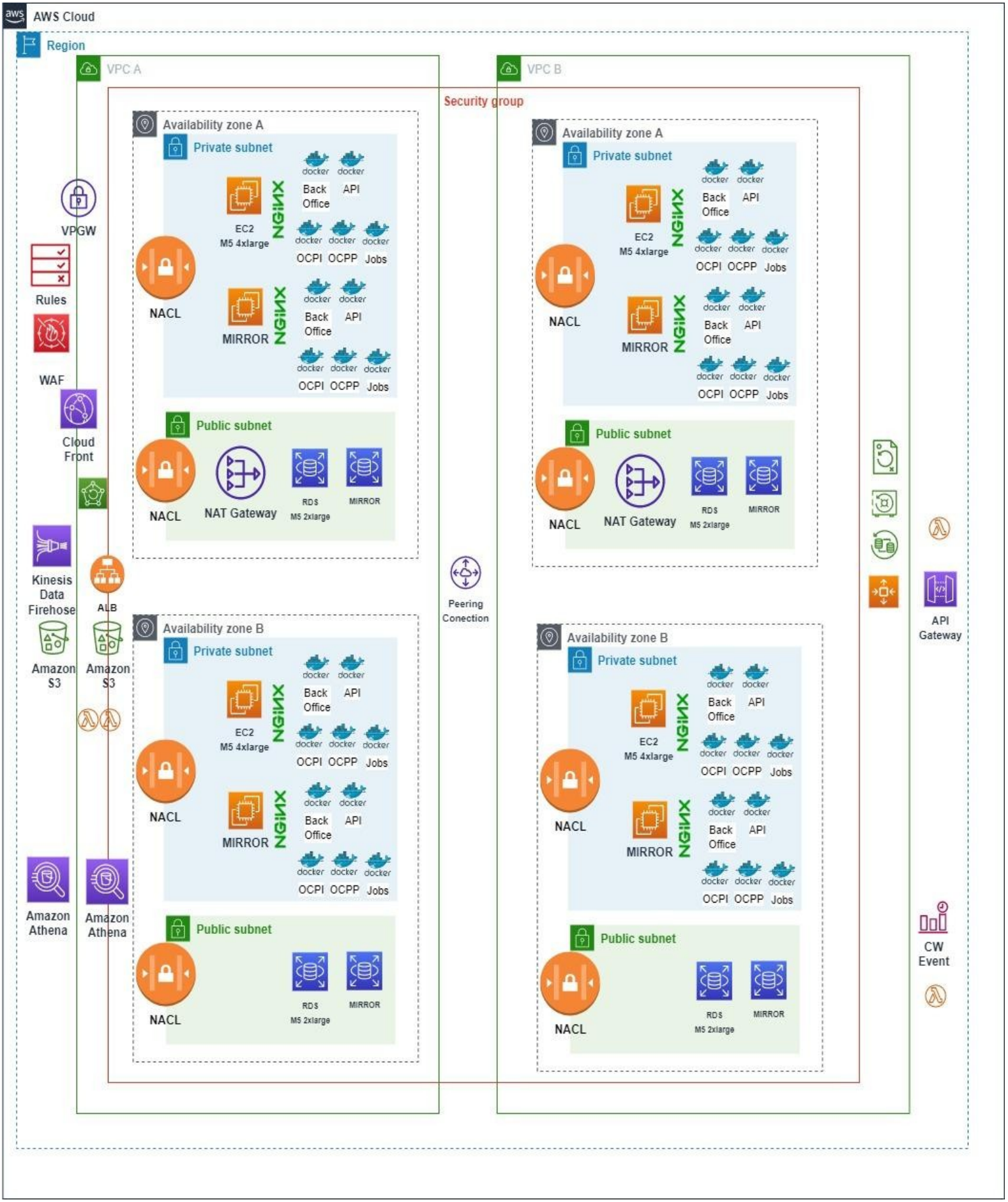
Arquitectura de servicios AWS.



Arquitectura de servicios AWS.

Networking.

Redes.

CloudFront (CDN).

- Hacemos uso del CDN propio para las peticiones públicas entrantes hacia la APP bajo el protocolo HTTP, como consultas de los recursos de la aplicaciones WEB, mitigando tiempos de latencia en respuestas de request.

Internet Gateway (IGW).

- La última milla o borde que utilizamos como acceso de entrada y salida hacia Internet de manera pública, evaluando la tabla de enrutamiento externo.

Virtual Private Cloud (VPC).

- Nuestra red privada de servicios en la nube, que contiene un CIDR Block de direcciones IPv4 reservadas, incluyendo las cinco consumidas por el proveedor de la nube.

Subnets.

- Las Instancias EC2 se administran bajo subredes públicas, obteniendo acceso en salida hacia Internet y peticiones externas entrantes para nuestras aplicaciones WEB.
- Las instancias RDS se administran por buenas prácticas bajo subredes privadas sin salida directa hacia Internet, mediante la consulta a través de las EC2.

Contenedores.

Elastic Cloud Compute (EC2).

- Hacemos uso de IaaS sobre distros GNU Linux como Ubuntu para la gestión de servicios.
- Utilizamos NGINX como nuestro proxy inverso para caché y balanceo de peticiones WEB hacia los recursos internos (dockers), mejorando el performance de nuestros servidores en procesamiento y memoria.
- Nuestros microservicios (Back Office, API, OCPP, OCPI, Jobs (tareas programadas)) están segmentados mediante docker para no impactar la disponibilidad de los diferentes servicios.

Bases de datos.

Relational Data Bases (RDS).

- Contamos con el PaaS para nuestras bases de datos relacionales con motor MySQL.

Arquitectura de servicios AWS.

Dominios.

Route 53.

- Contamos con las zonas directas e inversas de registros y peticiones externas e internas de dominios de nombres de servicios (DNS) a través de reenviadores públicos.

Simple Email Service (SES).

- Hacemos uso de respuestas ante emails con el servicio público de envíos y control de SPAM, listas negras y suprimidas, enviando las notificaciones y registros a un PUB/SUB del servicio SNS.

Serverless.

Lambda.

- Enviamos funciones para notificaciones de servicios ante CloudWatch y WAF..

Storage.

S3 (Buckets).

- Gestionamos un servicio de File Storage como repositorio de nuestro SFTP.

Arquitectura de servicios AWS.

Alta disponibilidad.

Failover & Failback.

Availability zones (AZ).

- Usamos la agilidad de la tolerancia a fallos entre dos zonas de disponibilidad dentro de la misma Región como punto de presencia (PoP).

NAT Gateway.

- Para acceder a la redundancia requerimos de un NAT como puerta de entrada que comunique las subredes privadas para salida hacia Internet.

Mirrors.

AMI.

- Los servicios principales de cómputo procesado como las instancias EC2 y RDS cuentan un espejo por AZ en stand by que replica cada nueva actualización de servicios dentro de un spot de instancias reservadas.

Balanceadores de carga.

Application Load Balancer (ALB).

- Al recibir tráfico entrante sobre cualquier petición HTTP sobre aplicaciones en la Capa 7 del modelo de intercomunicaciones, se redirecciona el mismo en proporción hacia cada target group sobre la redundancia de servicios bajo el método Round Robbin.

Network Load Balancer (NLB).

- Contamos con unas direcciones ip elásticas reservadas para la redundancia de conexión a la redes internas en Capa 3 y el transporte de las peticiones bajo la Capa 4 del modelo de intercomunicaciones.

RDS Proxy.

- Las instancias RDS hacen uso de un canal de backup como proxy inverso dentro de subredes privadas para la comunicación en la alta de cada servicio sobre las bases de datos.

Escalabilidad.

Autoscaling.

- Contamos con grupos de plantillas para realizar el escalamiento horizontal programado de los servicios para un alto tráfico entrante.
- Para el alto procesamiento el escalamiento vertical.
- Llevando una elasticidad de servicio según la demanda de recursos activos.

Arquitectura de servicios AWS.

Seguridad en Cloud.

Políticas WEB.

WAF.

- Controlamos el acceso o peticiones de entrada sobre la región (PoP), por medio del Cortafuegos de aplicaciones, evaluando las listas de control de acceso WEB (WACL) sobre la Capa 7 del modelo de intercomunicaciones.

WAF Rules.

- Mediante el servicio de Kinesis capturamos los registros del WAF, enviandolos particionados a un bucket S3, como información del tráfico de las WACL. Los cuales enviamos a unas lambda que utilizamos para los LOGs de los registros parseados al WAF, en conjunto del servicio Amazon Athena.

Alertas.

CloudWatch.

- Enviamos una lista de IP a través de una función lambda y un evento desde el CloudWatch hacia las reglas del WAF.

API Gateway.

- Mediante la API, enviamos por lambda los accesos manuales hacia las reglas del WAF.

Accesos.

Virtual Private Gateway (VPN).

- Accedemos por medio de la puerta de enlace para cada petición por un túnel cifrado privado desde el Internet público.

Peering Connection.

- Para acceder a la redundancia requerimos de una conexión en paridad hacia nuestras redes virtuales privadas con acceso a las subredes públicas.

Instancias.

Network Acces List (NACL).

- Evaluamos según la tabla de enrutamiento interno, filtrando reglas de entrada y salida stateless.

Security Groups.

- Administramos el tráfico entrante por medio del grupo de seguridad interno como Firewall para reglas statefull hacia puertos publicados, permitidos y denegados según el CIDR o reglas de ruteo de direcciones IPs externas.

Arquitectura de servicios AWS.

Plan de recuperación ante desastres (DRP).

Snapshots.

AWS Backup.

- Hacemos uso del servicio de copias de respaldo de la nube basado en las políticas de retención programadas,
- Diaria: De lunes a domingo iniciando a las 03:00 h en horario de España se realiza un backup diario el cual tiene un periodo de retención de 30 días.
- Mensual: Programadas para el primer día de cada mes, con retención de un año.
- Semestrales: Programadas para el primer día de enero y julio del presente año, con retención de cinco años.
- Con ello centralizar las políticas y automatización de los datos de nuestras instancias EC2, RDS.

Backup Plan.

- Analizamos el plan de cada copia de seguridad programada para respaldos incrementales y full según las políticas de backup.

Backup Vault.

- Dependiendo del cambio por aplicar según el CUD de actualización de servicios: Se almacena o elimina el volumen con la fecha solicitada.

Backup Restore.

- Después de evidenciar el volumen de shadows copy, se realiza el rollback al punto de restauración relevante ante el DRP sobre las políticas de backup.