API GATEWAY

Introduction

ESDC Interoperability directorate identified a technology gap in ESDC infrastructure that is critical to enable sharing of data and functions via APIs.

This document will review the background and capability enablement needed to that is required to have ESDC comply with the GC Architecture Standards, the Directive on Service and Digital, and meet or exceed the industry standard of API management services.

Background and GC Direction alignment

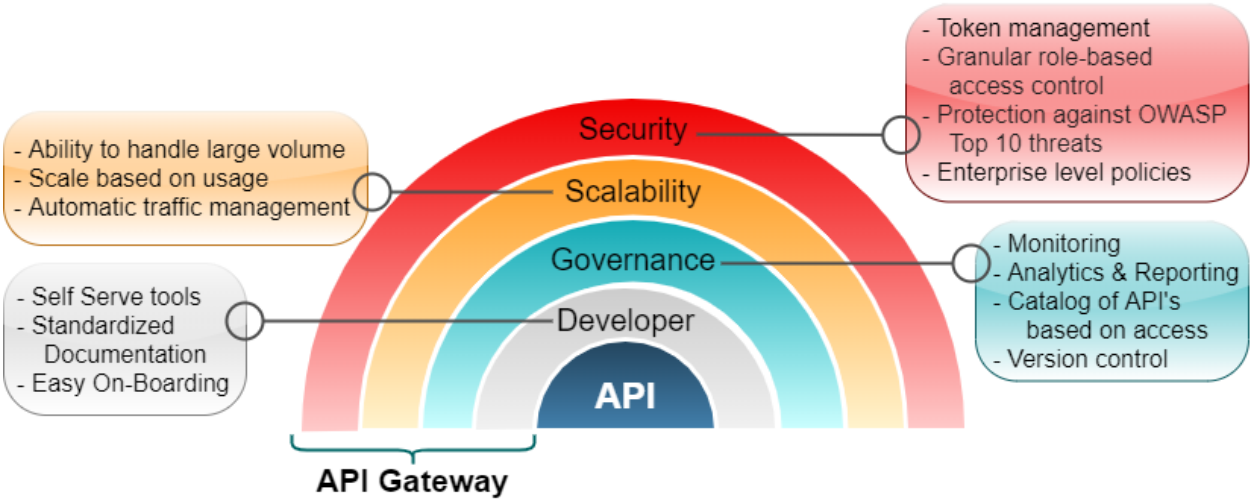
Application Programming Interfaces (API's) are the basis of an interconnected ecosystem of application and can be leveraged to facilitate the sharing of government data. TBS collaborated with ISED to create a Government of Canada API Store in the cloud that serves as the authoritative source of APIs made available to external GC clients, as part of the greater Canadian Digital Exchange Platform initiative. The Directive on Service and Digital has specifics requirements relating to data interoperability (Directive requirement #4.3.1.3) and ensuring IT services are designed and managed to support interoperability (Direcetive requirement #4.4.1.8). The Government of Canada Architecture Standards further embeds these requirements as Application Architecture domain standards to enable Interoperability via APIs.

These requirements will require departments to produce and manage APIs as they are the main technical methods to enable interoperability. The Directive requires departments submitting initiatives to the GC Enterprise Architecture Review Board to be assed against Mandatory Procedures for Application Programming Interfaces (Directive requirement #4.1.1.5). Complying with this directive would contribute to growing the capabilities of the government of Canada to share its data, position ESDC as a leader in the digital enablement of the GC, and move the government as a whole closer to its OneGC vision

API Enablement

In order to expose vital services and information with the private sector, provincial governments, other government agencies and departments, or Canadian citizens, ESDC must use APIs. The use of APIs require investment in an API architecture where the ESDC Interoperability directorate identified a key gap in security to enable the department in meeting the Government of Canada's expectations and TBS Canadian Digital Exchange Platform roadmap.

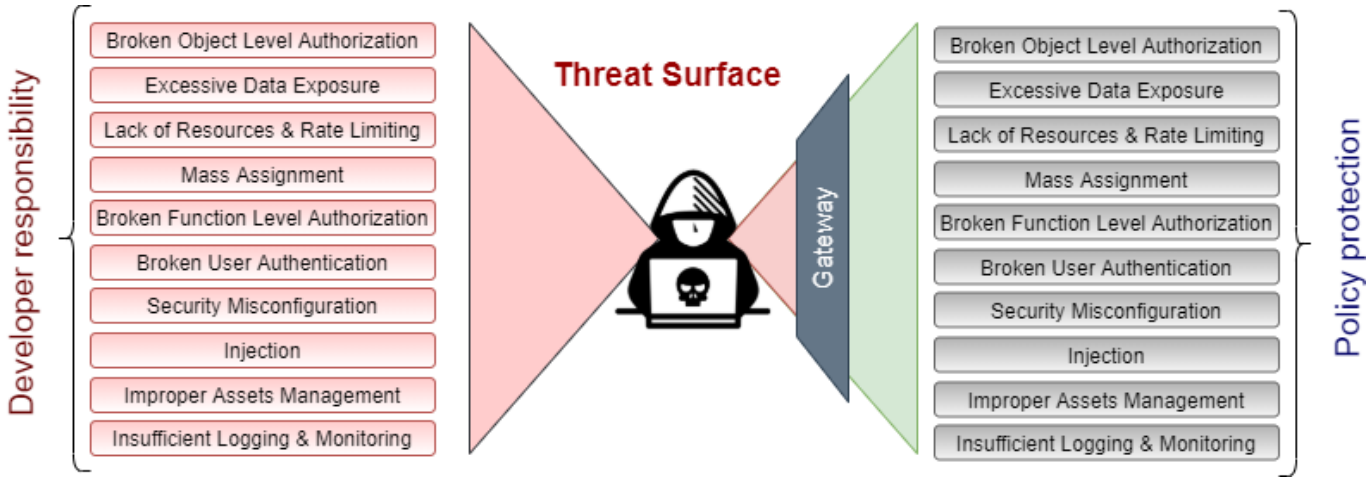
ESDC Interoperability directorate identified a key gap in security to achieve the TBS API roadmap. The following diagram provides areas of interest for enabling the API Gateway at ESDC:



API Security

Security is a major concern with the type of data that ESDC deals with and that is iterated in the Policy on Service and Digital when it calls all departmental deputy heads to designated a new official responsible for leading the departmental cyber security management function (Policy requirement #4.1.3.4). When dealing with API Security, API Gateways are the best tool to protect our APIs. Security was traditionally aligned toward website architecture, where the website interfaces were zoned to allow data to be protected, and for websites to 'secure' the access and exposure of information to a visitor. With API's the traditional website architecture does not offer security, as there is no web interface that protects a service from malicious or incorrect usage, this is where a API Gateway enables and empowers the API Architecture.

OWASP is the authority in terms of tracking the biggest security vulnerabilities and they keep a Top 10 list. Securing an API is so different than securing a website that they have a Top 10 specifically for APIs (see appendix). On their own, each developer would be required to protect their API against each of those vulnerabilities. The API Gateway automates and standardizes the protection at an enterprise level, providing administrators a wide range of tools to secure the API ecosystem.



Through key security functions of an API gateway, the API threat exposure is reduced and mitigated to allow a proper adherence to GoC API development guidelines & GoC API security best practices[1]. An API Gateway is the key enabler to ensure proper exposure of ESDC API services to external or internal partners.

API Developers

Another main advantage of a gateway is the removal of many burdens from the developers. Security is applicable at the enterprise level instead of being the responsibility of the developer. Discovery is also made a lot easier since a single catalogue is available which minimizes the potential of duplication of capability. Administrators can set global policies at many levels which developers no longer need to worry about. Metrics and monitoring are also done at the Gateway level, thus centralizing those key capabilities making it easier for reporting or incident post-mortems. This strategic direction is supported by the GC Architecture Standards directive on Information Architecture and Application Architecture[2]

[1] Section 5. Secure the API

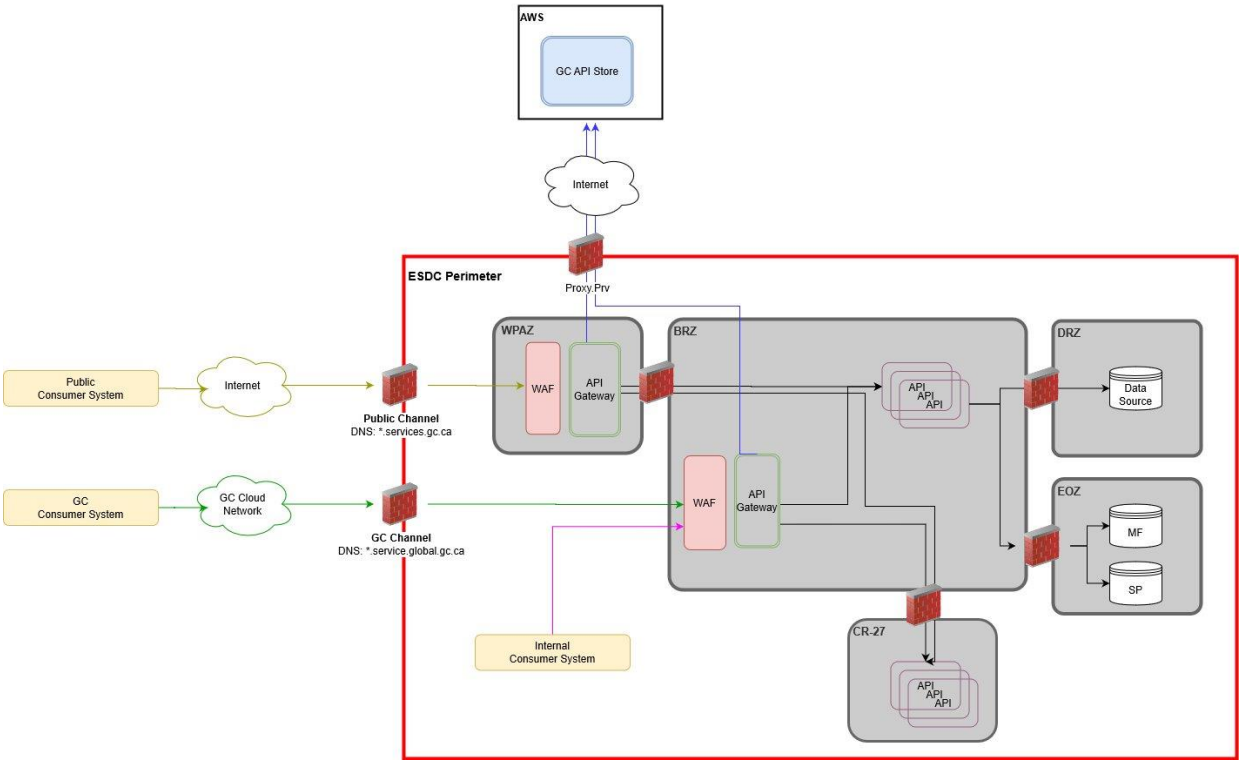
- https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html
- https://wiki.gccollab.ca/Government_of_Canada_Architectural_Standards

[2] Information Architecture and Application Architecture

- https://wiki.gccollab.ca/Government_of_Canada_Architectural_Standards

API Hosting Architecture

Network Architecture



Areas to note:

- each zone has its own gateway to allow management and access to the exposed service

API Gateway Solution

Google Cloud (Apigee) cited as a leader in the 2019 Gartner Magic Quadrant for Full Life Cycle API Management

Gartner positions Google (Apigee) overall highest for its ability to execute. This is the fourth time in a row that Google (Apigee) has been named a Leader

Figure 1. Magic Quadrant for Full Life Cycle API Management

Source: Gartner (October 2019)

Systems of engagement would be required so ESDC can safely expose and share their digital assets across the enterprise to drive efficiency, to better connect with partners and consumers, and to thereby create an API economy for future revenue growth. Apigee's Intelligent API Platform will provide ESDC with the ability to quickly adapt to changing regulations and market conditions. Apigee have helped over 800 customers, across multiple industries adapt to changing business requirements.

Apigee Capabilities that target ESDC's technology gaps.

- Scale : Support for massive call volumes– concurrency, peaks, spikes, auto/rapid provisioning, analytics-driven devops with Apigee running at providing 99.9999 availability
- Performance: Raw horsepower in API processing pipeline; policy engine that collapses development from days and weeks to seconds. Network-routing style latency. Programmable caching at the edge distributed close to consumers.
- Multi Data Center Support: Apigee offers deployment choices namely SaaS, Hybrid and On-prem. that can align with unifying technology access across legacy and End-state data centers.
- Governance: WIth Apigee hybrid, ESDC can manage and control the runtime, enabling ESDC to leverage the existing compliance, governance, and security infrastructure.

- Proven technology: Hundreds of major customers in a fully multi-tenant platform, Thousands of proxies, Tens of Thousands of policies, 50K+ API RPS (requests/sec) peaks, ~1B+ API transactions/day (in Apigee public cloud solution alone)
- Global Replication: sync seamlessly in a multi-DC, multi-Cloud, multi-geo Distributed Network – critical for Scale and Performance. No DR needed, no Downtime
- Easy to do sophisticated API processing you used to have to code: extensible, pre-developed policies for most critical API processing needs
- Polyglot extensibility – Use Java, Node, Python or JavaScript
- Sophisticated Integrated Real-Time Analytics: Out Of The Box for API developers, API consumers, Operations and Business – fully customizable
- Advanced Security: Comprehensive, in-depth, full-lifecycle, narrowed risk profile, predictive bot-detection and protection (public cloud today). Highly scalable key and token management. Regular compliance and pen testing.
- Management API for streamlining DevOps.
- Zero Downtime Deployment: fits in with ANY SDLC, no service interruptions
- Open & Full Featured Developer Portal - full access to html, css, javascript UI/UX. Built in Developer Analytics, Lifecycle management, integrated monetization, full globally distributed key and token management, and much more
- Full-featured Monetization module: every API monetization use-case available, flexibly configurable, and easily integrated to billing systems.
- APIs everywhere: Apigee is built API-first on a modern (not 20 year old) architectural pattern. That's why Cloud Foundry phase-1 integration only took a few weeks. Apigee Microgateway allows for distributed, secure, at scale API processing with centralized control.
- Microservices Management and Istio - Through native integrations with Istio, Apigee is the only API platform that provides common visibility and management across both APIs and microservices for organizations. It is important to note that despite all these advantages, we still believe there is no substitute for hands on use of the Apigee Edge API Platform. It is in that mode that ESDC developers will experience the ease of use, visibility, API-consumption orientation of the platform, which will fundamentally drive the success of API-first efforts going forward.

Key area's Apigee can help ESDC succeed, are the following:

API Management

API Management enables the transformation of existing backend services to APIs with over 30 policies designed for configure rather than code deployment, which simplifies customer self-service and reduces time-to-value.

Security

In the world of accelerated digitization, the IT mandate is still to provide secure access to services while protecting customers and the business from threats, back-end overload, and service issues.

Edge provides a unified security infrastructure that ensures optimized performance, reduced latency, and enterprise-grade security.

API Programmability

API Services can be extended using a choice of options, including support for JavaScript, Java, Python. There is also the ability to deploy custom proxies developed in node.js, and enhance them with Apigee API management features, such as OAuth security and traffic management, using Apigee configuration capabilities.

Developer Services

Apigee Edge Developer Services provides the tools and infrastructure needed to drive your developer and partner success. Internal and external app developers and partners represent brand new channels. The greater the success of the developer's product - the app - the more likely is the success of your digital strategy.

Empowering Developers

Edge Developer Services enables you to create an onboarding and community experience that empowers developers, streamlines their adoption and supports them in a successful development experience.

Analytics Services

Edge Analytics Services delivers the analytics tools and infrastructure that provides end-to-end visibility across the entire digital value chain. With Edge Analytics, enterprises can make data-driven decisions to grow the reach and revenue of your digital program, increase customer engagement, and accelerate digital transformation. In addition, Edge Analytics provides unmatched flexibility to meet changing business and analytics needs

In Closing

As demonstrated in this document, to help onboard ESDC to industry standards and best practices, and enable and empower ESDC to share information with partners, a API Gateway is the technology gap that needs to be adjusted, in order to participate in TBS's exciting Open Government, and mandatory architectural design practices.

Apigee is uniquely positioned to address all of these requirements and enable ESDC to unleash the talent and creativity of their development team to build hundreds of new services with ease.

Apigee has many unique features and operational aspects as an all purpose-built API Management Platform, designed to address your challenges of building a world-class API programs, by an assortment of capabilities. <see appendix>

A Apigee hybrid model would resolve many of the cloud to ground connectivity issues, by introducing a division of control and access by allowing parts of Apigee solution to be maintained and managed in the cloud, and synchronising with Apigee clients installed in on prem environments.

Other solutions were investigated such as Mulesoft, 3Scale Red Hat and IBM Data Power. None of these solutions were as mature as Apigee. Security capability from 3Scale is inexistent and limited with Mulesoft solutions. IBM Data Power is outdated solution that does not provide level of flexibility that we are looking for to ensure interoperability with Government of Canada API Store. Finally, Apigee is the only solution providing a SAS solution with capability to fully integrate with SSC EDC and Legacy data center which are critical for the success of this initiative.

Apendix

Section: Appendix C - Mandatory Procedures for Enterprise Architecture Assessment

- https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249&section=procedure&p=C

Digital Operations Strategy Plan 2018-2022

- https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html

Government of Canada Standards on APIs

Section 5. Secure the API

- https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html

Reference Document - ESDC Apigee Proposal.PDF / Submitted March 25, 2020
Title: ESDC - Full Life Cycle API Management Platform Apigee Proposal

OWASP Top 10 Vulnerabilities

Top 10 Web vulnerabilities	Top 10 API vulnerabilities
Injection	Broken Object Level Authorization
Broken Authentication	Broken User Authentication
Sensitive Data Exposure	Excessive Data Exposure
XML External Entities (XXE)	Lack of Resources & Rate Limiting
Broken Access Control	Broken Function Level Authorization
Security Misconfiguration.	Mass Assignment
Cross-Site Scripting XSS	Security Misconfiguration
Insecure Deserialization	Injection
Using Components with Known Vulnerabilities.	Improper Assets Management
Insufficient Logging & Monitoring	Insufficient Logging & Monitoring