dns belgium

Query Log Analysis

Detecting anomalies in DNS traffic

dns belgium

Presentation

- *Goal*
- *Challenges*
- *Implementation*

- *DEMO*

dnsbelgium

Goal

Design and build a working query log analysis platform using available components and custom development, able to predict, detect and report on common attack and abuse patterns in an open architecture, allowing for future growth and improvement.

dnsbelgium

Challenges

- Huge data volume
  - efficiency and scalability !
  - easy to stay under the hood
- Wide range of attacks, under constant evolution
- Specific nature of DNS traffic
  - periodicity and trends
  - few (typically two) packets per flow

dnsbelgium

Implementation

- Masters thesis (University of Leuven)
- Main components
  - Entrada
  - QLAD-flow
  - QLAD-global
  - QLAD-UI

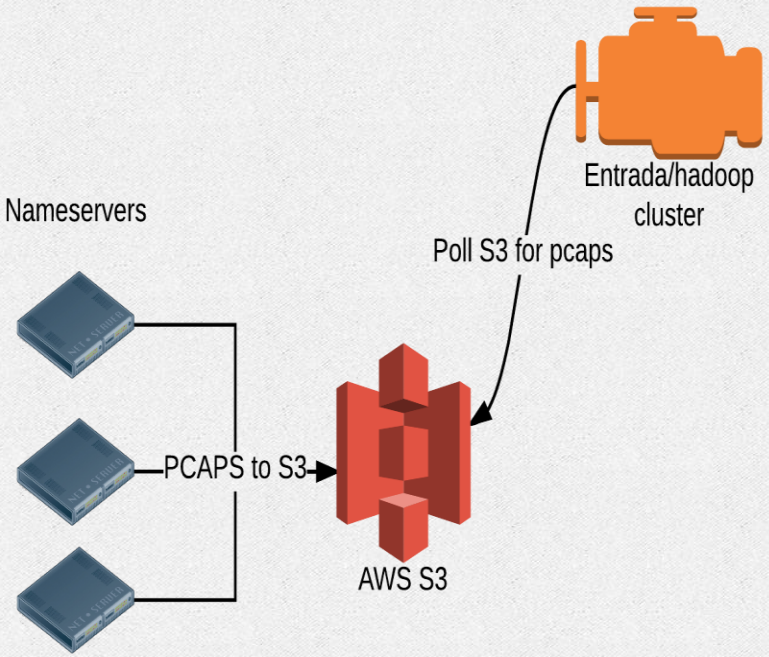
dnsbelgium

Implementation Entrada: why

- Efficiently store the data
- Efficiently query the data
- Designed to work with DNS

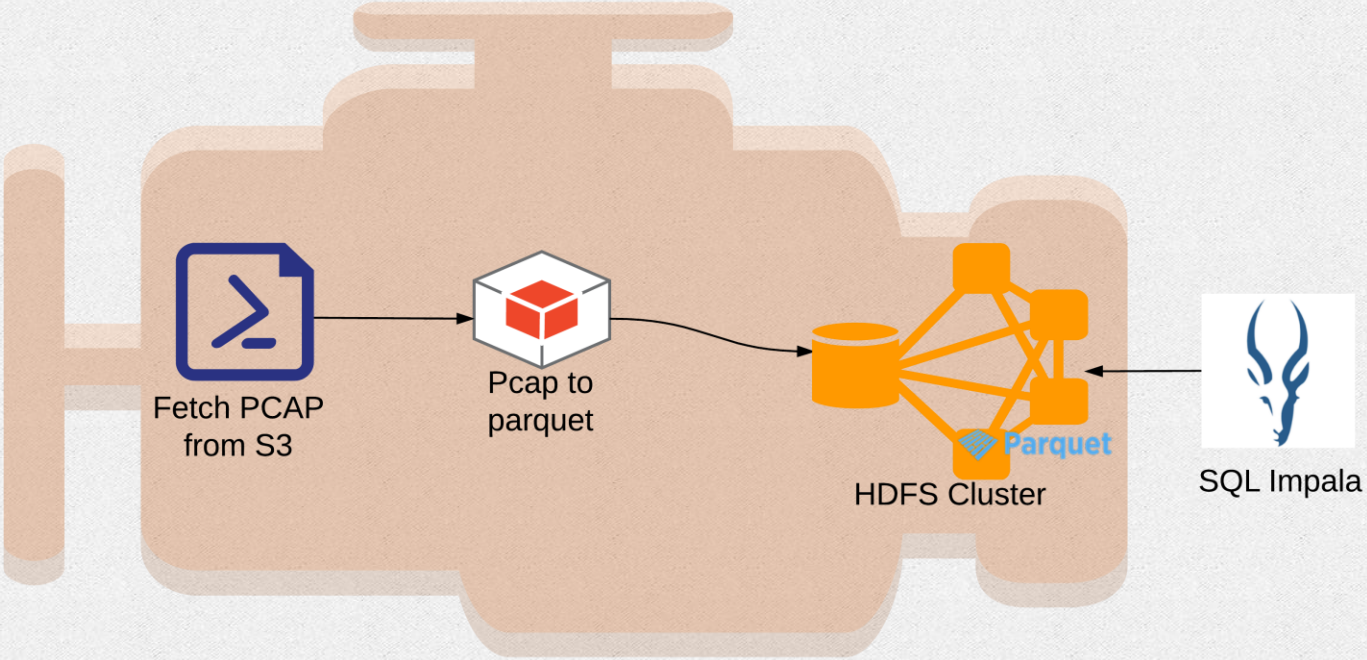
dnsbelgium

Implementation Entrada: architecture



dnsbelgium

Implementation Entrada: flow



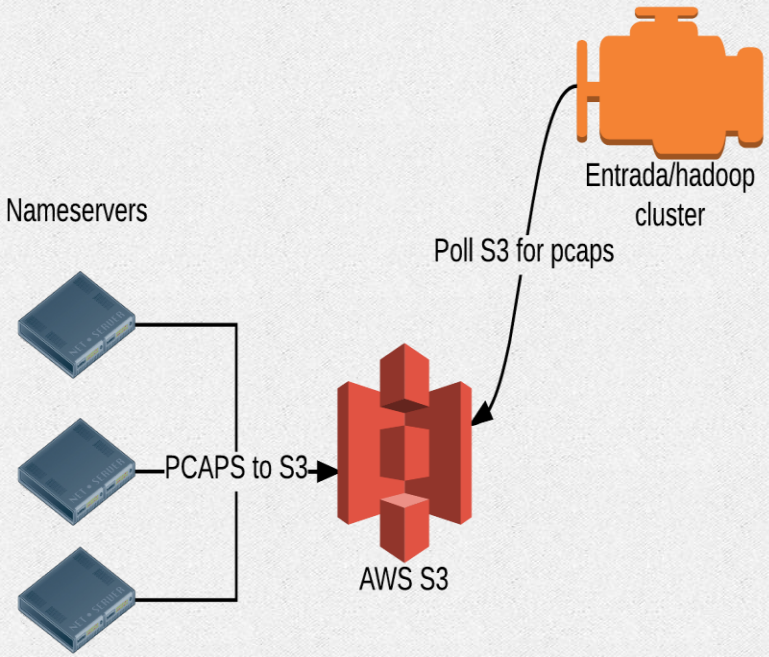
dnsbelgium

Implementation QLAD-flow: why

- Focus on anomalies (≠ attacks/abuses)
- Inspiration from network anomaly detection
- Able to detect low traffic anomalies
- Uses the algorithm developed by CZ.NIC

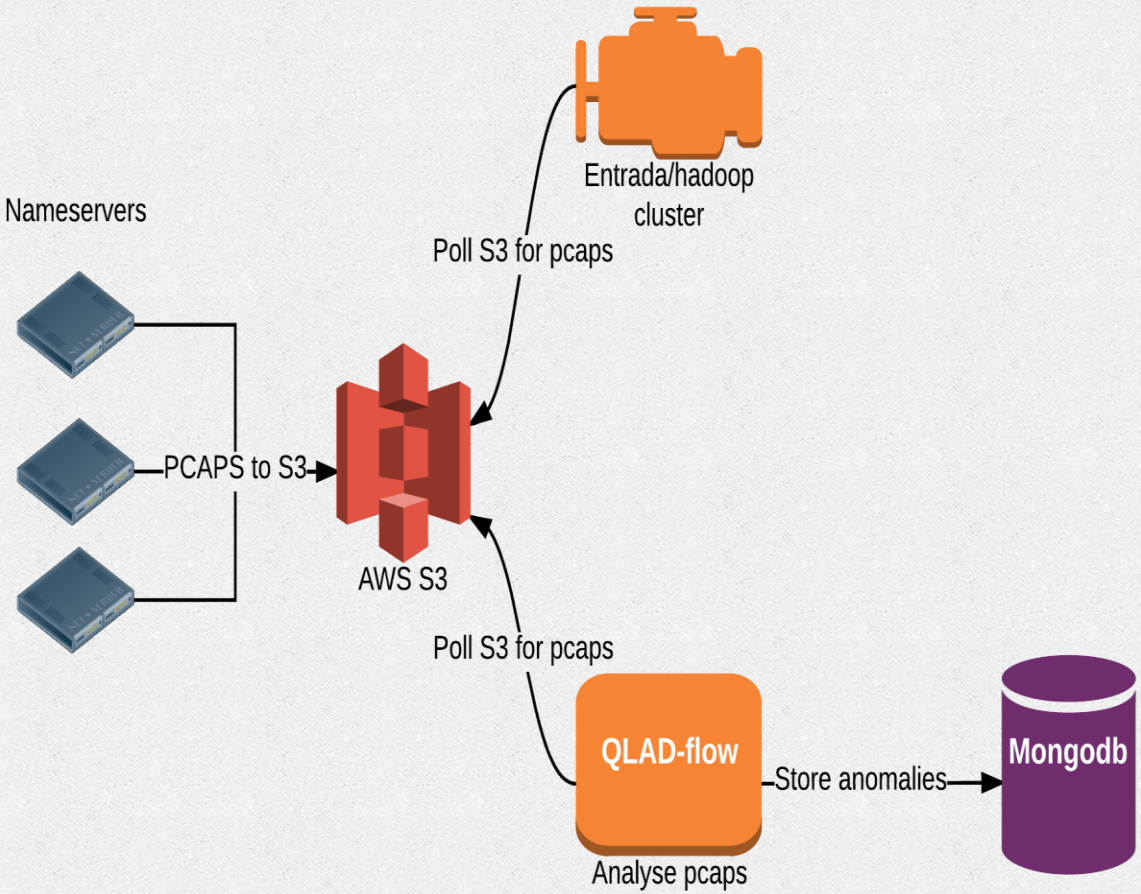
dnsbelgium

Implementation QLAD-flow: architecture



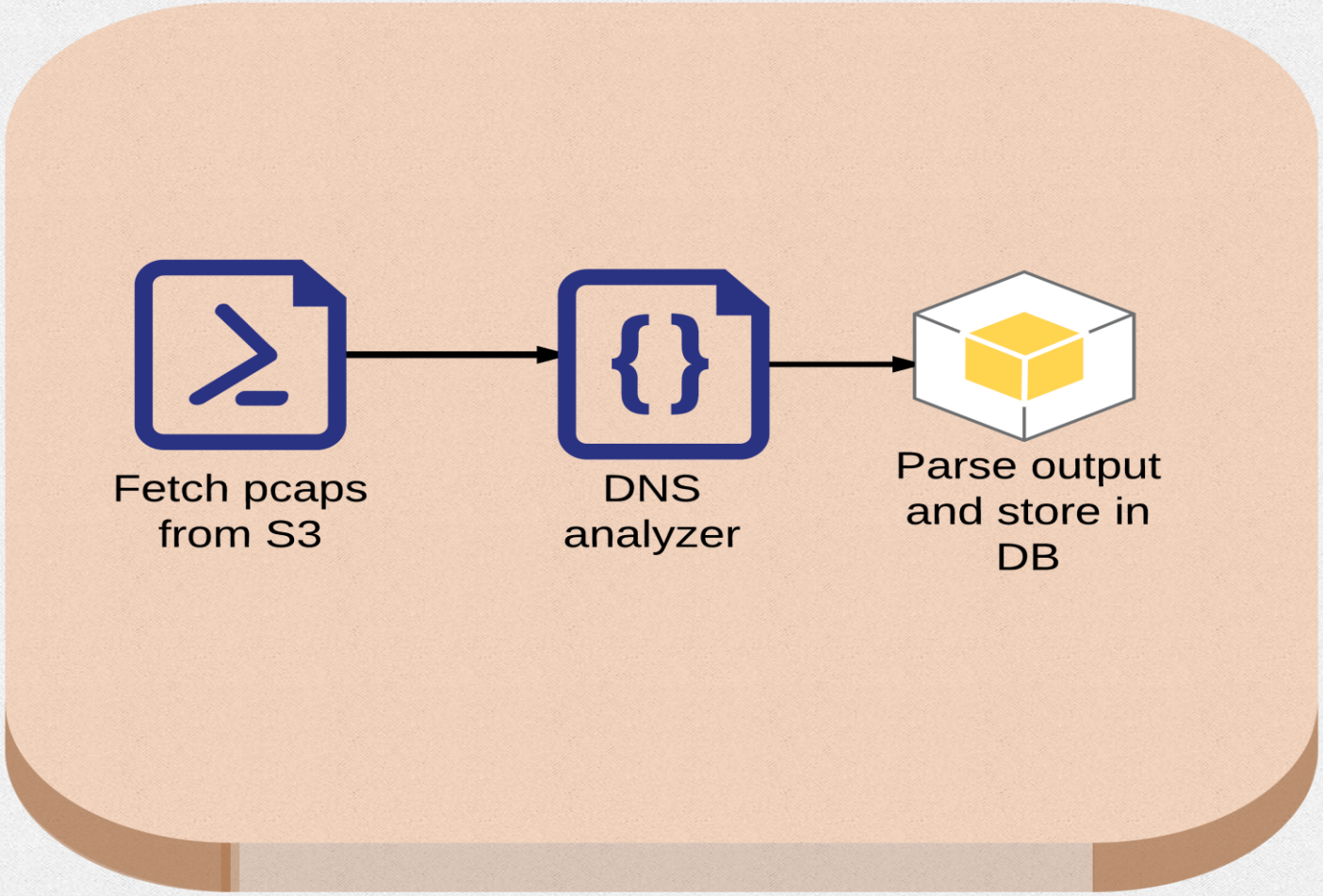
dnsbelgium

Implementation QLAD-flow: architecture

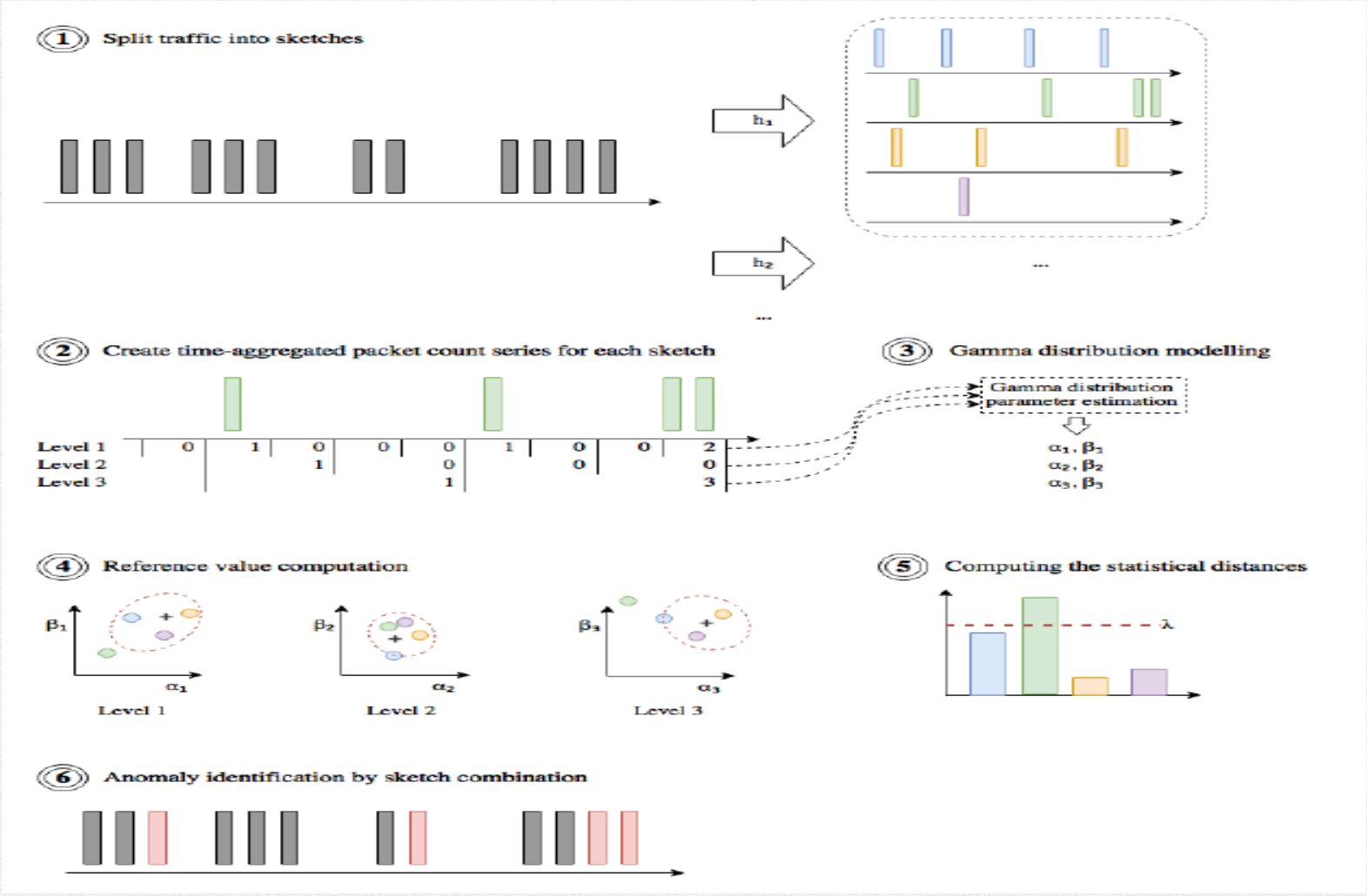


dnsbelgium

Implementation QLAD-flow: flow



Implementation QLAD-flow: algorithm



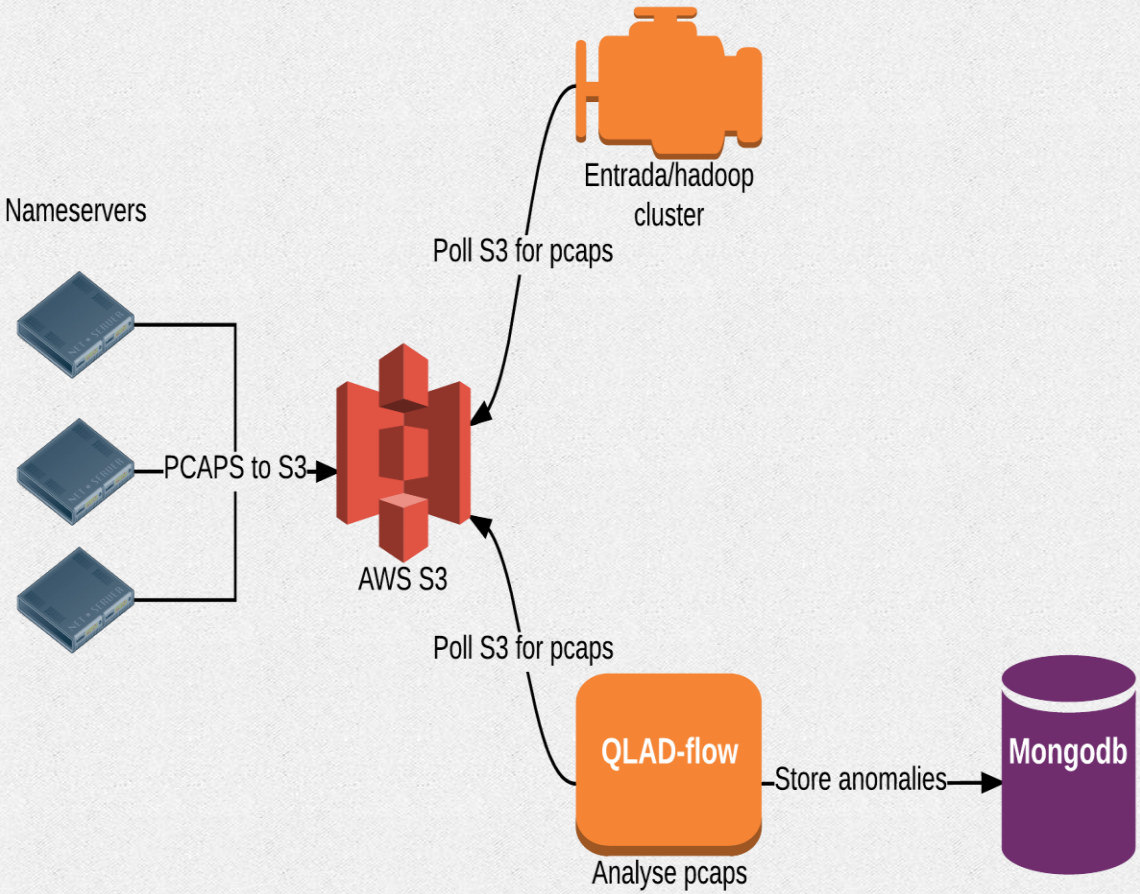
dnsbelgium

Implementation QLAD-flow: shortcomings

- Some attacks span a lot of flows -> QLAD-flow is unable to detect these (e.g. like DoS with spoofed IP address)
- QLAD-global was implemented to fill the gap

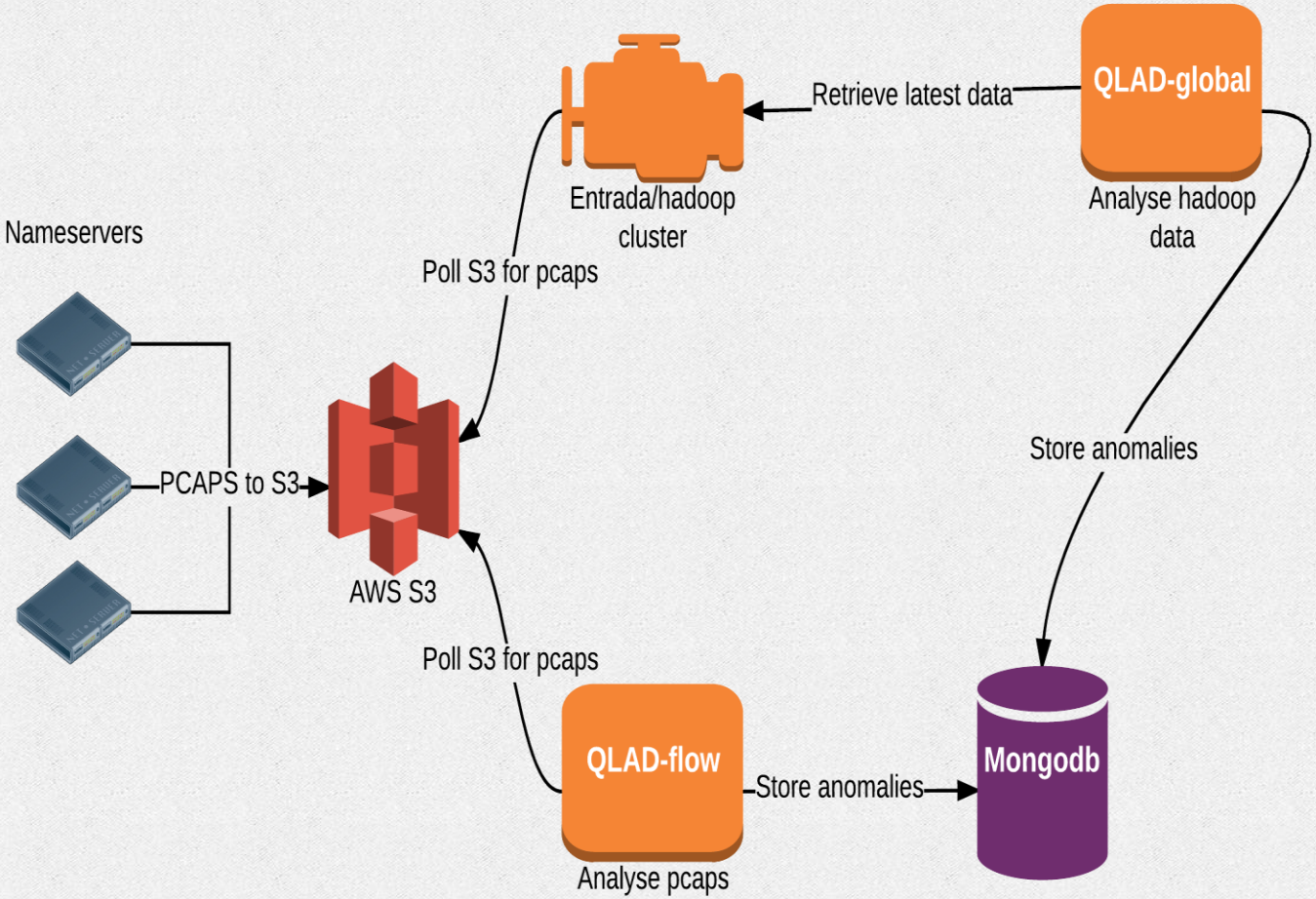
dnsbelgium

Implementation QLAD-global: architecture



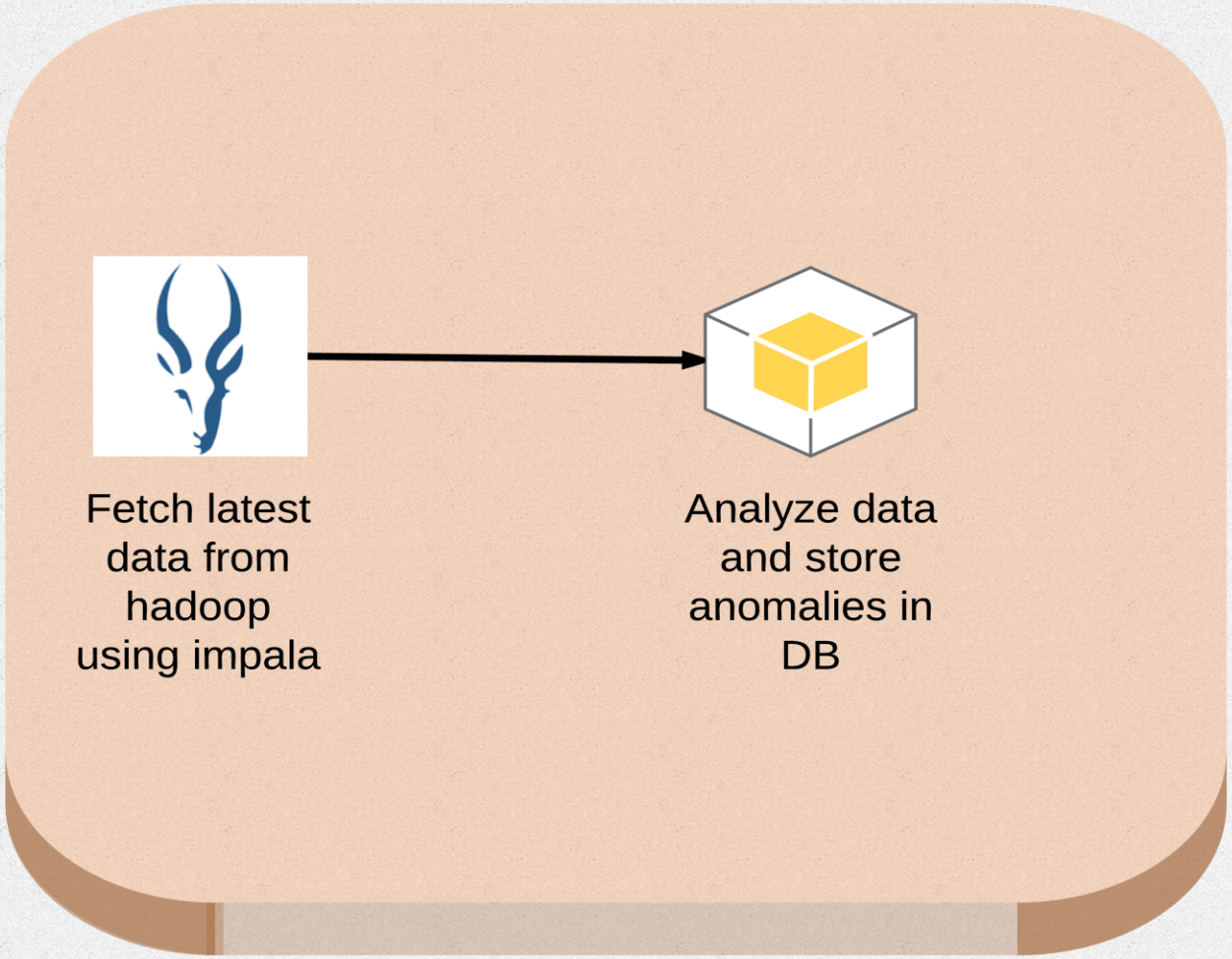
dnsbelgium

Implementation QLAD-global: architecture



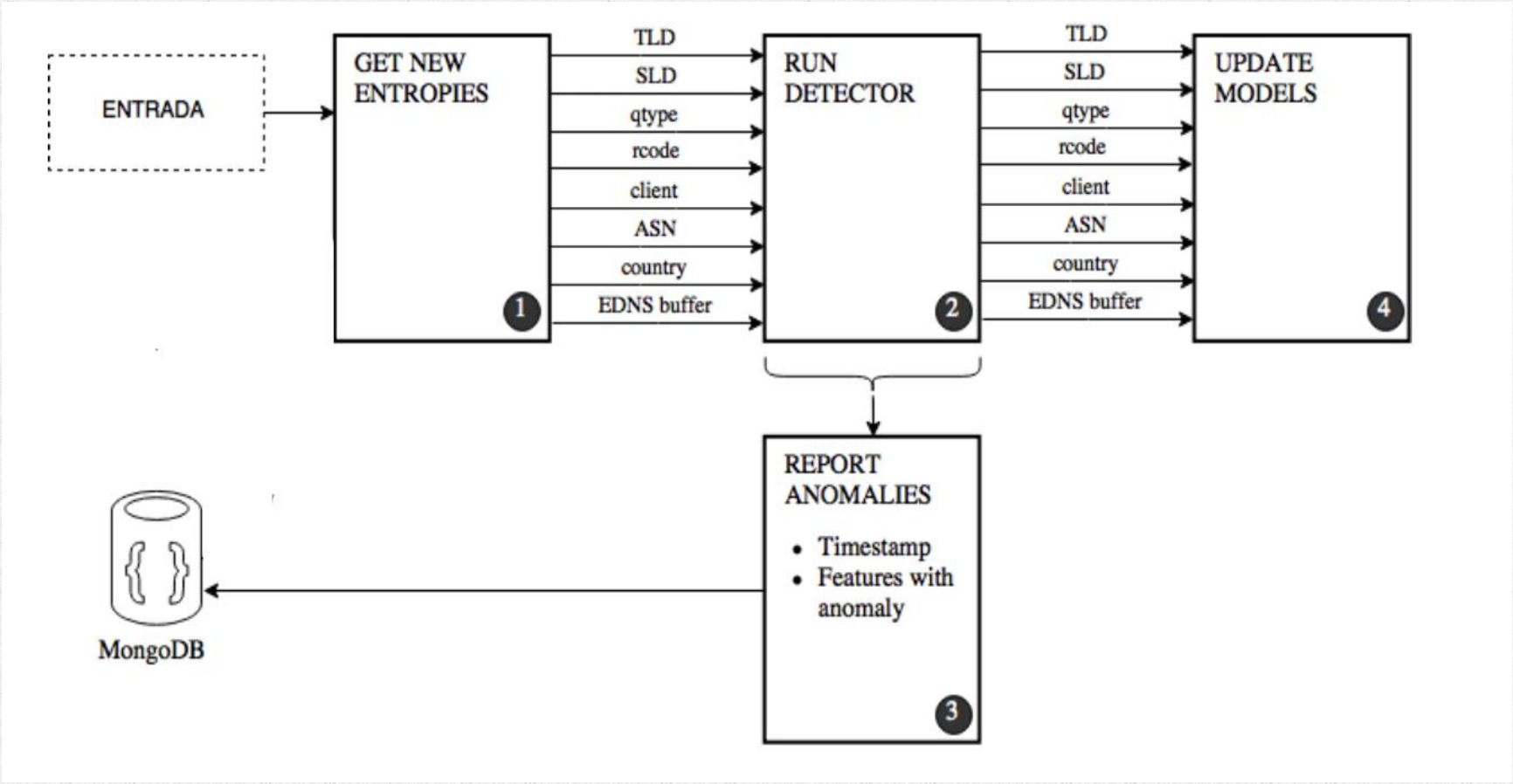
dnsbelgium

Implementation QLAD-global: flow



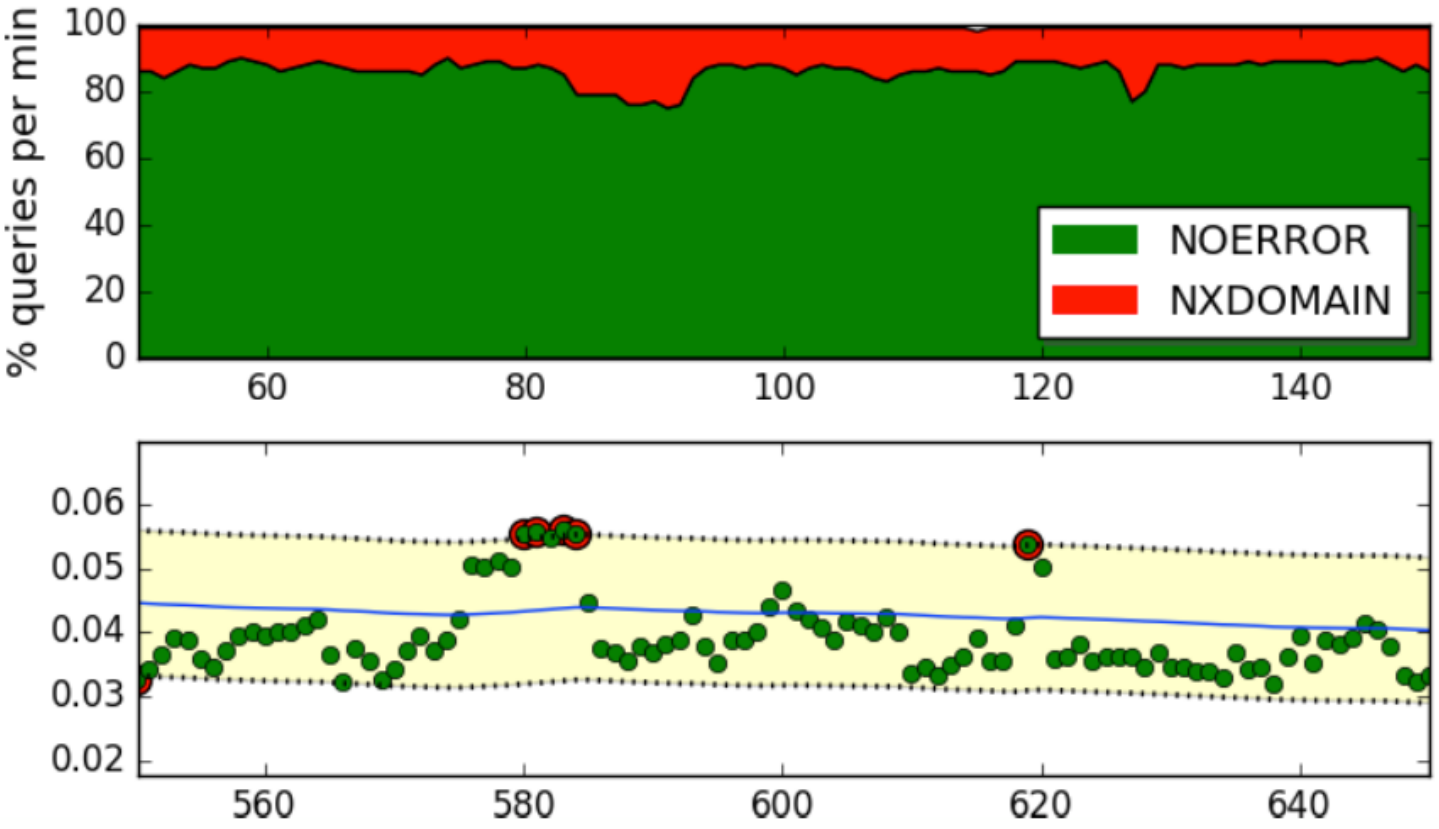
dnsbelgium

Implementation: QLAD-global: algorithm



dnsbelgium

Implementation: QLAD-global: algorithm result



dnsbelgium

Implementation: QLAD-UI

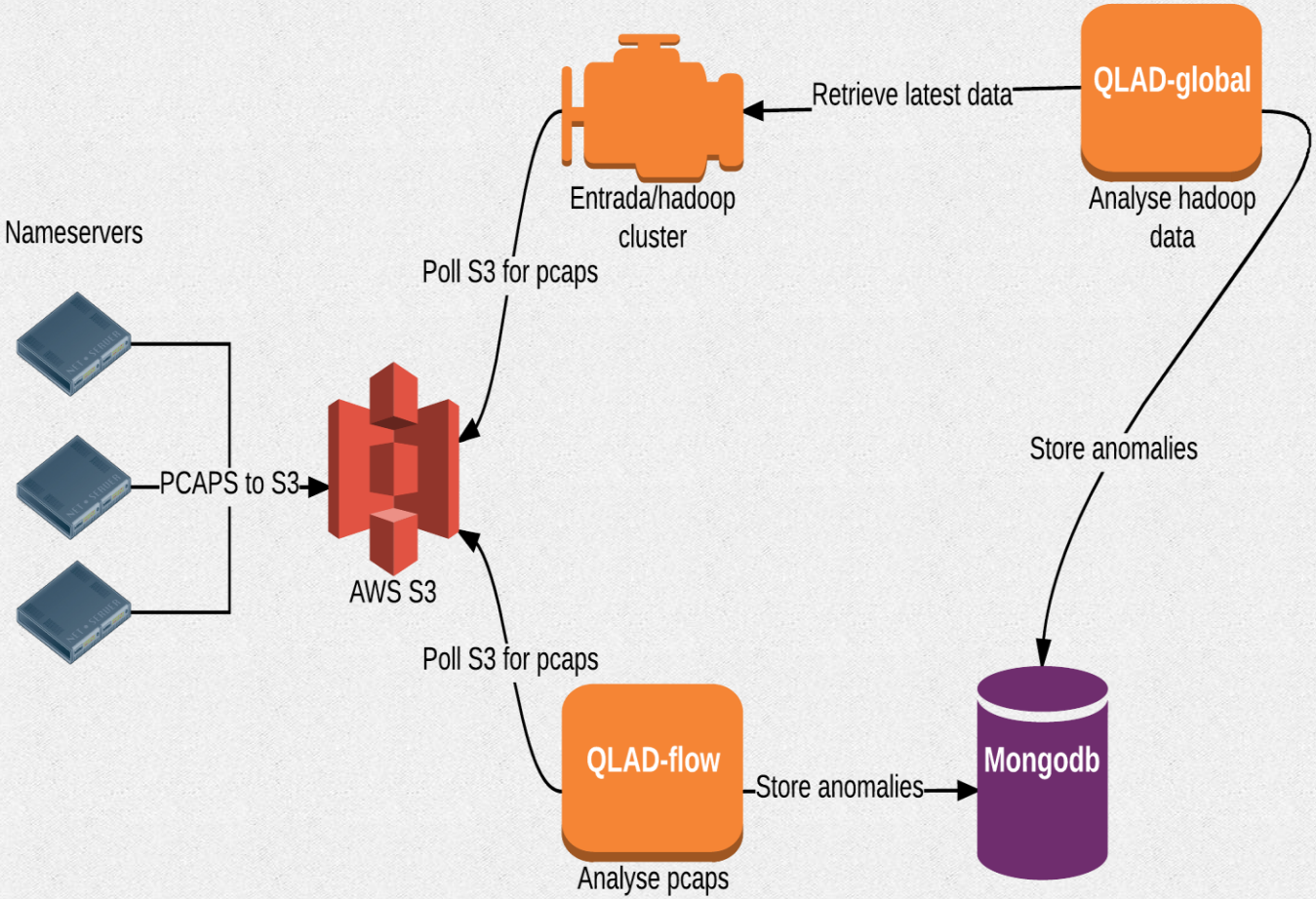
Automatic classification is challenging

- wide range of anomalies
- subtle differences

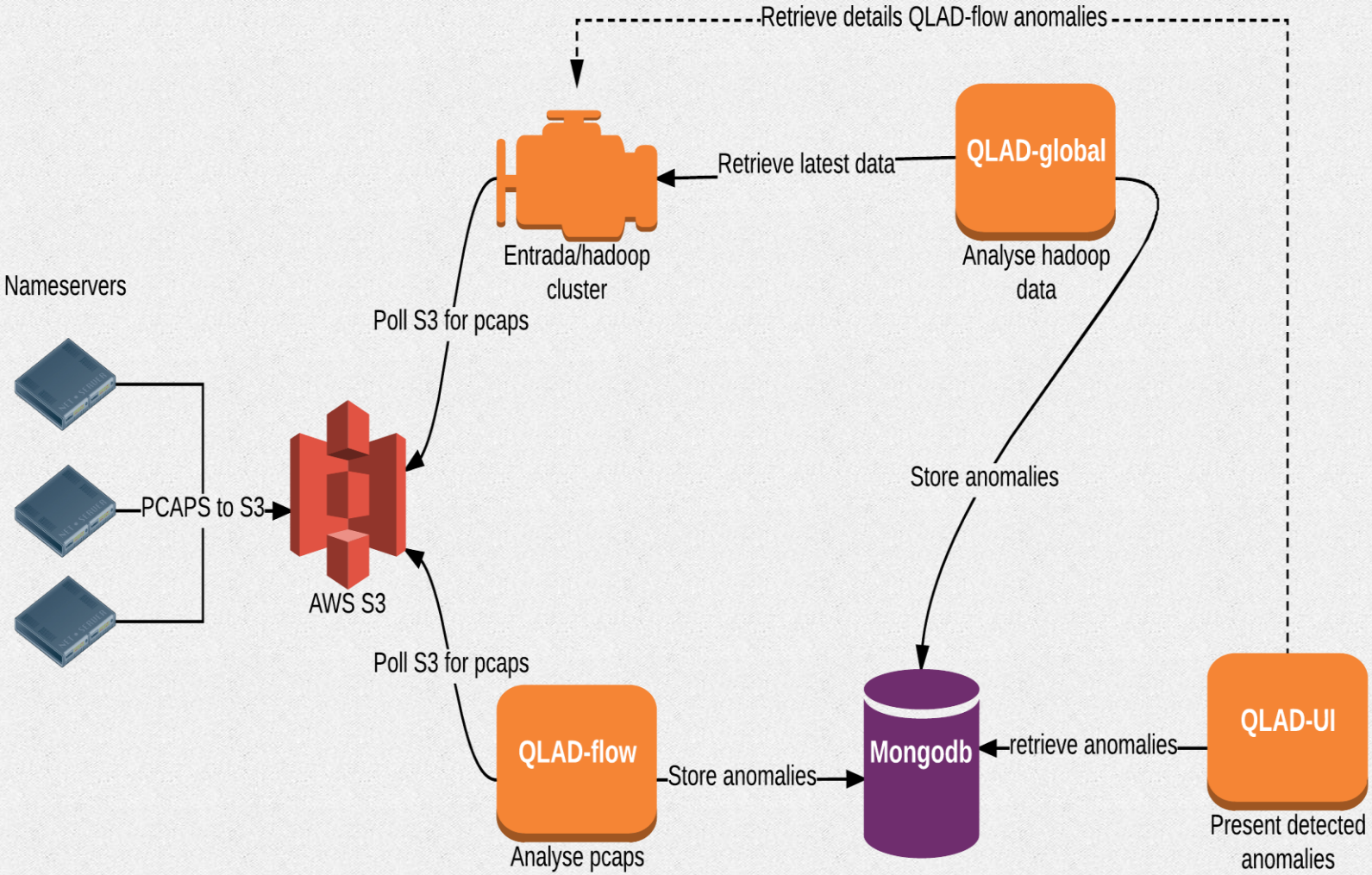
=> Rely on human interpretation of the detected anomalies by QLAD-global and QLAD-flow

dnsbelgium

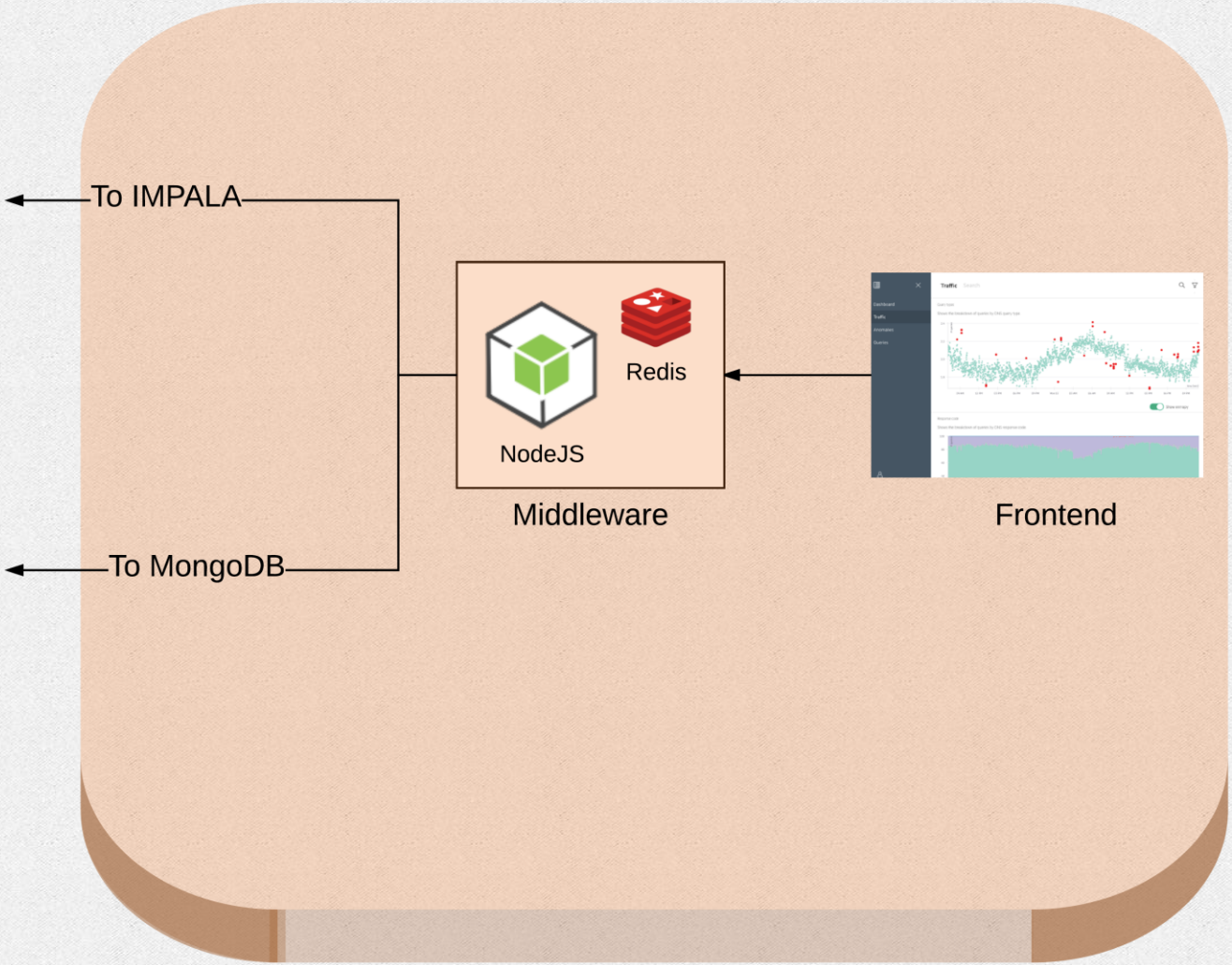
Implementation QLAD-UI: architecture



Implementation QLAD-UI: architecture



Implementation QLAD-UI: flow



dnsbelgium

Demo

dns belgium

Questions?