EXERCICE 4 — Conception d’une architecture Zero Trust

**Contexte professionnel**

Après avoir :

- cartographié les actifs (Exercice 1),
- identifié les menaces STRIDE (Exercice 2),
- dérivé les exigences de sécurité (Exercice 3),

vous devez maintenant concevoir une **architecture Zero Trust** pour ShopNow.

L’entreprise veut :

- réduire les risques d’usurpation,
- limiter les mouvements latéraux,
- renforcer l’authentification,
- protéger les données sensibles,
- isoler les composants critiques.

Le CTO exige une architecture **Zero Trust by Design**, documentée et justifiée.

**Objectifs pédagogiques (version Master)**

À l’issue de cet exercice, l’étudiant doit être capable de :

**1. Appliquer les principes Zero Trust à une architecture réelle**

Ne jamais faire confiance, toujours vérifier, appliquer le moindre privilège.

**2. Définir les contrôles Zero Trust adaptés aux menaces STRIDE**

Aligner les mesures avec les risques identifiés.

**3. Segmenter l’architecture en zones de confiance minimales**

Micro-segmentation, isolation des composants critiques.

**4. Mettre en place une authentification et autorisation continues**

MFA, RBAC, tokens courts, vérification dynamique.

**5. Définir des politiques de sécurité dynamiques**

Basées sur le contexte, le comportement, le risque.

**6. Concevoir une architecture défendable et observable**

Logs, SIEM, monitoring, détection d'anomalies.

Répondez à ces questions sous la forme d'un rapport en anglais (le rapport devra prendre en compte une page de garde, un sommaire, une numérotation de page et une conclusion et bien sûr la réponse aux questions. Aide-toi des annexes.

1. **Quels composants doivent être isolés pour limiter les mouvements latéraux ?**
2. **Quels flux doivent être authentifiés et autorisés systématiquement ?**
3. **Comment appliquer le principe du moindre privilège à chaque acteur ?**
4. **Quels contrôles dynamiques doivent être mis en place (MFA, device posture) ?**
5. **Comment garantir la visibilité et la traçabilité de toutes les actions ?**
6. **1. Comment intégrer Zero Trust dans un environnement existant sans perturber les opérations ?**
7. **Comment adapter Zero Trust à un environnement distribué (microservices, cloud, API externes) ?**

Annexe Actifs critiques concernés par Zero Trust

| Catégorie | Actifs |
|---|---|
| **Données sensibles** | D1, D2, D4, D6 |
| **Composants critiques** | C2, C3, C5 |
| **Flux sensibles** | F1, F2, F4 |
| **Acteurs à privilèges** | A2 Administrateurs |

**Principes Zero Trust appliqués à ShopNow**

**Principe 1 — Vérification systématique (Never Trust, Always Verify)**

- Authentification obligatoire pour chaque requête
- Tokens courts + rotation
- Vérification de l'intégrité des requêtes (HMAC)

**Principe 2 — Moindre privilège (Least Privilege)**

- RBAC strict
- Séparation des rôles admin / client
- Accès DB minimal

**Principe 3 — Micro-segmentation**

- Isolation du backend, DB, API Auth
- Interdiction des communications directes non nécessaires

**Principe 4 — Contrôles dynamiques**

- MFA obligatoire pour admin
- Détection d'anomalies
- Rate limiting adaptatif

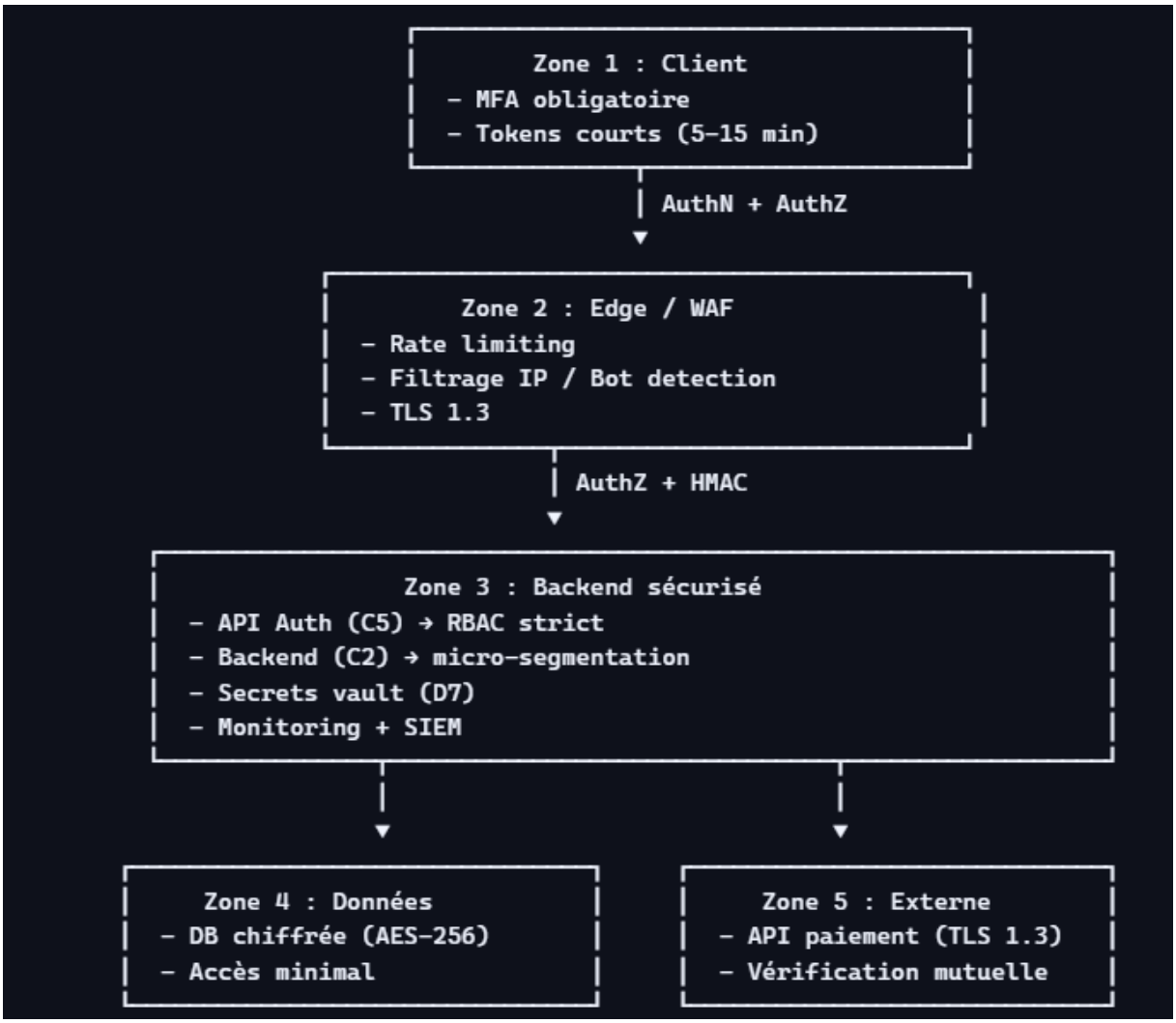
**Principe 5 — Visibilité et traçabilité**

- Logs signés, horodatés
- Monitoring temps réel
- Alertes sur comportements suspects

Tableau des mesures Zero Trust

| Menace STRIDE | Principe Zero Trust | Mesure | Priorité |
|---|---|---|---|
| **Spoofing** | Vérification systématique | MFA + tokens courts | Haute |
| **Tampering** | Intégrité | HMAC + signatures | Haute |
| **Information Disclosure** | Chiffrement | TLS 1.3 + DB chiffrée | Haute |
| **DoS** | Contrôles dynamiques | Rate limiting + WAF | Haute |
| **Elevation of Privilege** | Least Privilege | RBAC strict | Haute |
| **Repudiation** | Traçabilité | Logs immuables | Moyenne |

Architecture Zero Trust — Schéma ASCII




**Légende du schéma**

- **AuthN** : Authentification
- **AuthZ** : Autorisation
- **RBAC** : Role-Based Access Control
- **HMAC** : Signature des requêtes
- **SIEM** : Monitoring centralisé
- **Vault** : Stockage sécurisé des secrets