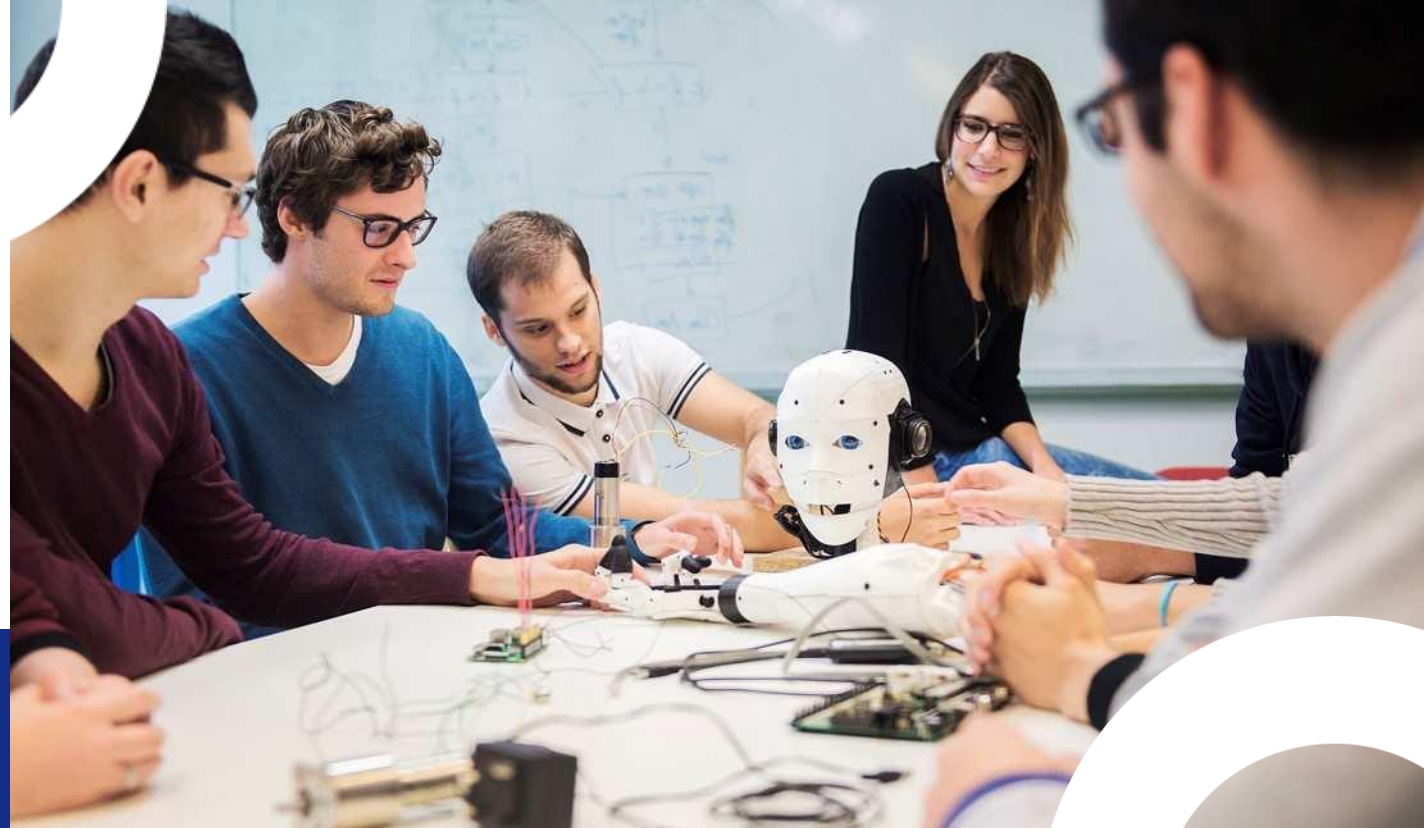




L'ÉCOLE DE L'INNOVATION
TECHNOLOGIQUE



Exercice Scientifique et technique

GUERIN Clément

Une école de





Contexte



Développement d'applications mobiles et web qui doivent accéder à des données internes.

→ Situées sur un **réseau intranet sécurisé**

→ **Non accessibles** depuis internet



Mise en place d'une architecture pour faire transiter les données entre : **Internet** — et — **Intranet**

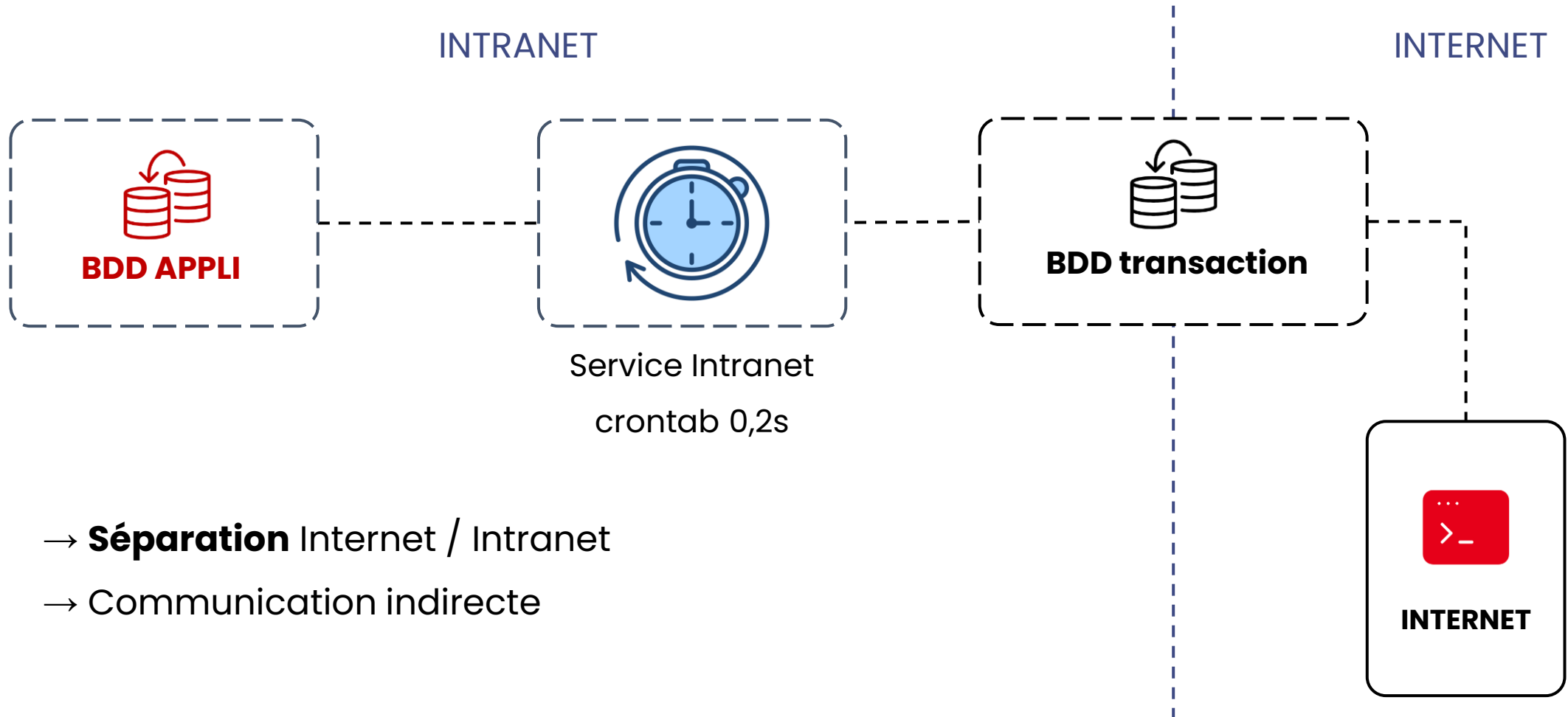
→ sans exposer directement ce réseau.

Problématique

« Comment accéder à des données d'un intranet sécurisé sans exposer directement ce réseau à Internet ? »

- Applications (mobile / web) sur Internet
- BDD internes protégées
- Sécurité et contrôle nécessaire

Architecture générale



- **Séparation** Internet / Intranet
- Communication indirecte

Transactions client – serveur

- Requêtes via **HTTP** (GET / POST)
- Données structurées en **JSON**
- Stockage des demandes dans une **table de transactions**
- Traitement par un service interne
- Queue de messages
- Traitement asynchrone

L'application envoie une **demande de données** structurée, sans accès direct à la base.

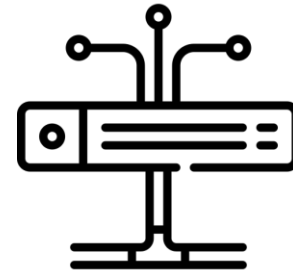
Sécurité de l'architecture

Le concept de **segmentation réseau** est clé ici.

→ Aucune connexion direct internet vers intranet.

→ Serveur interne agit comme une **passerelle**

→ **Traitement** uniquement côté **backend** interne



Comparaison avec API classique

API classique

- Client appelle directement le serveur interne
- Exposition des Endpoints
- Surface d'attaque plus grande

Architecture utilisée

- Aucune requête directe
- Actions **prédéfinies**
- Contrôle complet en backend

Principe du moindre privilège

Réduction de la surface d'attaque

Limites...

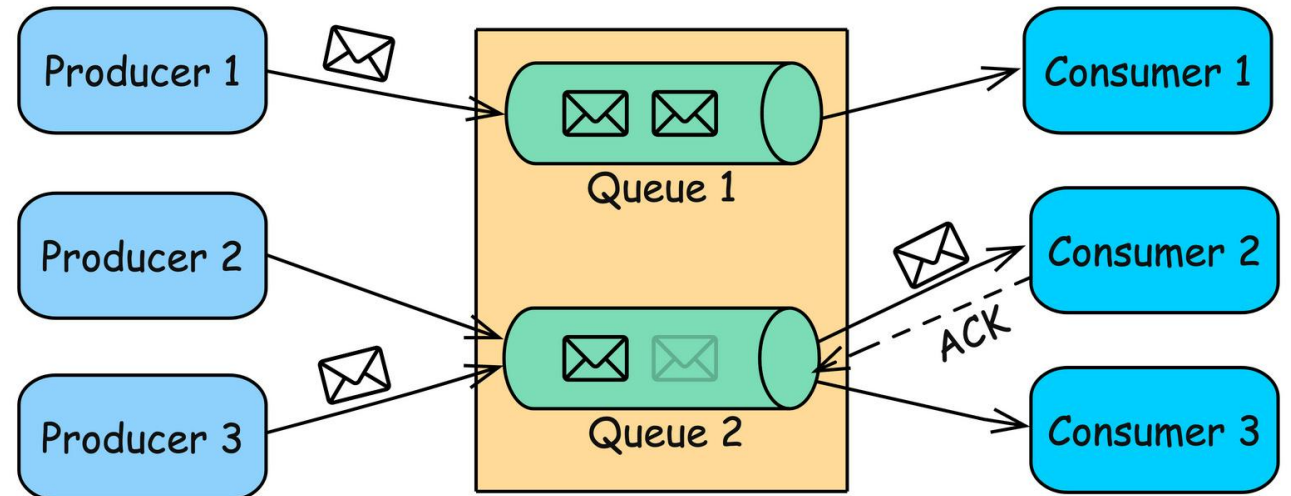
Ce mode de fonctionnement a aussi des limites...

→ **Latence** (environ 0,2s /requête)

→ Table peut être surchargée

→ Architecture plus complexe

→ **Queue de messages**



Conclusion

Cette architecture permet de faire communiquer des applications Internet avec un intranet sécurisé tout en évitant toute exposition directe des bases internes.

- **Isolation stricte** des réseaux
- File (table) de **transaction**
- **Traitement** backend **contrôlé**

Cette approche réduit fortement la surface d'attaque et garantit que seules des actions **prédéfinies et validées** peuvent être exécutées sur les données internes.