



- + Reliability
- + Compliance
- + Traceability
- + Integration

## 8 REASONS TO CHOOSE DENYALL WEB SERVICES FIREWALL

1. **Time-tested security**, effective against known and unknown attacks
2. **Graphical, logical approach** to model the business process as a security policy
3. Integration with any WS-Security environments, providing validation, encryption and decryption
4. Seamless integration in machine to machine (M2M) communications achieving web service security and validation
5. The ability to profile web services, learn how they work and build a whitelist
6. XML and JSON request & response content transformation
7. Web Services Routing
8. Can be deployed as an API Gateway

## ENSURING YOUR WEB SERVICES ARE SAFE AND SOUND

With cloud and mobile computing on the rise, **APIs, XML and JSON traffic are at the heart of modern IT.**

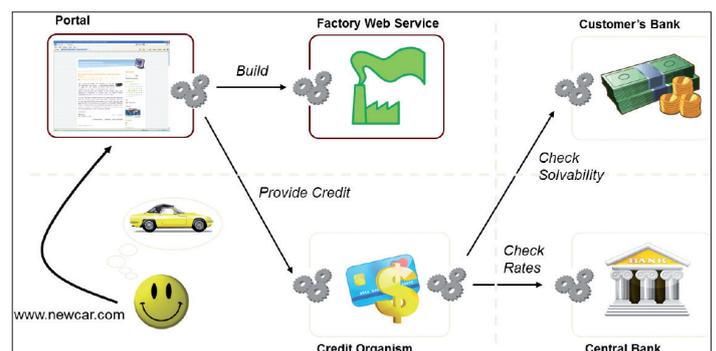
Web Services and automated machine-to-machine communications support processes which are often business critical, be they internal only or also involving external members, such as suppliers, consumers and regulatory bodies.

When it comes to Web Services security, a simple schema validation is, by far, not enough.

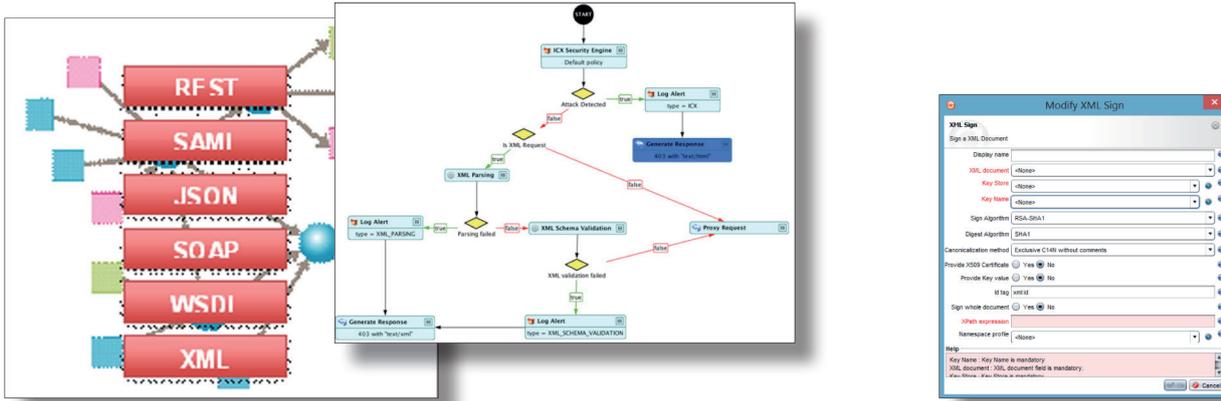
If you really depend on your Web Services, you need to:

- **Protect** application servers against malformed messages, thus guaranteeing the compliance of the SOAP/XML flow, REST full JSON API,
- **Prevent** Denial of Service (DoS) attacks,
- **Anticipate** traffic overload,
- **Guarantee** service availability,

DenyAll Web Services Firewall makes it easy to optimize and secure these XML and JSON-based data flows, with capabilities found in no other WAF, SOA/API Gateway.



*A web services exemple*



## KEY FEATURES

### Administration

- Visual policy & traffic control with an intuitive, powerful workflow approach.
- Web Services discovery and profiling.
- Central provisioning, monitoring and reporting on multiple devices.
- Log replay for policy testing and forensic analysis.
- Virtual patching: integration with DenyAll Vulnerability Manager.

### Platform

- Deployment on physical and/or virtual appliances.
- Reverse proxy clustering and load balancing to ensure high availability and redundancy.
- Secure HTTP traffic with DenyAll Web Application Firewall.
- Add Single Sign on capabilities with DenyAll Web Access Manager.

### Web Service Security

- XML/JSON parsing and scheme validation for DTD, WSDL, XSD, WADL.
- REST profiling and security using JSON or XML/JSON formats
- Integration in any WS-Security environment.
- Ability to encrypt and decrypt parts of the content.
- SAML authentication integration as a Service Provider (SP).
- Can also act as the Identity Provider (IDP) at the same time or be integrated with any other IDP.
- Extensive XPath injection protection filters.
- JSON and JWT parsing.
- Schema validation with JSON schema.

### API Gateway

- Thanks to its flexible workflow and content rewriting and routing capabilities, WSF can easily replace an API gateway.

## ABOUT DENYALL

DenyAll is a software vendor, expert in application security. For 15 years, we have been helping demanding customers secure their web applications and services. Our products detect IT vulnerabilities, protect infrastructures against modern attacks targeting the application layer and connect users to the applications which allows them to create and share information. In 2017, DenyAll was acquired by Rohde & Schwarz Cybersecurity.

🏠 6 avenue de la Cristallerie 92310 Sèvres - FRANCE

☎ +33 (0)1 46 20 96 00  
📠 +33 (0)1 46 20 96 02

✉ info@denyall.com  
@ www.denyall.com