**Image for the blog background:**

TODO

**Title:**

How to automatically validate the configuration of your API Gateway

**Abstract:**

Deploying an API Gateway is a critical operation in an Information System or regarding the exposure of API to customers. Let us deep dive in approach to automatically validate that the configuration of the exposed API stay secure across its evolution….

**GitHub repository associated that will moved to public when blog post will be released:**

<https://github.com/ExcelliumSA/APIGateway-Study>

**SEO rules indicated by Mathilde:**

* Paragraphs with less than 300 words.
* Keyword used as much as possible: Here test, api, gateway
* Presence of sections.

# API everywhere…

Today, it is common for a software, companies, etc. to provide a web API to expose data to their customers or partners [1]. The objective is to facilitate the integration and create new business opportunities. For example, for bank, API was a way to provide more services to their customers through mobile application. Do you remember the last time you needed to contact your bank directly?

# The era of API Gateways

With the increase of API created, companies needed to find a way to “*easily*” manage different aspect of the API like exposure, monetization, access control, documentation, versioning, aggregate services etc.

Therefore, API Gateway [2] were born to achieve these goals. Even if the objective of this post is not to describe “*what an API Gateway is?*” but rather, “*How to test its configuration?*” Let us see what is its role in an API context.

The goal of the API Gateway is to be a central access point for any call to an API offered to client apps. Therefore, to be effective, **all call to API must be routed, without exception, to it**. In this way, Backend API (internal API performing the real business processing) can delegate several aspects to the API Gateway like authentication, authorization, rate limiting, alter the requests/responses, etc.

# Overview of the communication flow

The schema below show an overview of the flow involved during the call of an API from a client application. A “*policy*”, refer to a set of processing/validation rules applied on a request or a response.

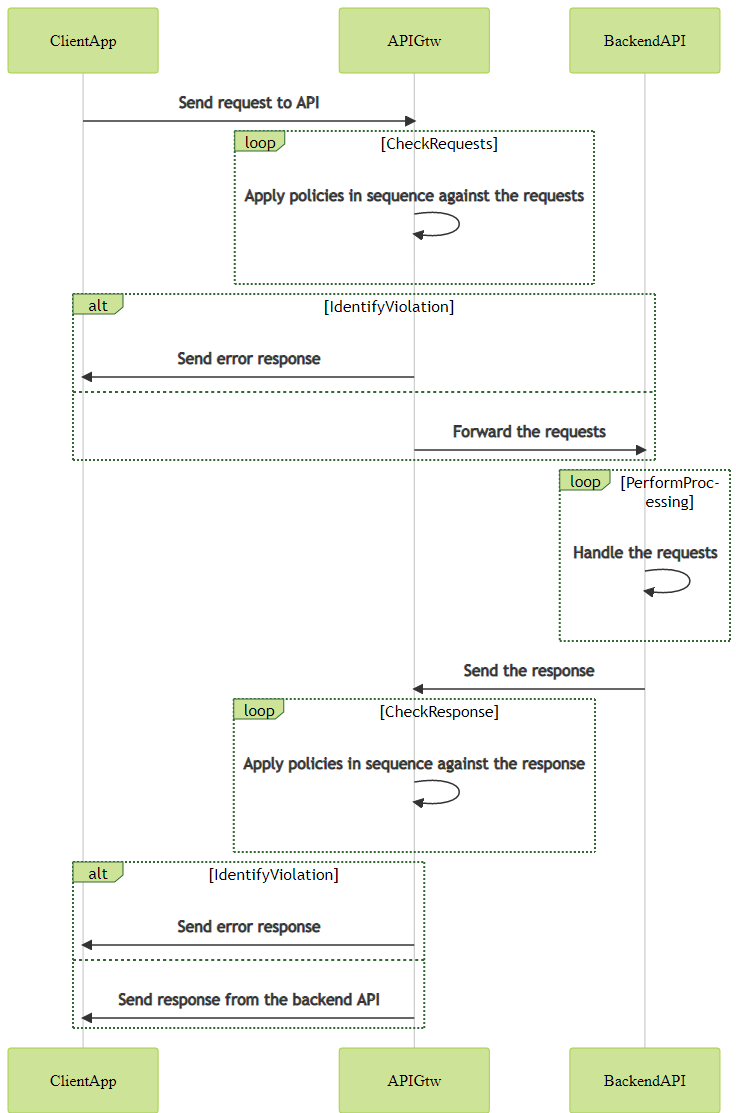


Figure 1: Image file Figure01

# You should not (by)pass!

When an API Gateway is deployed to handle access to a backend API, it is important to ensure that only the API Gateway is allowed to call the backend API. The following kind of alternate path must be avoided:

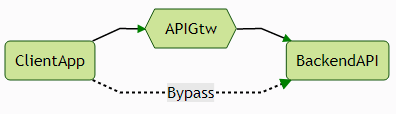


Figure 2: Image file Figure02

The path in dotted line represents a call channel that bypass all the protection and restriction applied by the API Gateway. To restrict backend API call to the API Gateway, the following measure, among other, can be leveraged:

* Mutual TLS authentication between the API Gateway and the Backend API.
* Network segregation alongside specific firewall.
* Etc.

Depending on the API Gateway software, depending on the software, different kind of built-in measure are supported out of the box.

# The challenge

Even if an API Gateway help to manage the exposure of API, with the time, it will contains a significant number of API definition including different version of the same API. The more API definition an API Gateway contains, the more is difficult to ensure that each configuration stay secure across the different iteration of its configuration.

The common pattern meet is the “*Configure, test and forget*”. Precisely, a API is configured in the API Gateway, the configuration is validated by a configuration or an intrusion test against the API and then the API live his life until someone notice a problem or an incident happen…

# Automation to rule them all

In software development, a kind of test named “Integration testing” [3] is performed “*to evaluate the compliance of a system or component with specified functional requirements.*”

The idea will be to apply the same kind of test on an API definition, in an automated way, in order to constantly ensure that it stay secure. To achieve this objective, it will be great if mainly:

1. The test can be described, without needed to code something, like a cooking recipe.
2. The test recipe can define assertion on results.
3. The test syntax can be easy to read.
4. The test can generated report that can be integration in popular CI/CD platform [4].
5. The test description file support versioning.
6. The test tool can be cross-platform and require no or minimal installation.
7. The test tool can be free, open source, maintained and well documented ☺

The test flow for an API definitions will be the following:

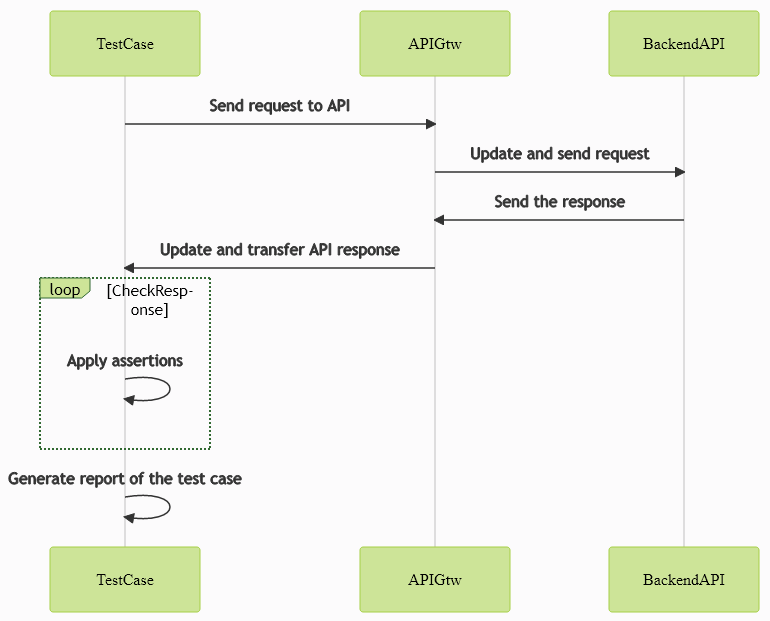


Figure 2: Image file Figure03

For this purpose, the tool named **Venom** [5] was chosen because it fulfill mostly of the criteria mentioned above.

Below is an example of test case description (more on this later) – No code needed:

|  |
| --- |
| **# The test case is named *Strict-Transport-Security* because**  **# it check the presence of this security HTTP response header**  - name: Strict-Transport-Security  steps:  **# We want to perform an HTTP request**  - type: http  **# The request is a GET**  method: GET  **# To the URL referenced by the variable *target\_site***  url: {{.target\_site}}  **# As we will only check the headers then body is not**  **# important and can be skipped**  skip\_body: true  **# We allow 20 seconds to the requests to finish**  timeout: 20  **# We define a list of assertions**  assertions:  - result.statuscode ShouldEqual 200  - result.headers.strict-transport-security ShouldNotBeNil  - result.headers.strict-transport-security ShouldContainSubstring "includeSubDomains" |

# The global lab

To confirm that the idea is viable or not, a lab based on the following technical components was created:

* API Gateway: **Apiman** from Red Hat (free and open source) [6].
* Test tool: **Venom** from OVH (free and open source) [5].
* Provisioning & infrastructure: **Docker** and **Docker Compose** (free and open source) [7].

# The lab API definitions

Two API were defined in the API Gateway used for the lab:

1. One using the API from <https://requestbin.net/>, as backend API – named **public**:
   * RequestBin gives you a URL that will collect requests made to it and let you inspect them in a human-friendly way.
   * This API is public and it is **not** published through a “*Plan*”.
   * Policies applied via built-in-plugins: [8]
     1. **CORS**: Only allow origins **https://localhost:8443**, **http://localhost:8080** and apply cache of 10 seconds.[9]
     2. **HTTP Security**: Enable **Content-Security-Policy** / **X-Frame-Options** / **X-Content-Type-Options** headers. Disable **HSTS** (local POC) / **X-XSS-Protection** headers. [10]
     3. **Simple Header**: Remove following headers from backend API response: **cf-request-id**, **Report-To**, **Server**, **CF-RAY**, **NEL**, **CF-Cache-Status**.
2. One using the API from <http://jsonplaceholder.typicode.com/>, as backend API – named **published**:
   * Free fake API for testing and prototyping.
   * This API is not public and it is published through a “*Plan*”.
   * Policies applied via built-in-plugins:
     1. **IP Whitelist**: Only allow requests from **127.\*.\*.\*** and **172.\*.\*.\***
     2. **Rate Limiting**: Only allow 10 requests by minute by client app.
     3. **Basic Authentication**: Require basic authentication from users defined statically and forward the login to the backend API in header **X-User**.

🛈 Explanation about the notion of “Plan” in apiman – Extract of the documentation [11]:

“*In apiman, a Plan is a set policies that together define the level of service that apiman provides for an API. Plans enable apiman users to define multiple different levels of service for their APIs.”*

🛈 Explanation of the different between a Public API and “Plan based” API [12]:

“*Public APIs are also very flexible in that they can be updated without being re-published. Unlike APIs published through Plans,* ***Public API can be accessed by a client app without requiring API consumers to agree to any terms and conditions related to a contract defined in a plan for the API****…”*

“*Publishing an API through Plans -* ***In contrast to Public APIs, these APIs, once published, must be accessed by a Client App via its API key****. In order to gain access to an API, the Client App must create a contract with an API through one of the API’s configured Plans…”*

# The lab API test plans

TODO

# References

1. <https://blog.postman.com/api-growth-rate/>
2. <https://www.redhat.com/en/topics/api/what-does-an-api-gateway-do>
3. <https://en.wikipedia.org/wiki/Integration_testing>
4. <https://www.atlassian.com/continuous-delivery/principles/continuous-integration-vs-delivery-vs-deployment>
5. <https://github.com/ovh/venom>
6. <https://www.apiman.io/latest/crash-course.html>
7. <https://docs.docker.com/get-docker/>
8. <https://www.apiman.io/latest/crash-course.html#_managing_policies_and_plugins>
9. <https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS>
10. <https://owasp.org/www-project-secure-headers/>
11. <https://www.apiman.io/latest/crash-course.html#_the_apiman_data_model>
12. <https://www.apiman.io/latest/crash-course.html#_publishing_apis>