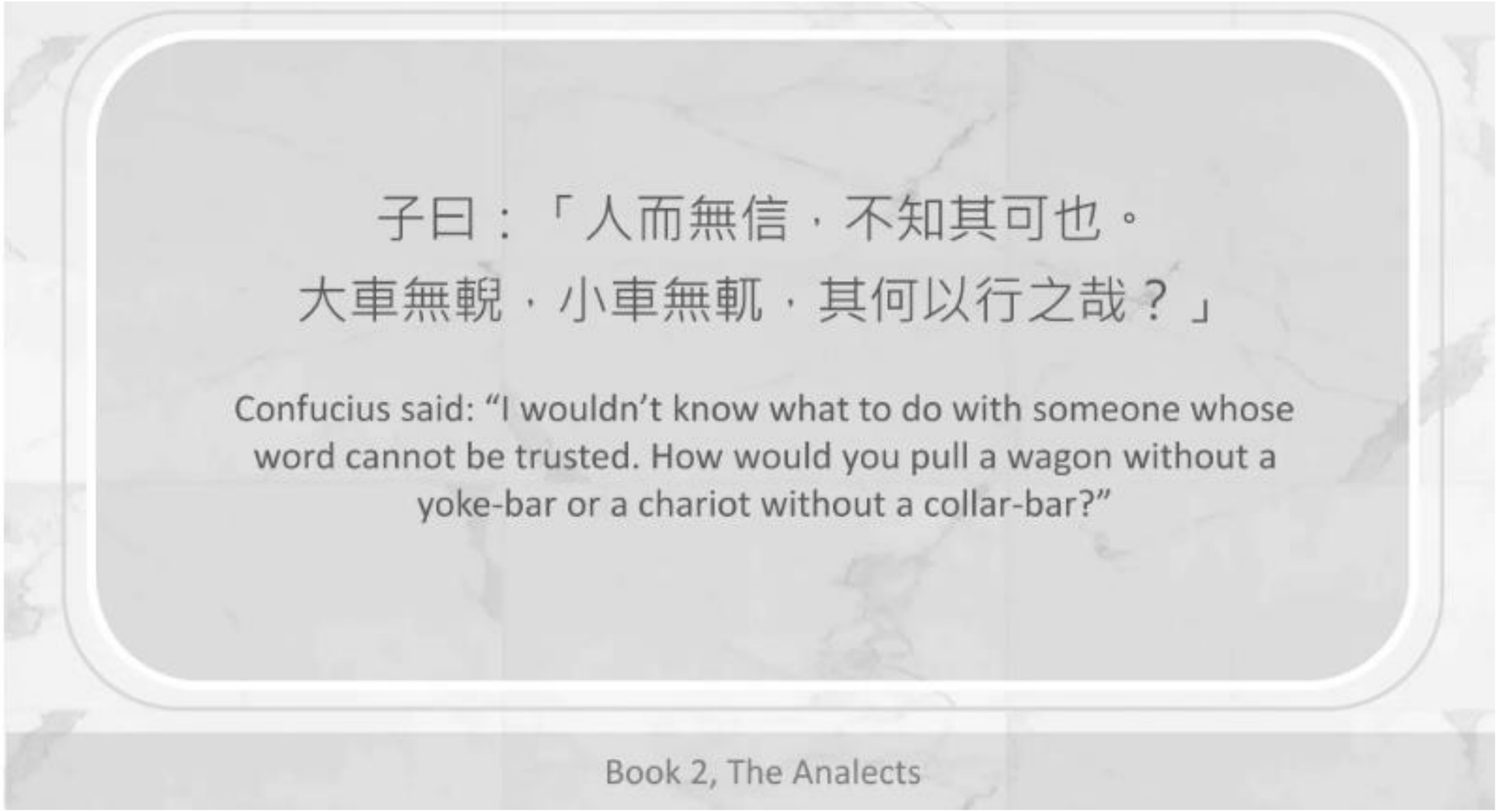
Яндекс

Zero Trust security model

Eldar Zaitov

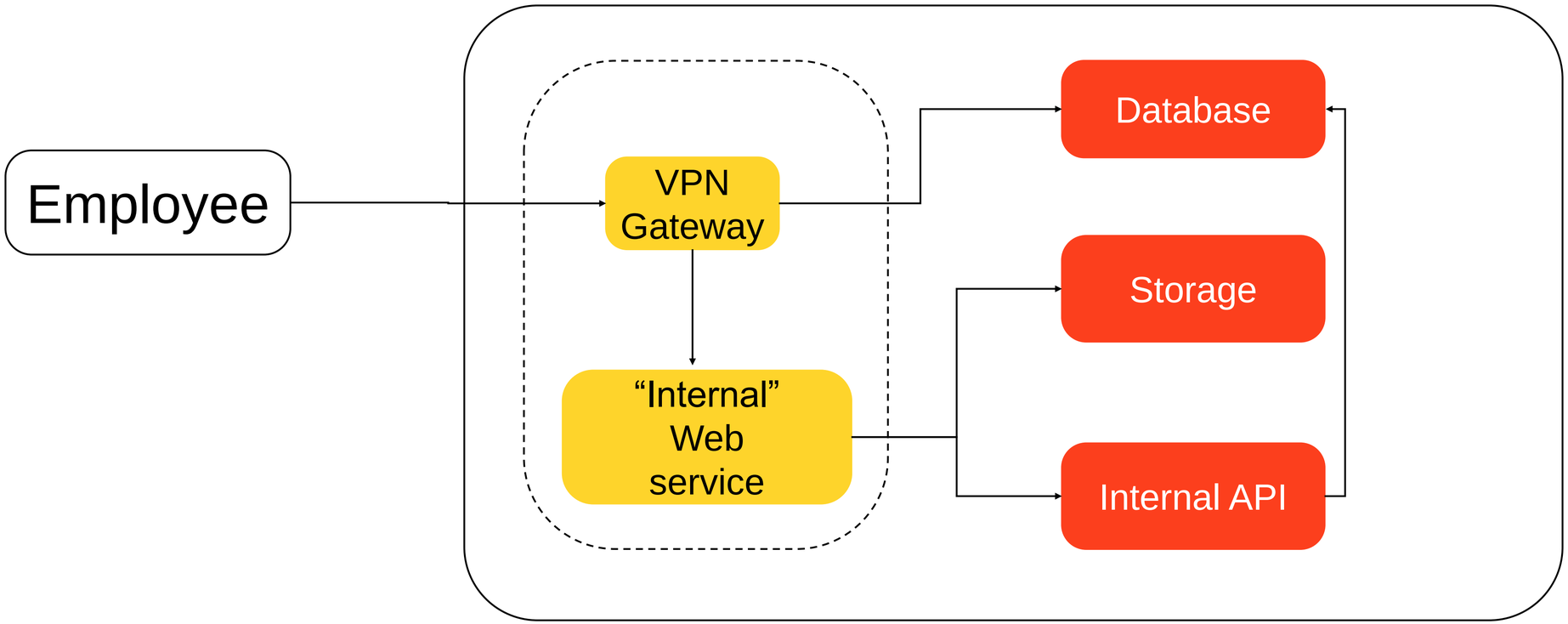
whoami

- Head of infrastructure and platform security at Yandex
- Used to play CTFs
- The maintainer of CTFtime.org

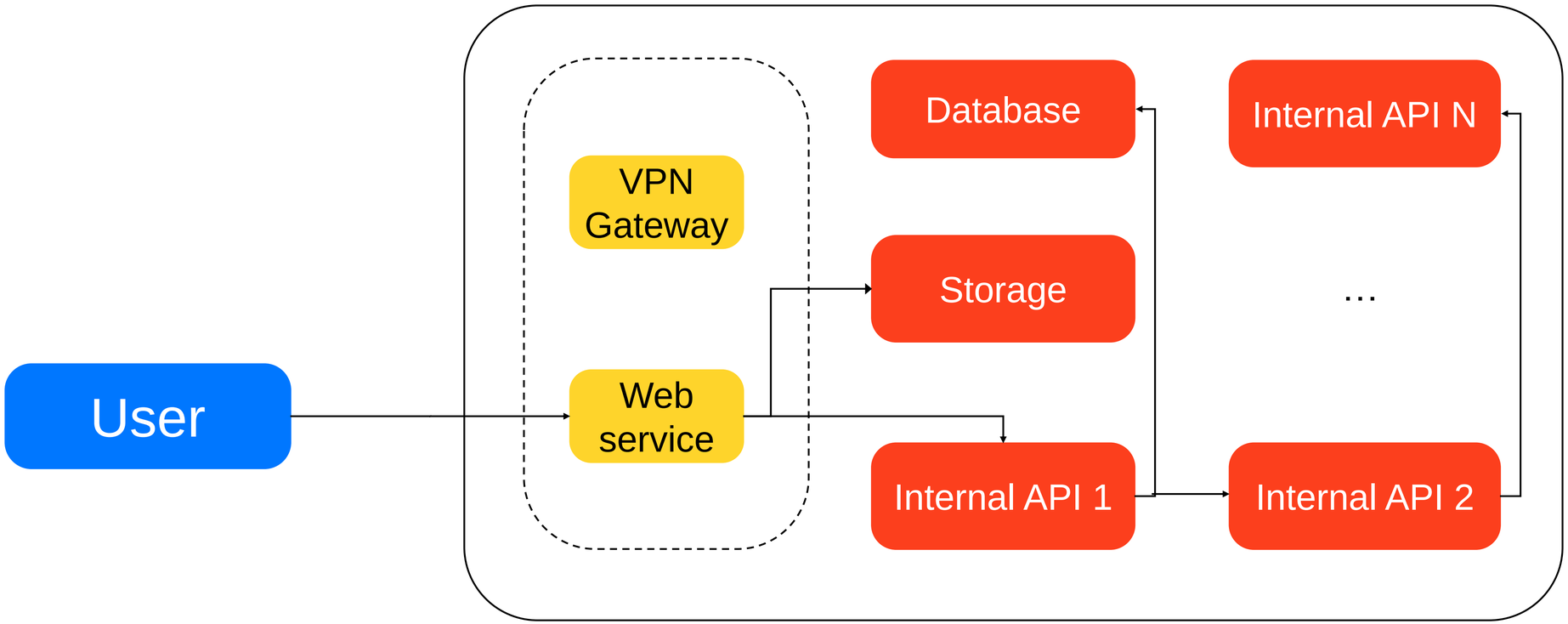


* New English translation of Book 2 of the Analects of Confucius

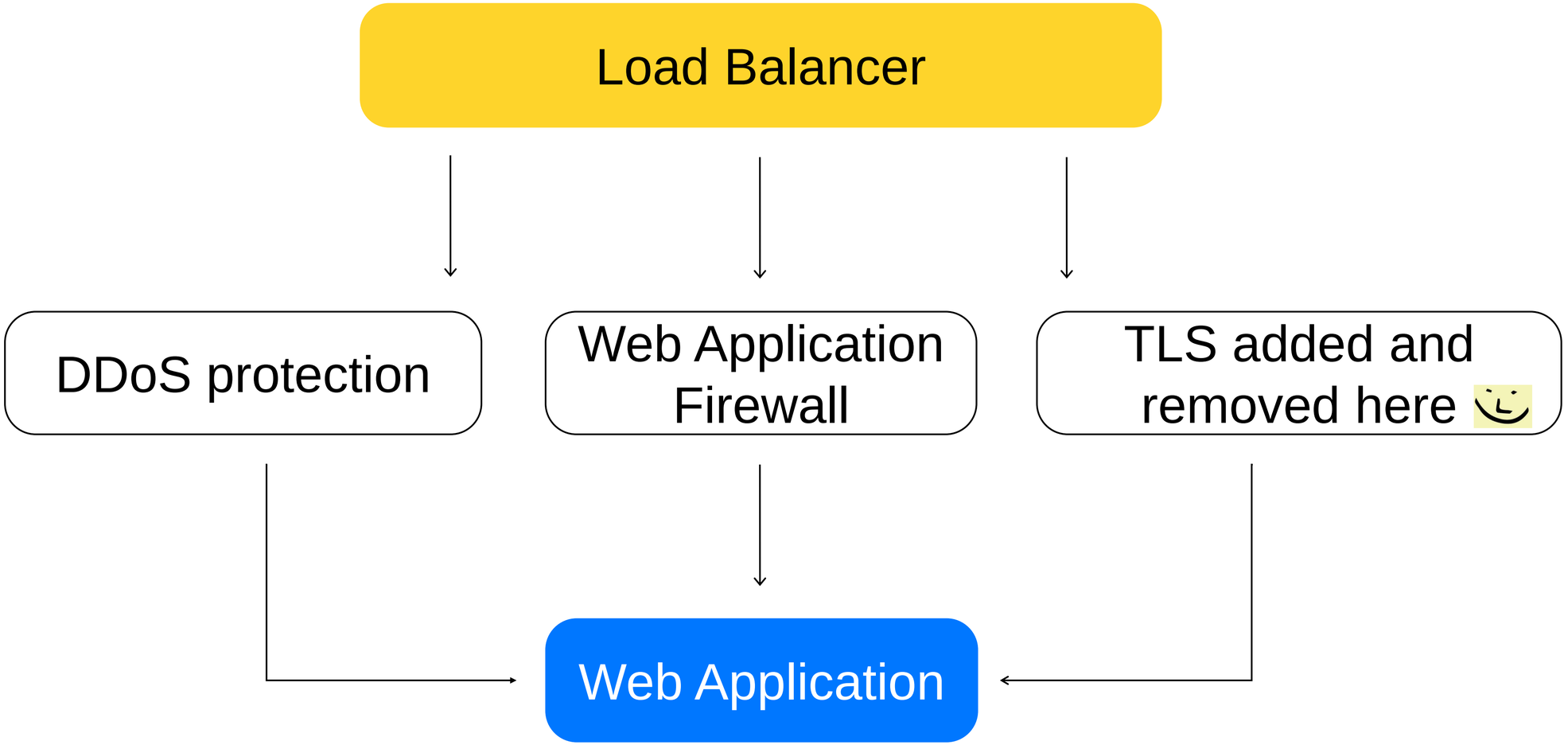
Old-school intranet



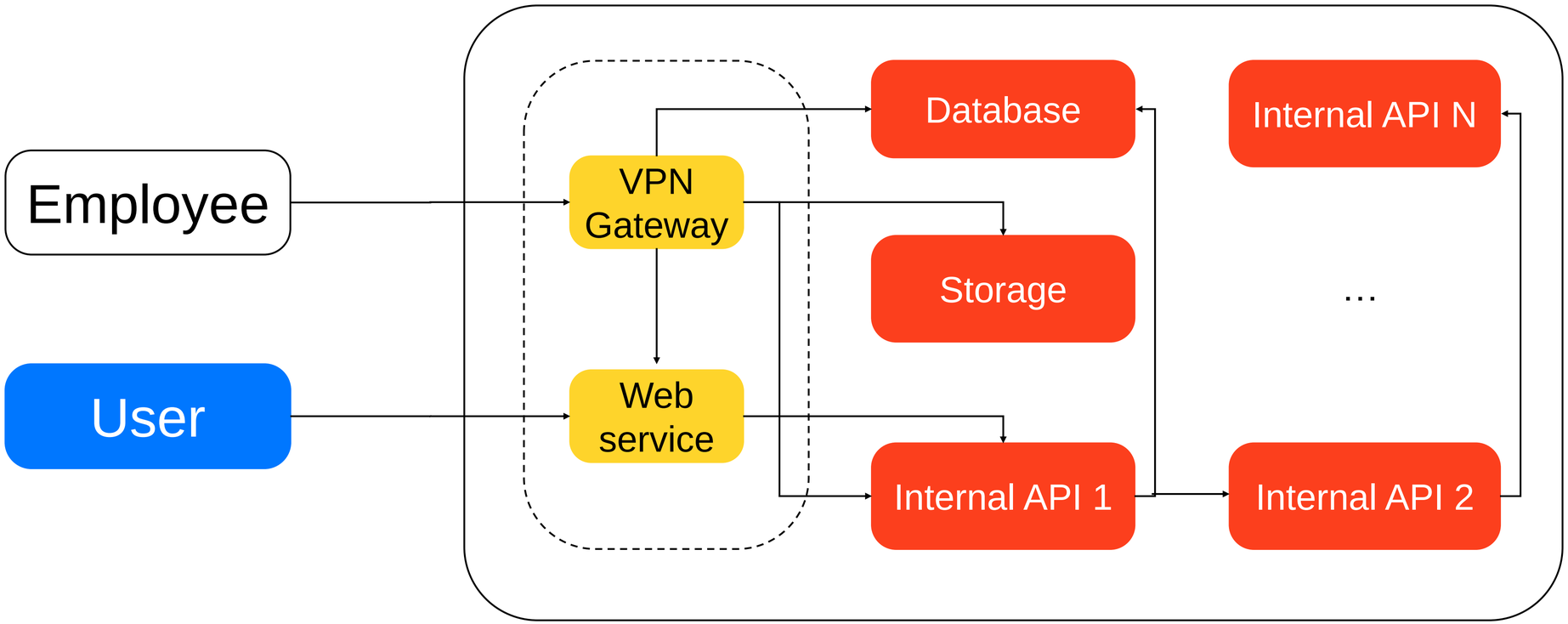
Old-school intranet



Web Service


Load Balancer
DDoS protection
Web Application Firewall
TLS added and removed here
Web Application

Old-school intranet



Main ideas of Zero Trust model

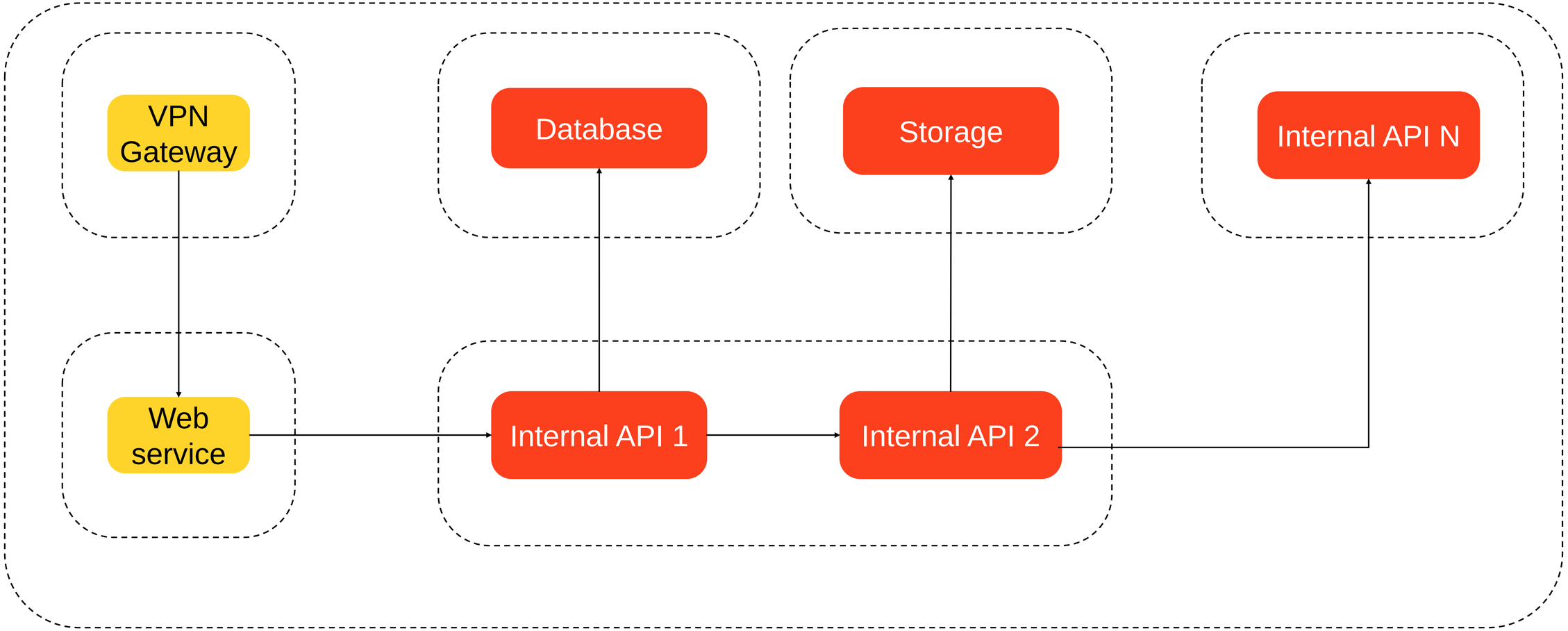
- Network is untrusted
- Authentication and authorization are mandatory
- Least privilege access
- Assume some devices and users are compromised

Zero Trust: network segmentation

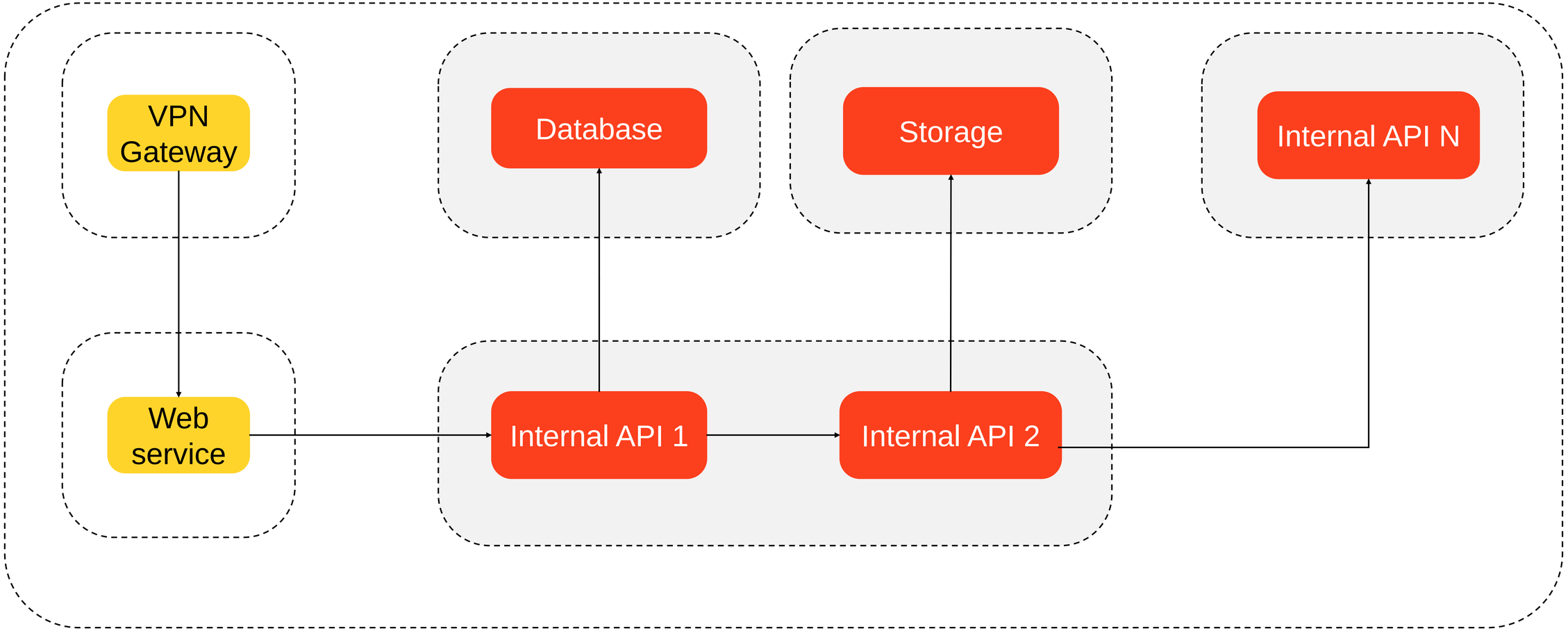
Zero Trust does not dismiss network segmentation

- Inventory
- L2/L3
- VPC/VNets
- Firewall / Security Groups

Zero Trust: network segmentation



Zero Trust: network segmentation



Zero Trust: authentication

Zero Trust demands strong identity of all parties

- Service identity
- Device identity
- User identity

Zero Trust: service identity

Service identity

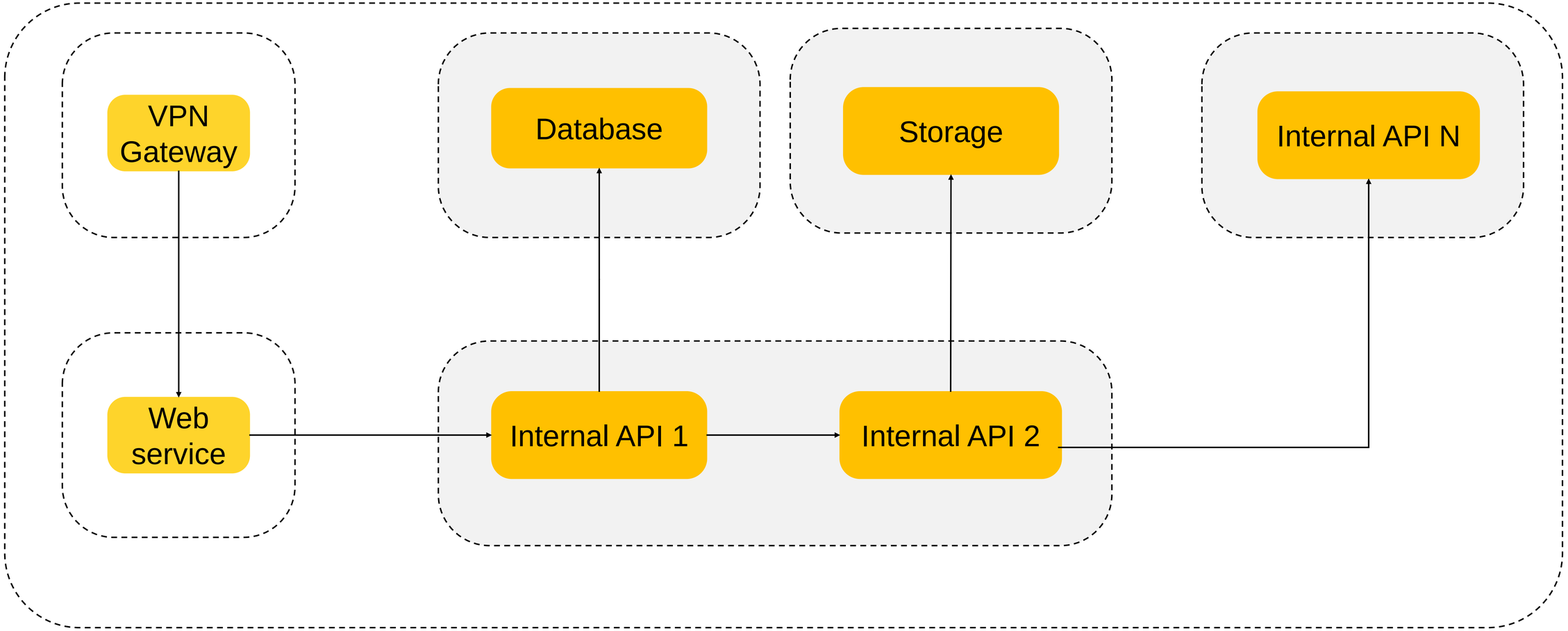
- Inventory
- PKI
- mTLS
- Secrets Management
- Data-plane identity propagation

Secrets Management

Secret management is vital for Zero Trust

- Credentials are identity based
- Short-lived credentials
- Rotatable secrets
- Detectable secrets

Zero Trust: authentication



Zero Trust: device identity and health

Device Lifecycle and asset management

- Hardware-bound secrets
- Managed devices

Hardware-bound device secrets

Device secrets should be stored in hardware storage

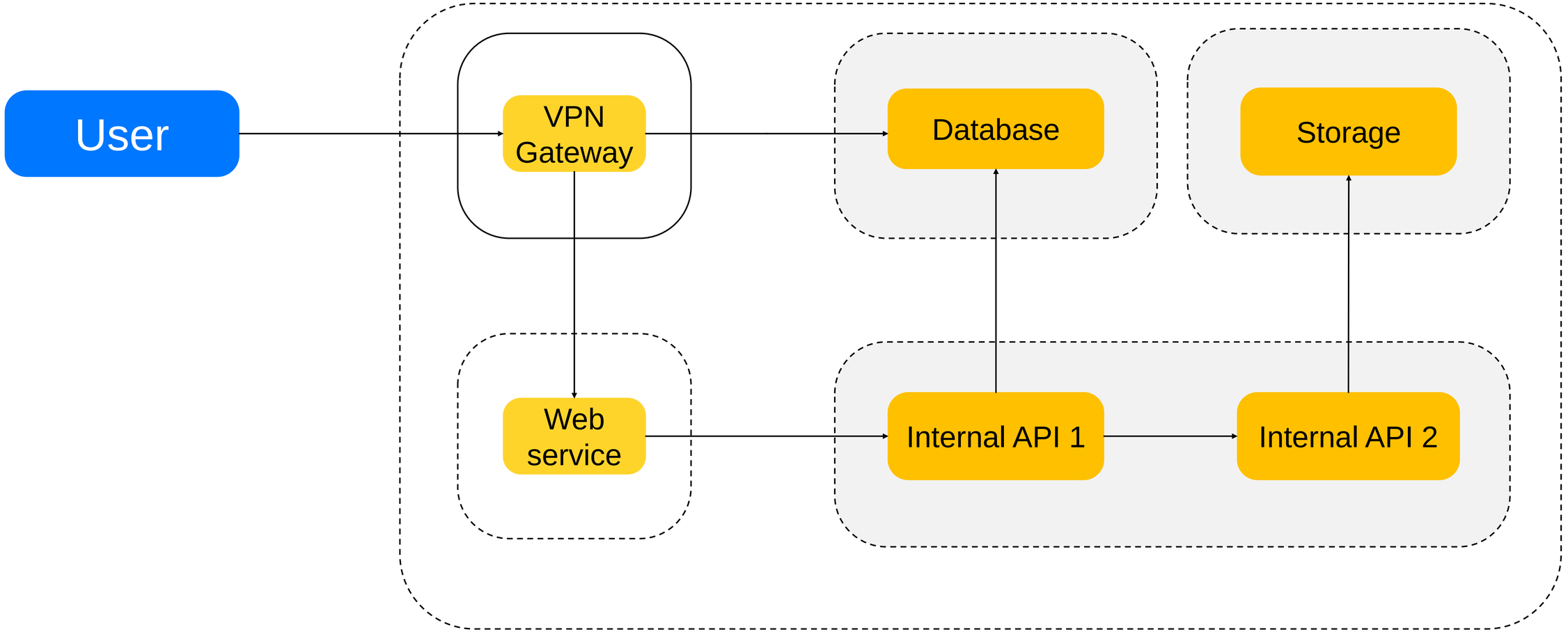
- TPM with attestation (Windows, Linux)
- Secure Enclave (iOS 14+)
- Keystore (Android 7+)

Device management and monitoring

Device management is MUST

- Compliance
- Patch management
- Endpoint protection
- Comprehensive logging from endpoints
- Remote wipe

Zero Trust: authentication



Zero Trust: user identity

User Lifecycle and source of trust

- Single Sign On (SSO)
- Multi-Factor Authentication (MFA)
- System for Cross-domain Identity Management (SCIM)

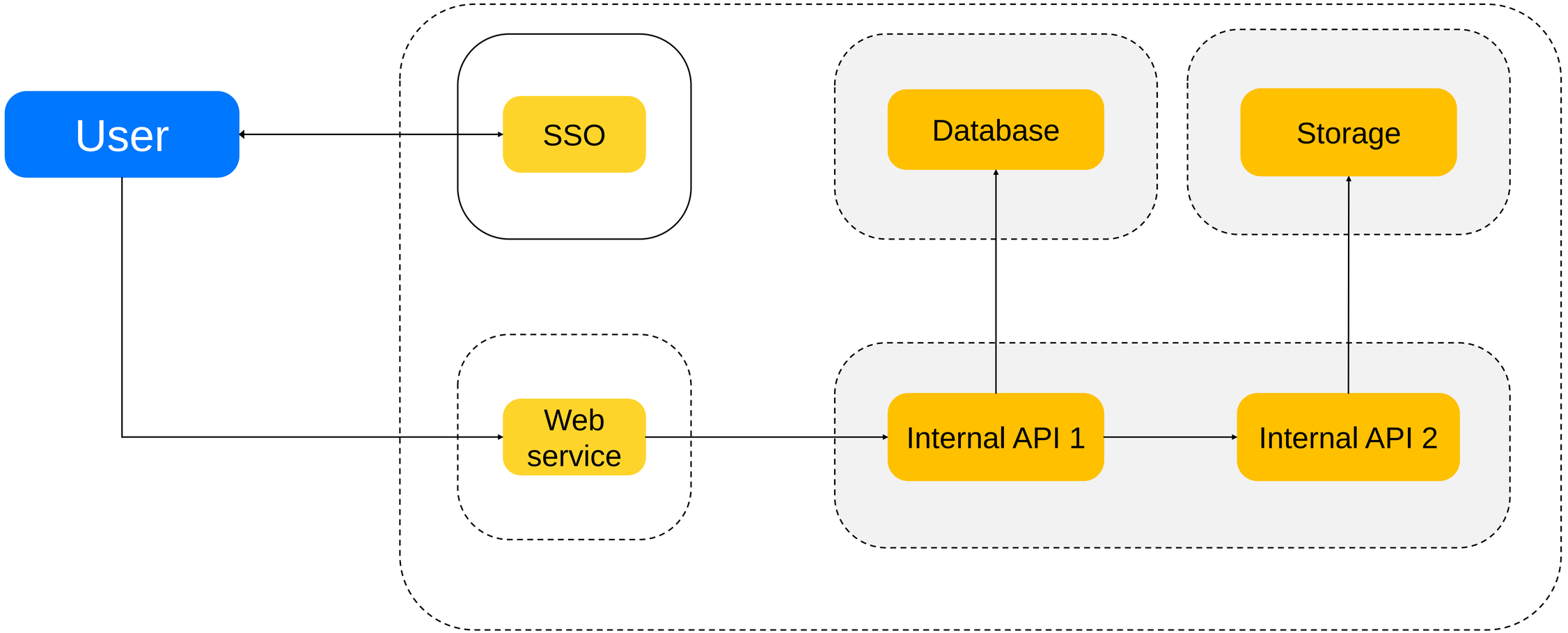
Single Sign On

- Source of trusted user identity
- Single management point for authentication methods

Multi-Factor authentication

- Knowledge (PIN, Password)
- Possession (Mobile Device, Token, …)
- UX

Single Sign On



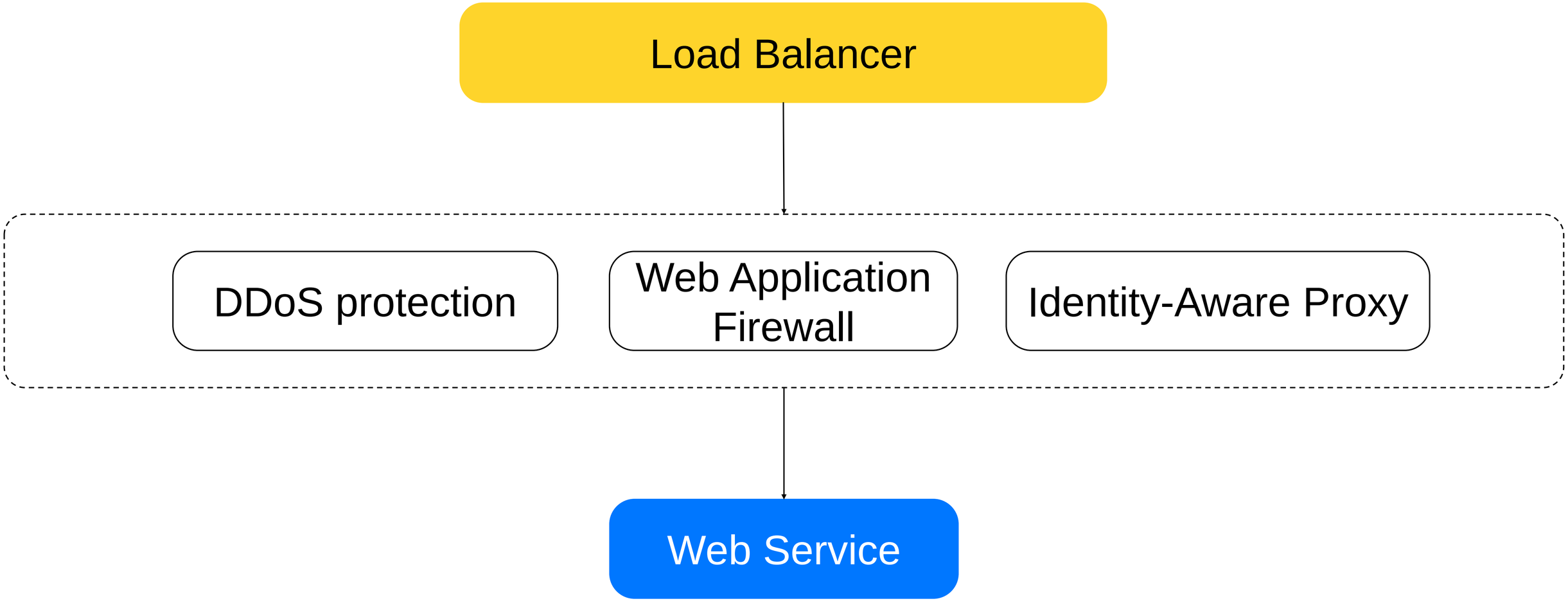
Zero Trust: attribute-based access control

- Identity Aware Proxies
- Zero Touch Production

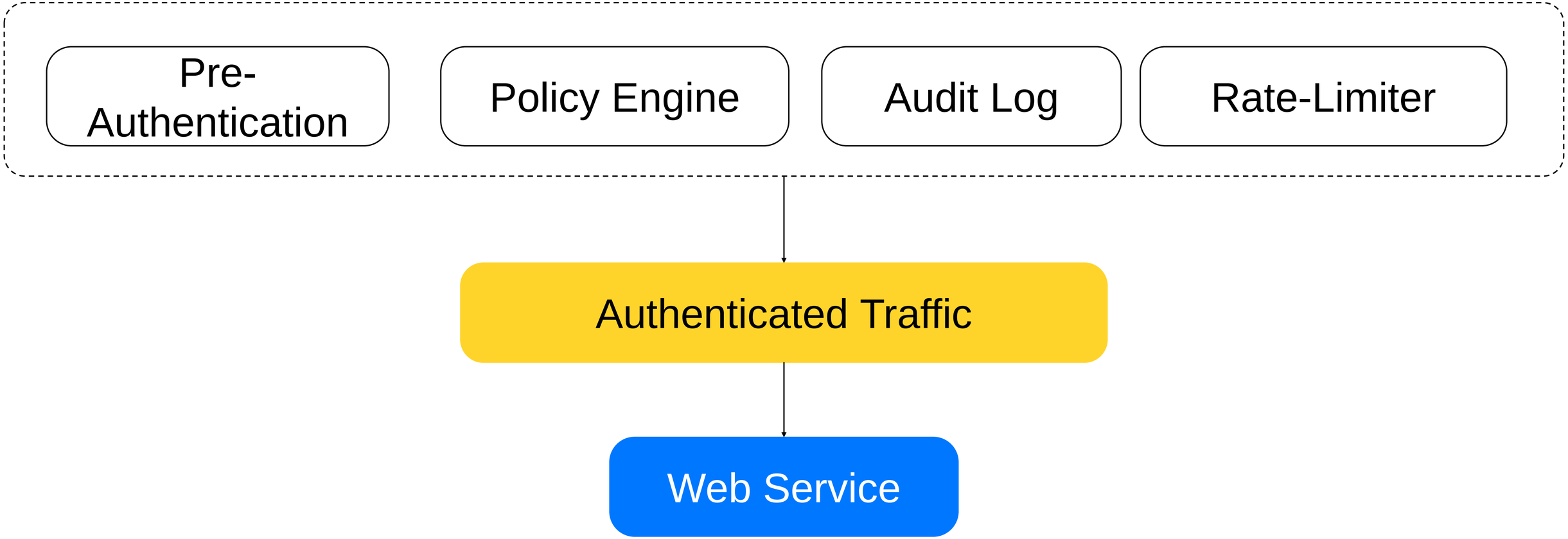
Identity Aware Proxies

- Authorization and policy enforcement
- Full audit log from services
- Rate-limits and anomaly detection
- Observability

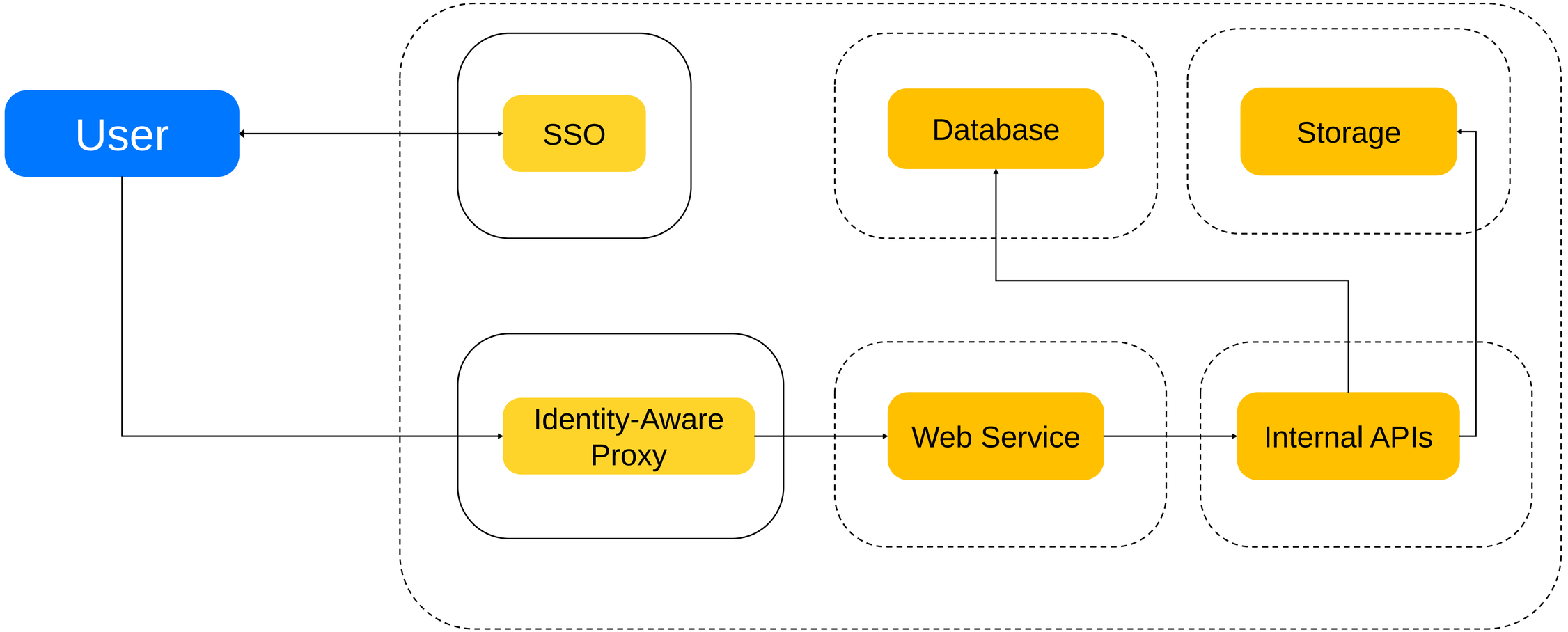
Web Service ZTP Access Scheme



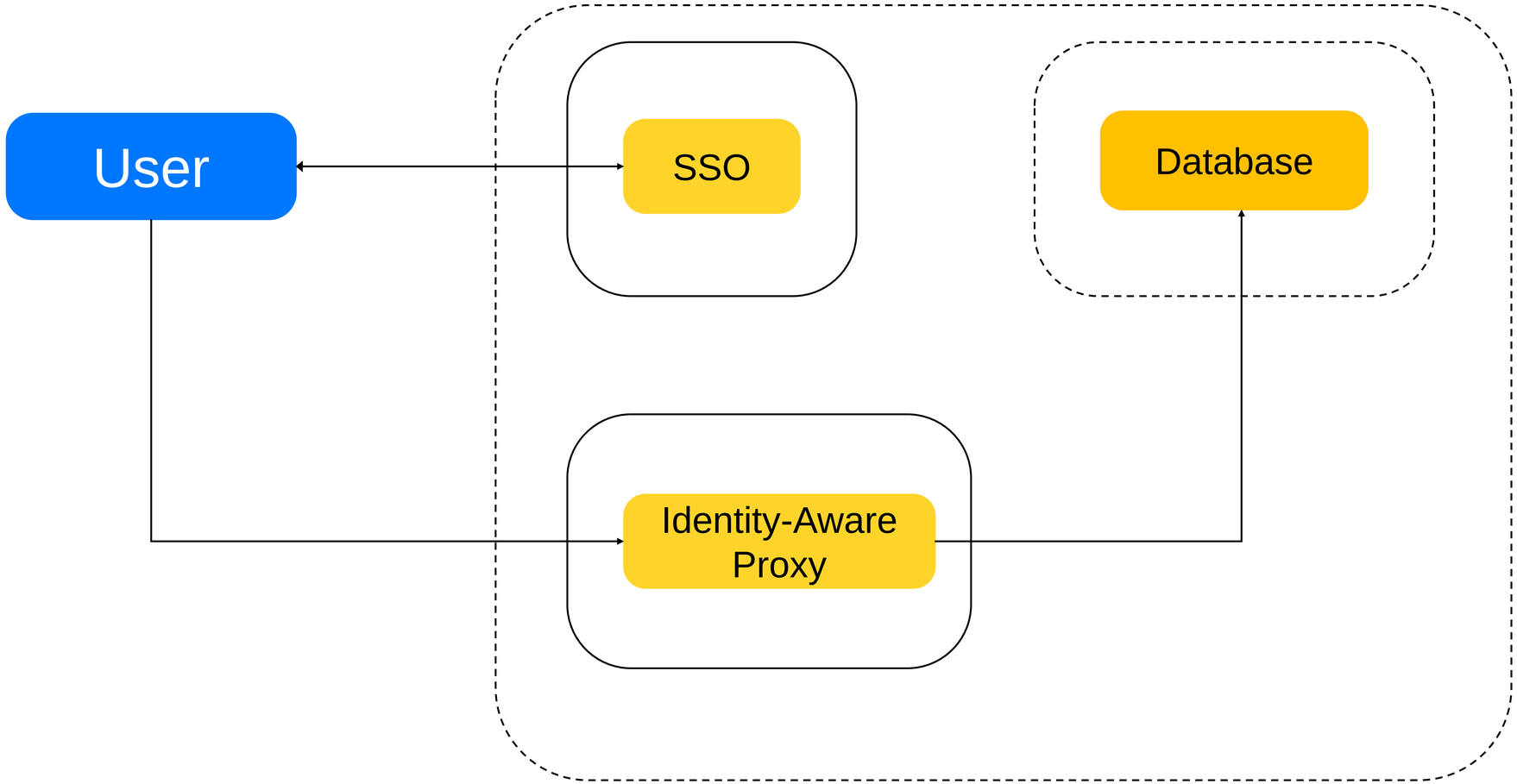
Identity-Aware Proxy



Identity Aware Proxy



Identity Aware Proxy



Zero Trust: software supply chain

- 3rdparty dependencies and Software bill of materials (SBOM)
- Code and artifact integrity
- CI/CD pipelines security

Zero Touch Production

- Humans do not have privileged access to production environments
- Changes in production are automated, described by code and pre-validated
- Humans use only break-glass mechanisms

Zero Trust: logging and monitoring

- Log coverage
- Behavior analysis
- Data-access flows
- Feedback to policy engine

Яндекс

Thank you! Questions?

Eldar Zaitov


ezaitov@yandex-team.ru


@kyprizel