Empowering DevSecOps

Unleashing F5, NGINX and Modern Applications

Fabrizio Fiorucci

Solutions Architect

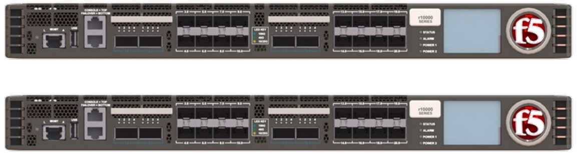
Solna - March 6th, 2024

Securing and Delivering Every App, Every API, Anywhere

The F5 solution portfolio – Full Proxy DNA

App Services for Traditional apps

F5 BIG-IP

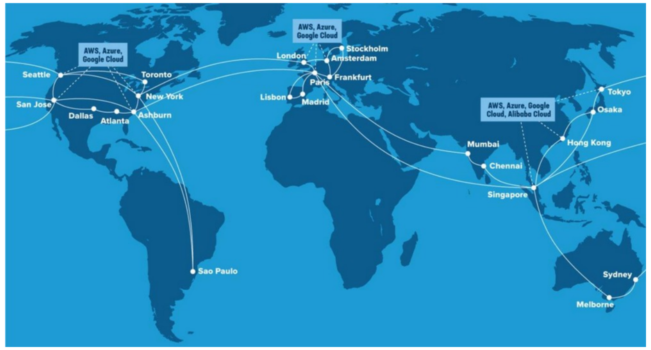


App Services in Micro-services environments

F5 NGINX

Self-service / SaaS Simplify Operations

F5 Distributed Cloud



The History of NGINX

- NGINX was created by Igor Sysoev in 2004 to solve the C10k problem
- The initial release of NGINX was in 2004
- NGINX is now used by over 450 million websites worldwide
- In 2011, NGINX, Inc. was formed to provide commercial support for NGINX
- In 2019, F5 Networks acquired NGINX Inc.
- **F5 and NGINX are committed to open source**
- https://opensource.f5.com/

NGINX Open Source

NGINX
JavaScript

Unit
An NGINX Project
Applications and API server

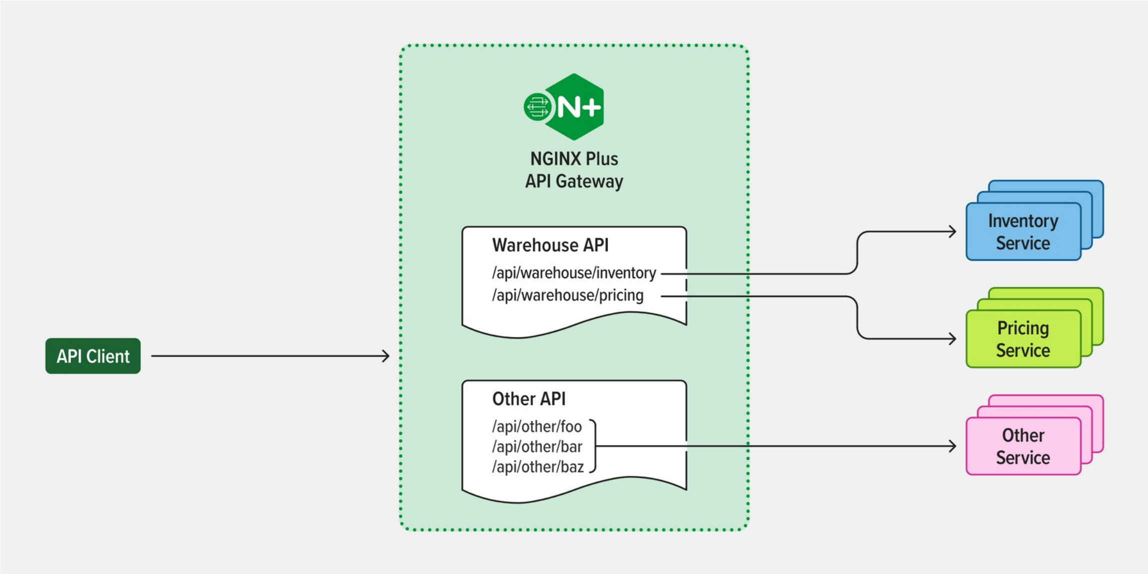
NGINX Gateway Fabric

Experiment with the new Gateway API using NGINX as the data plane

NGINX Primary Use Cases

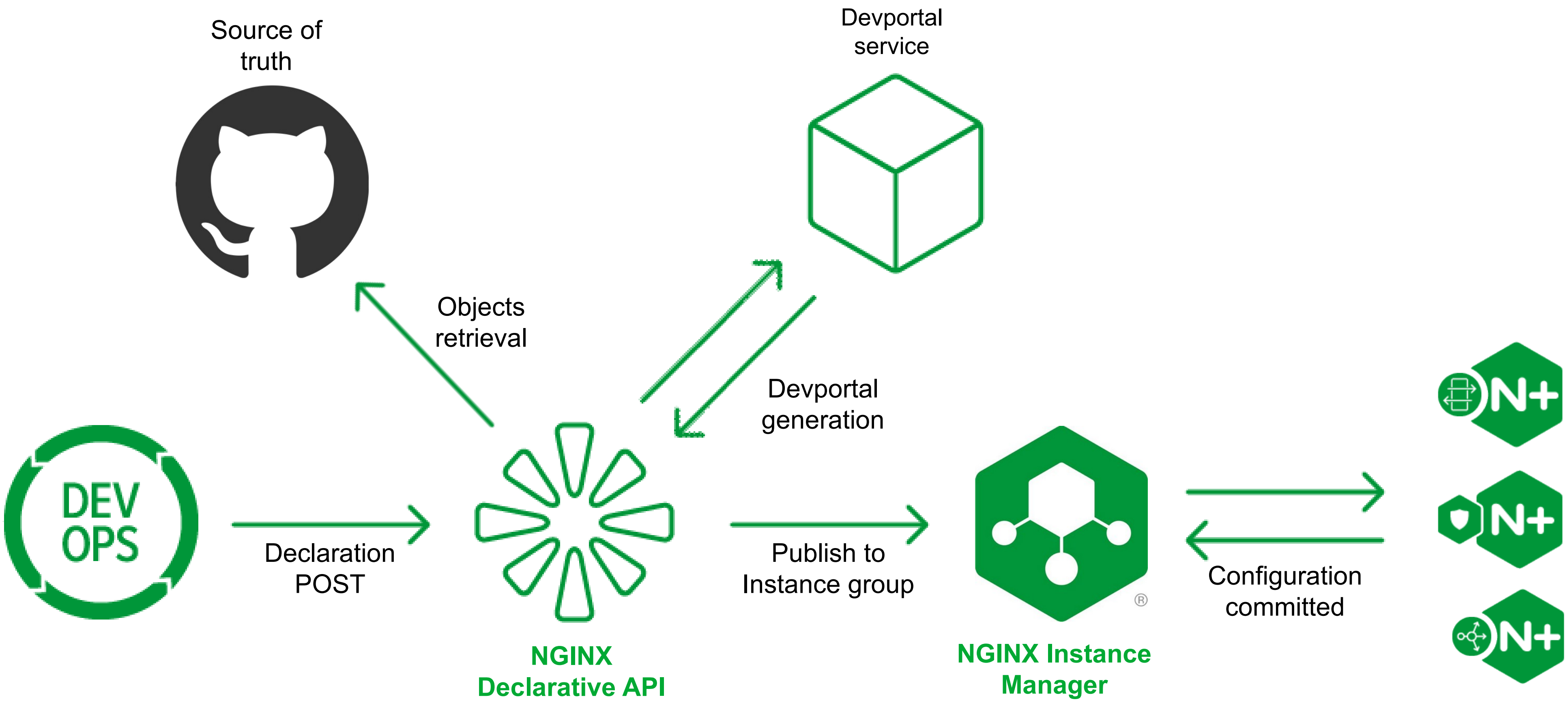
- **API Gateway**: A server that acts as an API front-end, receives API requests, enforces throttling and security policies, passes requests to the back-end service and then passes the service’s response back to the requester.
- **API and Web Apps Security**: The protection of the integrity, confidentiality, and availability of the APIs and the data they exchange.
- **Kubernetes Ingress Controller**: An API object that manages external access to the services in a cluster, typically through HTTP.
- **Kubernetes Gateway Fabric**: A set of components that provide a control plane for the configuration of ingress gateways.
- **Reverse Proxy**: A server that retrieves resources on behalf of a client from one or more servers and returns the resources to the client as if they originated from the reverse proxy itself.
- **Web Server**: A server that stores, processes, and delivers web pages to clients.

NGINX as an API Gateway



- NGINX acts as a central point of control for all API traffic.
- It helps in enforcing security policies by authenticating and authorizing API requests.
- It provides throttling to prevent API servers from being overwhelmed with requests.
- It improves performance through caching and load balancing.
- It enables versioning of APIs, which makes it easy to manage changes.
- It helps in reducing the complexity of the application architecture by abstracting the API layer.

NGINX as an API Gateway – the DevSecOps way



Demo

Q&A