18. DNS, CDN & Network services

Summary

- Continue using Cloudflare for domain registration, DNS, CDN, and managed SSL/TLS, with local alternatives for unsupported domain registrations.
- Consider Azure Traffic Manager, Application Gateway, or similar cloud-native offerings for DDoS protection, WAF, multi-layer load balancing, bot-mitigation, and analytics.
- Automate all networking setup and certificate management via infrastructure-as-code to ensure consistency, reproducibility, and minimal manual intervention.

Pending Decisions & Open Items

- Specify bot-fighting and traffic-analytics tooling, metrics to collect, and alert thresholds.
- Document certificate renewal workflows, key-rollover procedures, and disaster-recovery drills for network services.

Overlaps with

- 2. Security & Compliance
- 4. Microservices & Scalability & Performance & Reliability
- 16. Hosting

Overview

In the majority of cases this area is the first contact point between end-users and our services. It has to work flawlessly, performantly, securely but most of all: once setup, being able to stay completely under the radar and just working as expected. This **is a hammer**, it is of no use trying to reinvent it or finding a so much better one. When it works things work and when it doesn't everything else fails.

What we need to keep on using: Cloudflare

The minimum requirements to provide:

- domain registration
- DNS
- provider managed SSL/TLS certificates
- CDN

The LISAX platform already uses, understands and rarely has problems with these... so let's stick to our reliable **Cloudflare** to handle these few aspects at least.

Note: Cloudflare can't deal with all top level domains (e.g no *.nl*). So use local alternatives.

Alternatives: Service categories | European Alternatives

Nice-to-haves

Additionally the following concerns can also be achieved through Cloudflare, or a public cloud provider’s (e.g. Azure) similar offering for a deeper integration with the origin services, e.g. Azure Traffic Manager & Application Gateway:

- DDoS protection & WAF (Web Application Firewall)
- DNS-, layer 7-, layer 4 load balancing and certificate termination
- bot-fighting
- analytics

Mandatory improvements

Automatization and offloading responsibilities to the service provider (e.g. certificate management). The setup for apps, services, sites does not differ that much, the minimum should be possible to be automated with configuration- & code-as-infrastructure, to normalize the setup and reduce manual chores.