An API Gateway— the Secret Sauce to Prevent Under-protected APIs

Report

By Darryn Graham

Application Programming Interfaces (APIs) are a common approach for public sector engagement but when APIs are left under-protected, agencies leave themselves vulnerable to attack. The risk is so heightened that the Open Web Application Security Project (OWASP) added Underprotected APIs to its OWASP Top 10 2017. But by adopting an API gateway with a few special security considerations, risk can be greatly reduced.

Because systems of record, upon which APIs are exposed, typically reside within an agency's trusted network, additional considerations need to be made to expose them for consumption from outside of the trusted network in order to avoid security risks. Organizations can mitigate many of these security risks by using an API gateway to facilitate these requests. An API gateway acts as a specialized proxy server that controls the requested traffic, detects and defends against distributed denial-of-service attacks, and leverages existing investments in malware/antivirus scanners.

Darryn Graham is chief architect at Software AG Government Solutions, which helps agencies integrate and enhance the speed and scalability of their IT systems.

Here are seven key best practices to consider when designing a secure architecture needed to implement a trusted API gateway.

1. Control requests into the Agency's Trusted Network (ATN)

The API gateway should not permit connections directly into the ATN that originate from the network's Demilitarized Zone (DMZ). Instead, an internal gateway component in the ATN should connect outward to the API gateway in a tunneled fashion. This approach removes the need to open incoming firewall ports from the DMZ into the ATN, preventing any connections from servers in the DMZ should they become compromised. Additionally, connections from the ATN to the API gateway should be persistent, so that encryption handshakes are not continually re-established, which can negatively impact performance.

2. Establish filtering rules and alerts

The API gateway should be configurable to actively filter requests based on agency security and operating policies. Filters should include the ability to block specific IP address ranges and act dynamically based on request type, endpoint name, request payload size and authentication. Automated alerts should be sent to system administrators and management dashboards when requests violate filter rules.

3. Implement protective caching

Depending on the data and use case, the API gateway should be employed to store and serve frequently accessed data directly from caches of Random Access Memory (RAM). This provides a high-performance buffering layer that can insulate the internal endpoint from spikes in volume. In addition to protecting the internal endpoint, this technique increases API service performance, facilitates scalability, and decreases internal network traffic. For example, a weather API might only deliver updated data every five minutes, but during a hurricane the API might be inundated with concurrent requests. In this use case, protective caching could provide an extremely affordable scaling mechanism that helps the data provider avoid sizing their architecture to handle the often-unpredictable spikes in utilization.

4. Operationalize cyber threat information

The API gateway itself should provide flexible administrative APIs to allow for fast, automated and scripted configuration. With a dynamically configurable API gateway, agencies will be able to quickly operationalize actionable threat indicators from the National Cybersecurity and Communications Integration Center (NCCIC). Additionally, certain rule violations or alerts triggered on the agency's API gateway may reveal threats that should be shared with the cyber-community through the Department of Homeland Security's Automated Indicator Sharing (AIS) service.

5. Use identity and access management

The API gateway should provide a robust "Identify & Authenticate Consumer" policy action to effectively identify and validate clients, with the ability to support a wide variety of identification and authorization options. This allows your agency flexibility to identify clients who are trying to access the APIs. At a minimum, the gateway's supported identification options should include: Hostname Address, API Key, IP Address Change, SSL Certificate, OAuth2 Token, XPath Expression, WSS Username Token and WSS X.509 Certificate.

6. Use payload threat protection

Another important factor is how the API gateway should block attacks coming through JSONTM or XML in string lengths and payloads by several ways, including:

- Maximum number of entries allowed in an object
- Maximum string length allowed for a property name within an object
- Maximum number of elements allowed in an array

And limit XML attributes, such as:

- Maximum number of characters permitted in the namespace prefix
- Character limit for any namespace URIs present in the XML document
- Maximum number of child elements allowed for any element
- Maximum node depth allowed in the XML

7. Apply SQL injection filtering

The API gateway should include the ability to block SQL query requests based on custom blacklisted items. A blacklist could include such items as invalid special characters. The ability to dynamically configure rules gives an agency maximum flexibility to adjust as new threats are identified.

In closing, employing an API gateway and following these steps is a proactive way for agencies to address specific security challenges. This is essential when agency data and applications require open, public access. Although no security solution is ever complete, given the growing and changing threat environment, agencies must deploy the latest security techniques to reduce their risk profile. An API that fails to deliver the expected level of security, reliability and performance can have tremendous mission impacts—to both the organization producing it and those consuming it.

ABOUT SOFTWARE AG GOVERNMENT SOLUTIONS

Software AG Government Solutions is a market leader in best-in-class commercial software dedicated to serving the U.S. Public Sector and A&D supplier community. Our solutions remove the barriers of connecting data from every source – from cloud to edge – across an extended enterprise. We are recognized by Gartner and Forrester as leaders in API Management and Hybrid Integration (webMethods), Industrial IoT (IIOT) platforms (Cumulocity), and IT Portfolio Management and Enterprise Architecture (Alfabet). Widely embraced by our customers, we leverage a "Prove IT First and Prove IT Fast" approach to solving critical IT challenges. This approach has proven to minimize risks associated with IT investments while allowing us to prioritize building trusted relationships with our customers.

software AG
GOVERNMENT SOLUTIONS