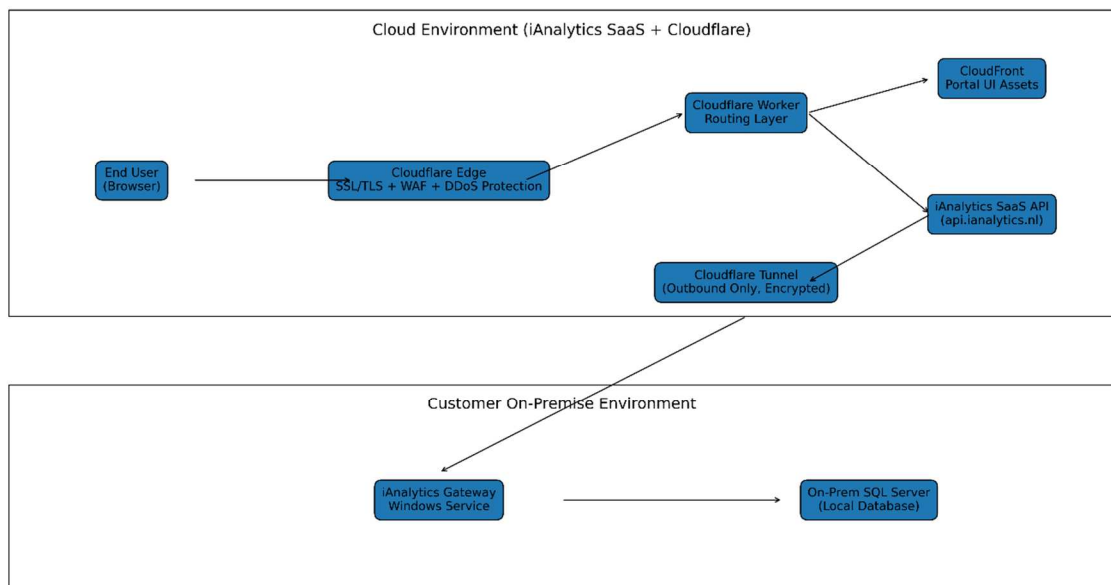


Afterbase Platform Architecture and Security Overview

1. Architecture Overview

The Afterbase platform combines a cloud-based SaaS environment with a secure on-premise gateway installed within the customer's infrastructure. The design ensures secure connectivity, logical isolation per customer, and minimal network exposure.



Traffic Flow

- End users access the portal via *portal.<customer-domain>*.
- Cloudflare Edge provides TLS/SSL termination, WAF protection, and DDoS mitigation.
- Cloudflare Worker routes UI traffic to CloudFront and API traffic to *api.ianalytics.nl*.
- The SaaS backend communicates with the customer environment via Cloudflare Tunnel.
- The on-premise Afterbase Gateway connects locally to the SQL Server database.

2. Network Security Model

The architecture follows a no-inbound-exposure principle. The gateway does not require any inbound firewall rules or publicly exposed services.

- No inbound firewall ports are opened.
- No port forwarding is required.
- No public IP address is required for the gateway.
- All communication is encrypted via TLS.

The gateway initiates an outbound-only encrypted tunnel to Cloudflare. Although communication is bi-directional at application level, no external system can initiate a direct inbound connection to the gateway.

3. Access Control and Isolation

Access to the gateway subdomain is restricted through IP-based firewall rules at the Cloudflare edge.

- Only traffic originating from the Afterbase backend infrastructure is permitted.
- All other traffic is blocked before reaching the tunnel.
- All SaaS endpoints require JWT-based authentication.
- Each company (Afterbase customer) operates with a dedicated gateway instance.

4. Availability and Continuity

The Afterbase Gateway runs as a Windows Service to ensure operational stability.

- Automatic startup on system reboot.
- Automatic restart upon unexpected failure.
- Persistent tunnel management and reconnection logic.

If the tunnel is temporarily unavailable, the SaaS platform remains operational. Once connectivity is restored, communication resumes automatically.