et Besoins

2/ Evaluation des besoins d’architecture AWS de l’application

3/ Evaluation des besoin sécurité de l’application

Sujet et Besoins

La région “Far west” a mis en place un nouveau portail d’appel à projets innovants. Ce portail permet aux acteurs locaux de proposer des initiatives citoyennes innovant

L’architecture a été déployée dans un centre de données local à la région, et s’appuie sur une architecture en trois-tiers.
1/ Un portail de soumission de projet, offrant :
- Un accès public où l’on peut visualiser les annonces d’appel à projets.
- Un accès privé pour chaque acteur local, pour qu’il puisse soumettre ses propositions.
2/ Une couche métier, offrant :
- Une application qui implémente un template de soumission, où un acteur local authentifié pourrait soumettre une nouvelle initiative citoyenne, et partager des documents de soumission.
3/ Une couche de stockage, offrant :
- Une base de données pour stocker les données d’utilisateurs, et les détails de soumission.
- Un système de stockage partagé pour les dossiers de soumission.

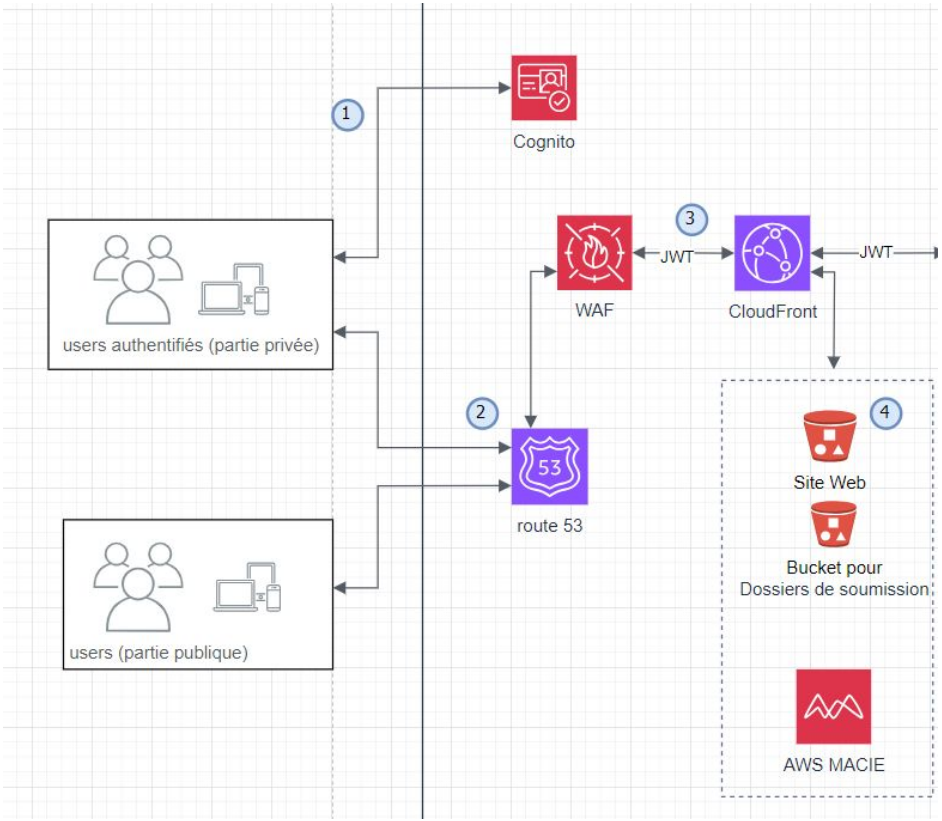
Problèmes:

➔ Attaques DDOS, le système s’est écroulé

➔ Migrer sur le cloud AWS pour bénéficier de plus de scalabilité, de disponibilité et de sécurité

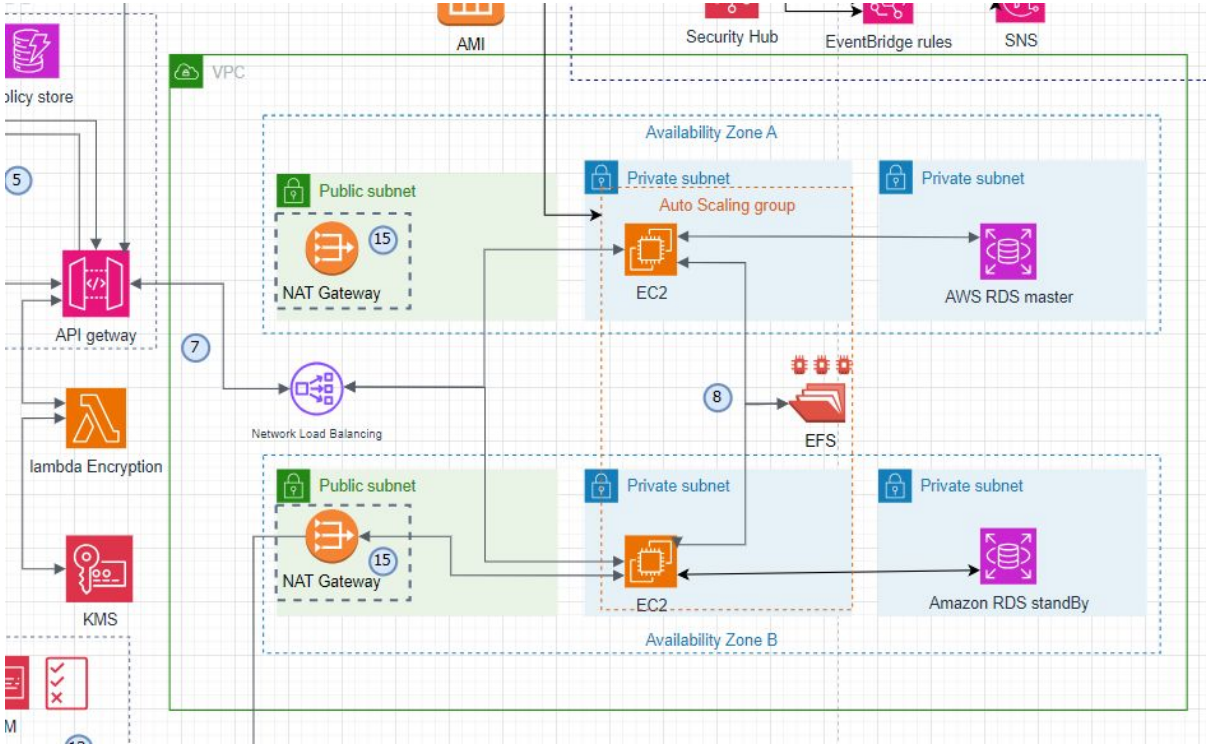
Evaluation des besoins d’architecture d’AWS

Evaluation des besoins AWS - **Front end**



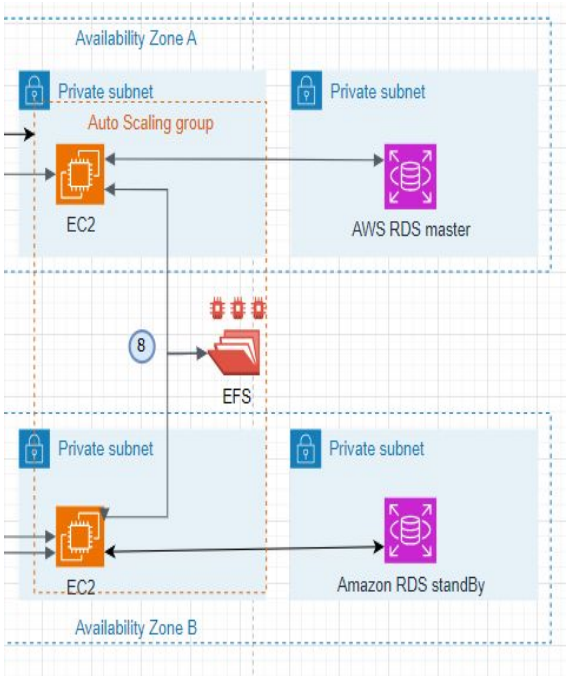
- CloudFront
  - Distribue le contenu
- S3
  - Les données statiques de l'application sont stockées dans un bucket S3

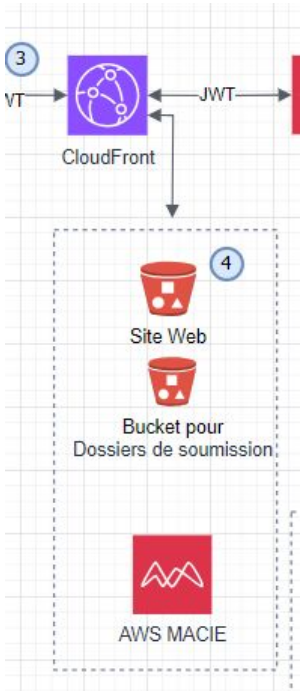
Evaluation des besoins AWS - **backend**



- EC2
  - Exécute la logique métier
- EFS
  - Stockage des artefacts de l'application backend
- Fonctions AWS Lambda
  - Tâches ponctuelles et opérations asynchrones
- API gateway
  - Exposition des fonctionnalités backend à l'extérieur
- ELB (Network Load Balancing)
  - Équilibre la charge sur les machines EC2

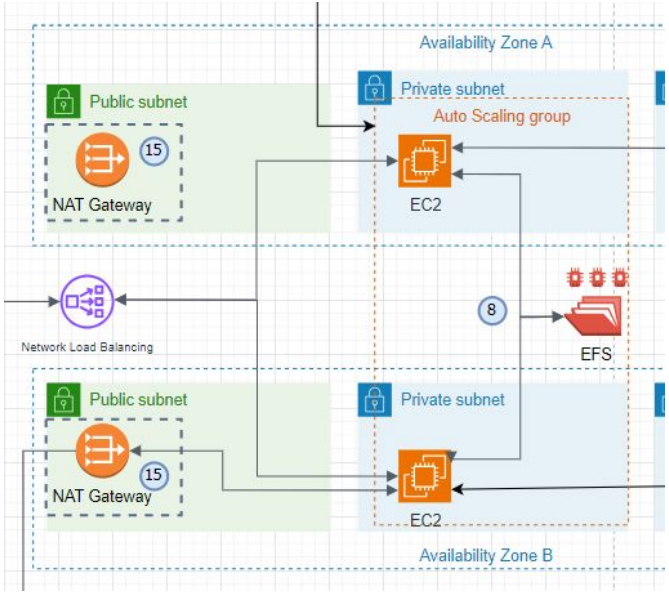
Evaluation des besoins AWS - **couche stockage**



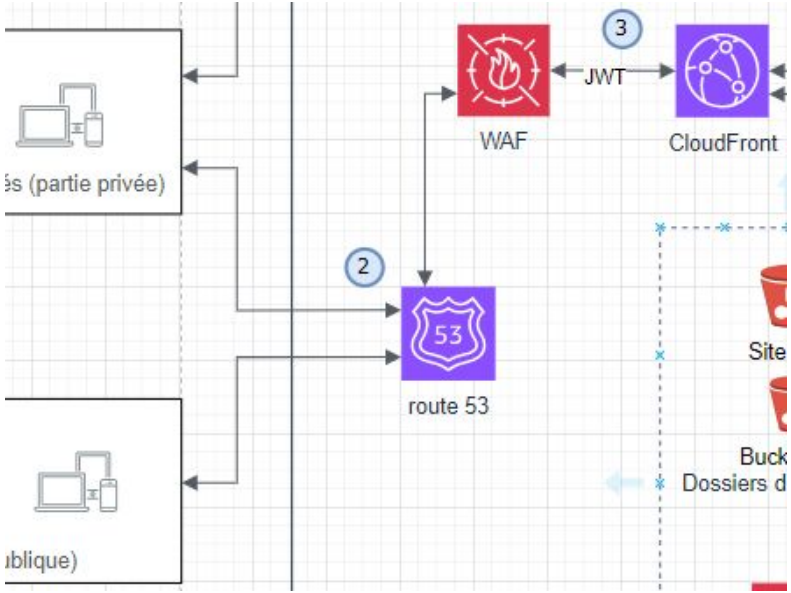


- **AWS RDS:**
  - Pour les données utilisateurs et les détails de soumission
- **S3** :
  - Pour les fichiers et autres détails des dossiers de soumission
  - Pour heberger le site static du front end
- **EFS:**
  - Stocker des artefacts de l'application

Evaluation des besoins AWS - **disponibilité / scalabilité**



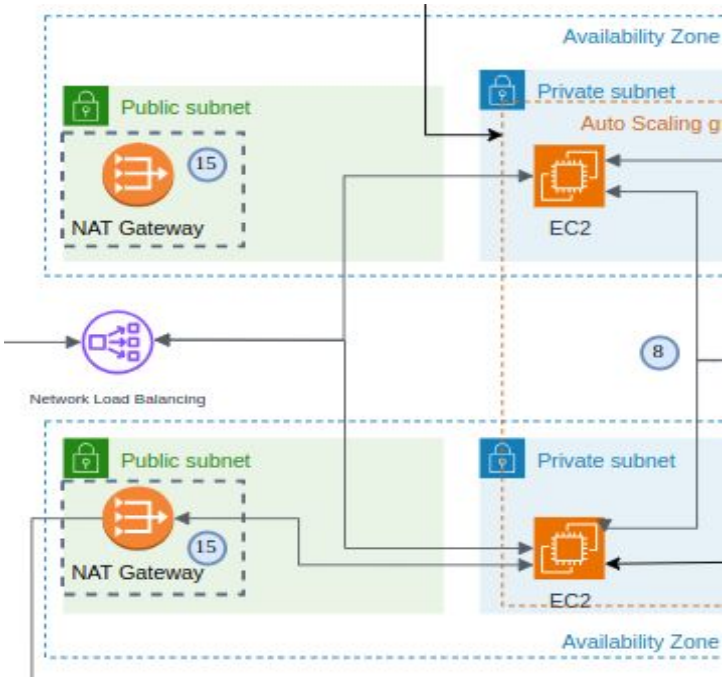
- 2 AZ : Redondance géographique
- NLB : Répartit le trafic entre les EC2
- Auto scaling group : Ajuste le nombre d'instances EC2 en fonction de la charge



- Route 53 : FailoverDNS
- S3 : Redondance
- CloudFront : Cache CDN

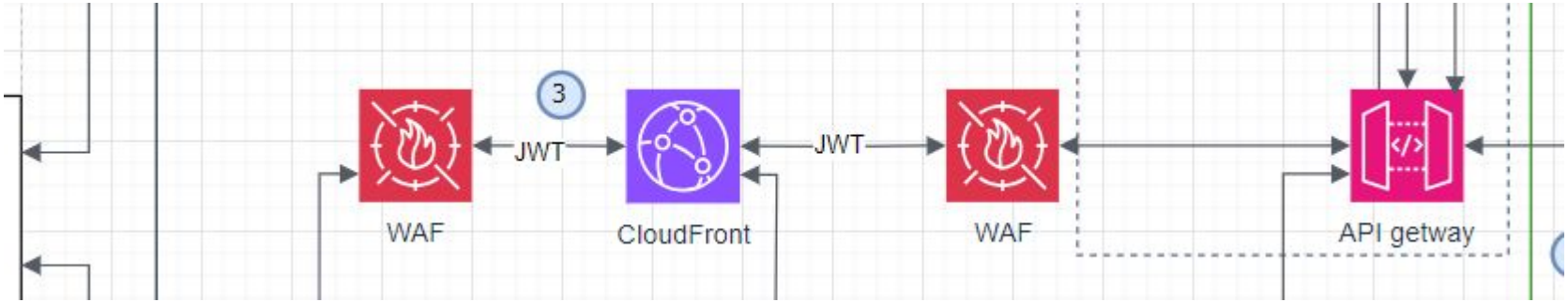
Evaluation des besoins spécifiques de sécurité

Besoins sécurité - **Sécurité des sous-réseaux et EC2**



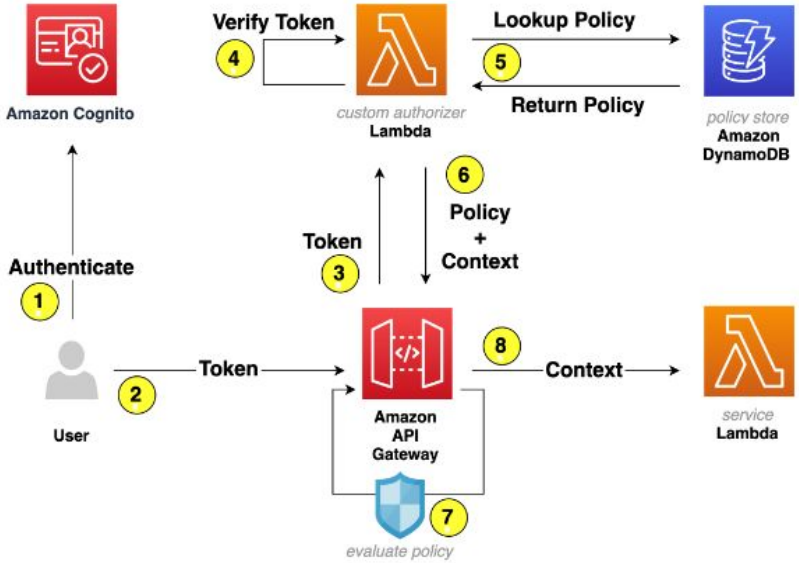
- Sécurité au niveau machine Ec2:
  - Les groupes de sécurité (security groups) : afin de réduire au minimum les surfaces d'attaque de l'application.
  - Protéger les paires de clés de SSH (key pairs)
  - Utiliser des images AMI sécurisées.
- Sécurité de ELB :
  - Pour autoriser le trafic provenant de certaines adresses IP uniquement, telles que celles de CloudFront
- NAT GATEWAY
  - Faire les patchs et en même temps bloquer les connexions initié de l'extérieur.
- AWS WAFs:
  - Éviter les attaques par injection SQL, les attaques XSS (Cross-Site Scripting) ou les tentatives d'accès non autorisées.

Besoins sécurité - **Firewalls**

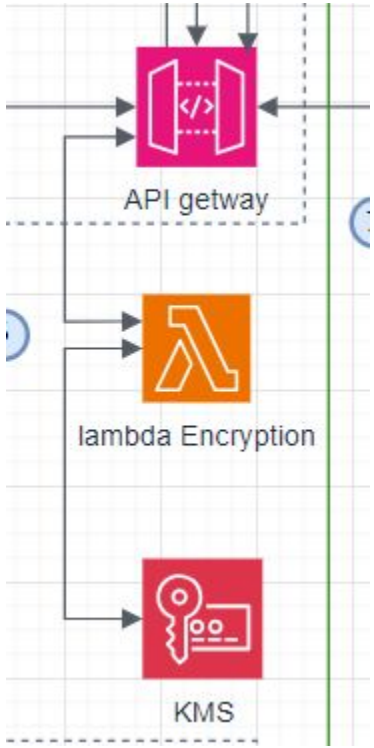


- Un WAF avant CloudFront
- Un WAF avant l'API gateway

Besoins sécurité - **Authentification et Confidentialité**



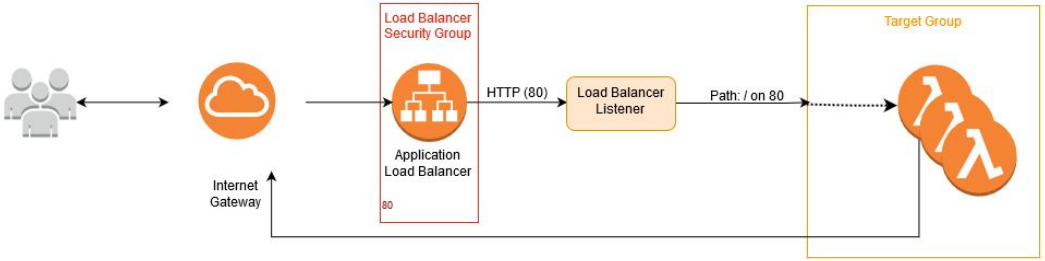
Authentication avec Cognito

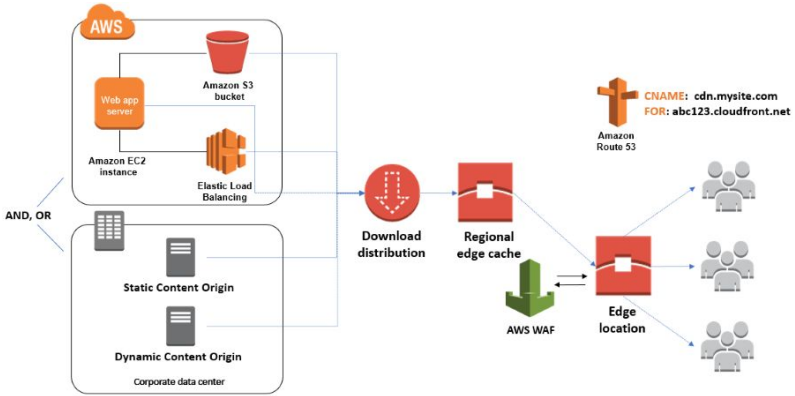


At rest data encryption with KMS

AWS Macie

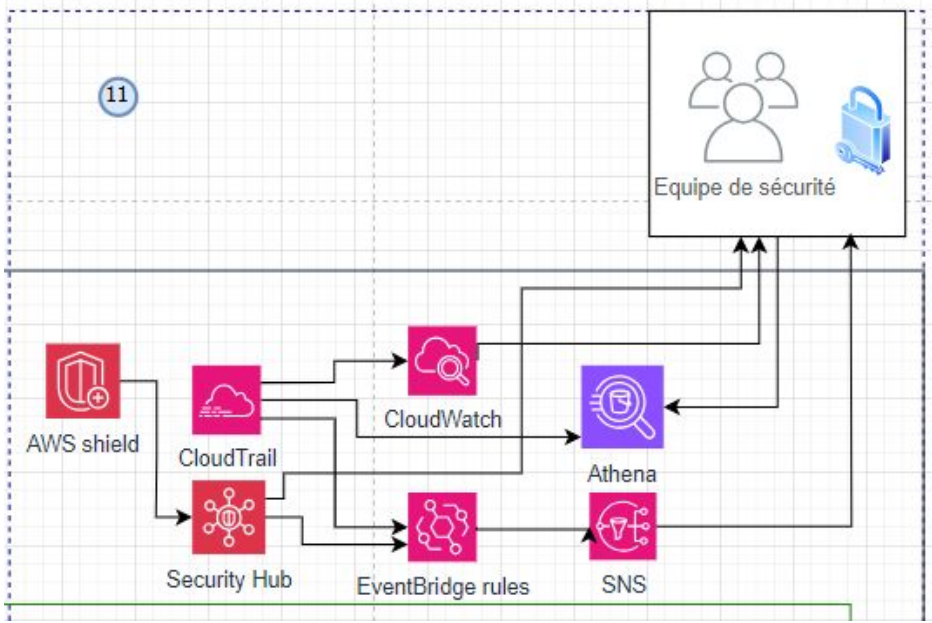
Besoins sécurité - **Protection contre DDOS**



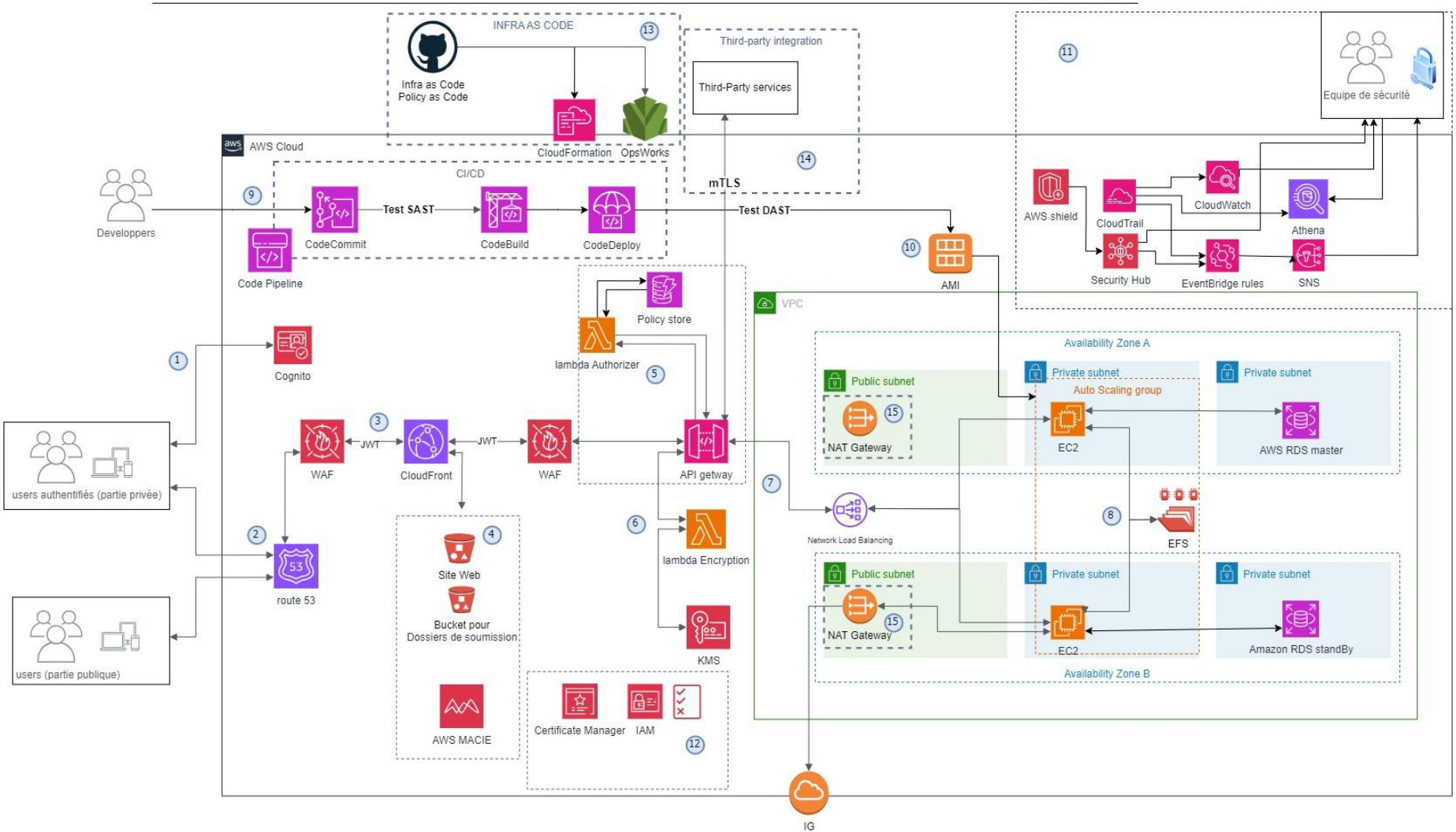


- AWS Shield :
  - Detection et reponse
- CloudFront & edge location
- Route 53:
  - Smart Dns resolution
- Mécanisme de scalabilité en cas d'attaque :
  - Auto Scaling group
  - Load Balancer
  - L'élasticité par défaut de S3 de l'api gateway

Besoins sécurité - **Surveillance / détection des incidents**



- CloudWatch
- EventBridge
- Amazon Macie
- CloudTrail
- SNS
- AWS Security Hub
- Athena


INFRA AS CODE
13
Infra as Code
Policy as Code
CloudFormation
OpsWorks
Third-party integration
Third-Party services
14
mTLS
11
Equipe de sécurité
AWS Cloud
CI/CD
9
Developpers
Code Pipeline
CodeCommit
Test SAST
CodeBuild
CodeDeploy
Test DAST
10
AMI
AWS shield
CloudTrail
CloudWatch
Athena
Security Hub
EventBridge rules
SNS
Policy store
lambda Authorizer
5
VPC
Availability Zone A
Public subnet
Private subnet
Auto Scaling group
Private subnet
1
Cognito
15
NAT Gateway
EC2
AWS RDS master
users authentifiés (partie privée)
3
JWT
WAF
JWT
CloudFront
JWT
WAF
API getway
7
Network Load Balancing
8
EFS
2
route 53
4
Site Web
Bucket pour
Dossiers de soumission
6
lambda Encryption
KMS
users (partie publique)
Public subnet
Private subnet
Private subnet
15
NAT Gateway
EC2
Amazon RDS standBy
Availability Zone B
AWS MACIE
Certificate Manager
IAM
12
IG