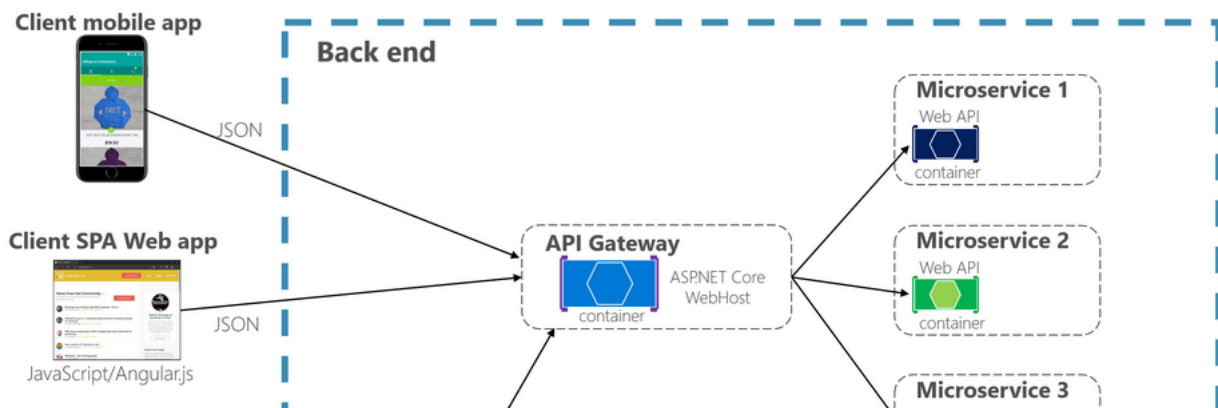


I - Annexe – Api Gateway

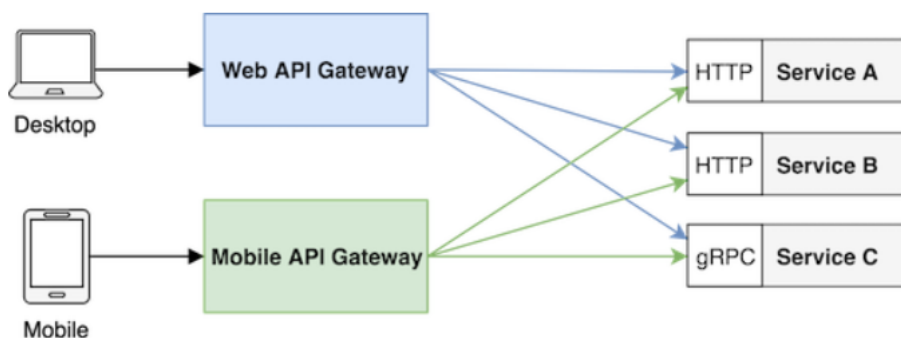
1. Gateway API

Le réseau interne (intranet) d'une entreprise est déjà en soi un domaine à bien sécuriser. Lorsque certains services sont exposés à l'extérieur du "S.I.", il faut prendre encore plus de précautions (attaques de toutes sortes : force brute , déni de service , ...)

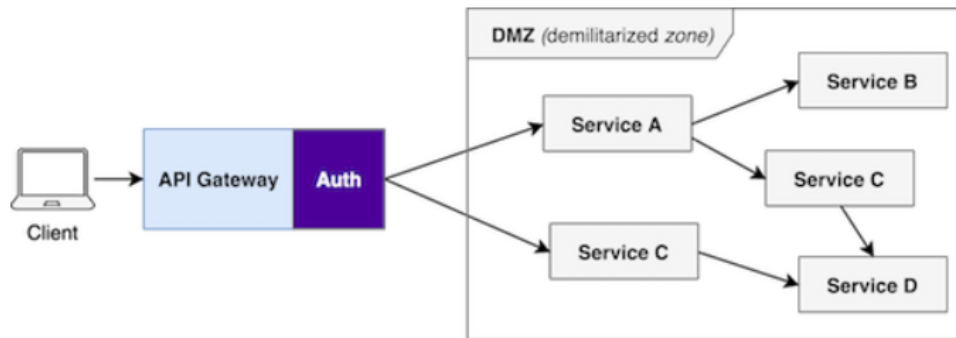
La solution la plus courante utilisée pour protéger l'accès aux services exposés à tout internet consiste à mettre en place des **serveurs d'intermédiation spécialisés appelés "Gateway"** .



On peut envisager des "gateway" spécifiques aux types de clients externes ("desktop" ou "mobiles") :



On peut éventuellement concentrer la sécurisation des web-services sur un "gateway" :



Si le principal rôle d'un "Gateway" est la sécurisation , beaucoup de solutions "gateway" apportent "dans la façade exposée" tous un tas de valeurs ajoutées intéressantes :

- Authentification et autorisation
- Intégration de la découverte de service
- Mise en cache des réponses
- Stratégies de nouvelle tentative, disjoncteur et qualité de service (QoS)
- Limitation du débit
- Équilibrage de charge
- Journalisation, suivi, corrélation
- Transformation des en-têtes, chaînes de requête et revendications
- Liste verte d'adresses IP

NB : Dans le cadre d'un cloud public , la plateforme d'hébergement "cloud" (ex : Microsoft Azure ou ...) peut directement en charge le "Gateway API" (avec plus ou moins de fonctionnalités associées) .

2. Monitoring d'API REST

Il est souvent intéressant de surveiller l'activité d'une API REST pour s'assurer du bon fonctionnement et améliorer le marketing associé .

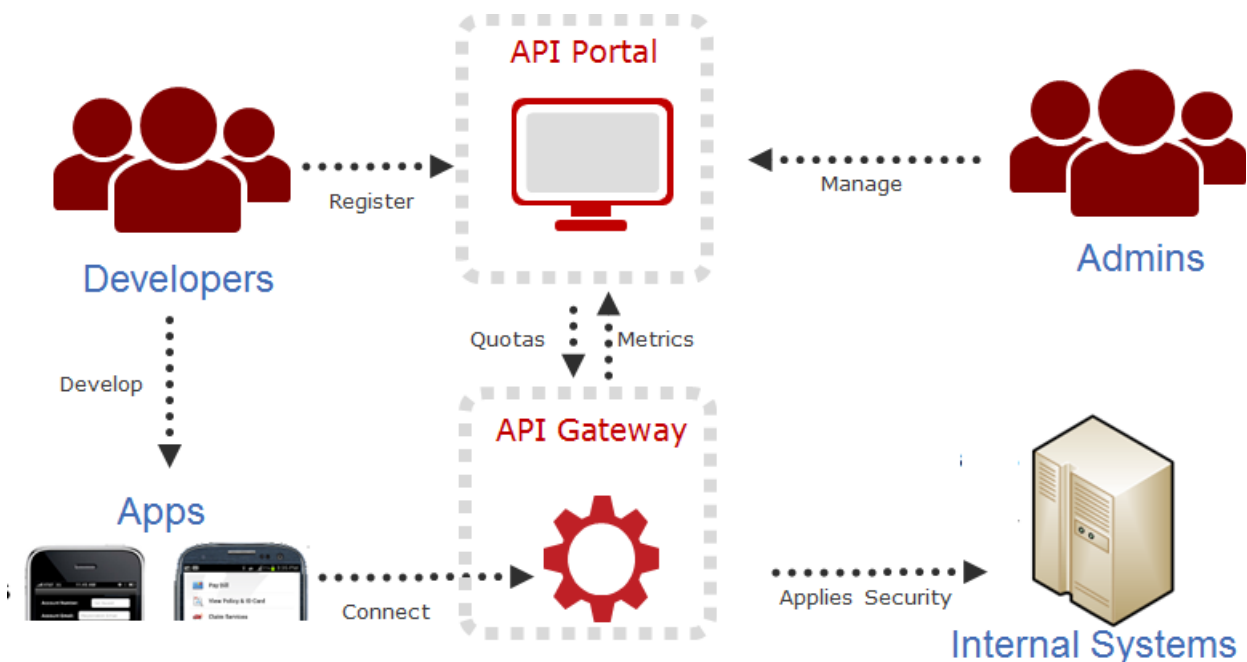
Il existe pour cela plein de solutions en "cloud privé" et "cloud public" .

L'aspect "monitoring" peut souvent être pris en charge par le serveur "gateway" en façade : cette sorte de "ESB exposé à l'extérieur du SI" doit idéalement servir à plein de choses pour éviter "3600 intermédiaires ajoutant une fonctionnalité à la fois" .

3. Portail développeur

Un **portail développeur** est un site web :

- exposé au réseau externe (vu par les développeurs des entreprises clientes)
- **documentant à fond la collection d' API exposée par le "API gateway"** (URL , exemples , descriptions SWAGGER , ...)



Un développeur (d'une entreprise "cliente") pourra ainsi :

- Déterminer quelles API sont disponibles
- Parcourir la documentation sur les API
- S'inscrire à leur propre clé d'API, qu'ils reçoivent immédiatement, nécessaire pour créer des applications
- ...

NB : Certaines "plateformes cloud" offre ce genre de service (ex : Amazon Web Services)