Internal Routes on cloud.gov

17 March 2021

Mark Headd

Consulting Engineer

Steve Greenberg

Platform Operator (contractor)

Overview

- What are internal routes?
- How do they work?
- What are the benefits of internal routes?
- When should you use them?
- Demo

What are internal routes?

- Routes used with apps that only accept traffic from other cloud.gov apps
- Traffic does not come through Gorouter, only from another container
- Granular control over source, type, and port(s) of traffic via network policies

How do they work?

- Created using the `*.apps.internal` domain
- Traffic to apps must be explicitly allowed using network policies
- Enabled by an overlay network that manages traffic between app instances
- Traffic never leaves cloud.gov environment

What are the benefits?

- Hide components of your solution from external traffic
- Enhanced security via private, container-to-container communication
- Reduced latency between components
- Service discovery

When should you use them?

- Front end apps w/ backend APIs
- Websites or apps that need access control (e.g., an “intranet” application)
- Companion services that are only used by your application (e.g., ClamAV service)
- Docker images that expose non-8080 port

Demo

Comments & Questions

- TLS and encryption of internal traffic
- DNS timeout issue
- Other questions?

Getting involved:

https://github.com/cloud-gov/tech-talk-internal-routes

Example apps:

- https://github.com/cloud-gov/custom-fluentd: Adds basic authentication to fluentd
- https://github.com/cloud-gov/docker-registry-mirror: Adds IP filtering to a docker registry mirror
- https://github.com/18F/clamav-api-cg-app: ClamAV service to scan file uploads