Press release
Paris, October 5, 2011

With rXML 4.0 – a Web Services Firewall – Deny All adjusts its offering to the needs of the market

Securing service oriented architectures (SOA) is a significant challenge. Deny All, the European web application firewall (WAF) market leader, innovates with the launch of rXML, a solution dedicated to the protection of web services. Based on proven, innovative technologies, this product blocks application-layer attacks and secures all XML/SOAP transactions between the actors of a Web Service, thus preventing denial of service attacks and sensitive data theft.

rXML, a firewall dedicated to securing Web Services

Web Services-based architectures are commonly used by enterprises and governments to enable new applications, leveraging distributed data sources. Because of the nature of the communication mechanisms that characterizes them, Web Services require a specific approach to security.

Deny All has been securing and accelerating Web Services for years with the XML option of its flagship product, rWeb. **In order to adjust its offering to the changing needs of the market,** Deny All now proposes rXML, **a product 100% focused on securing Web Services.** The product is built on the same platform as its other web application firewalls, rWeb and sProxy. It takes advantage of **Deny All's platform features** in the area of acceleration, Web security (black list, scoring list), high availability and centralized management features.

In addition, it offers a number of specific features which are required to effectively protect SOA applications from modern attacks:

- **Data model validation:** data transmitted by Web Services participants is verified and modified to comply with XML data models (WSDL, XSD, DTD). Additional rules can be specified ;
- **XML validation and transformation:** to avoid data leakage, requests are canonized, error messages removed, sensitive data replaced and complexity verified (including document maximum size and tree maximum depth) ;
- **Black list:** signatures specific to XML attacks (xPath injections, DoS, etc) combined with generic http filters ensure an excellent level of protection against attacks targeting Web Services ;
- **Stateful:** XML element tracking prevents data alteration, be it involuntarily by a legitimate user, or during transmission as a result of an attacker's actions ;
- **SOAP attachments:** they can be authorized or not, a maximal size can be defined, text attachments will be analyzed by the XML Black List and generic http filter, as well as a third party anti-virus engine, thanks to the support of the ICAP protocol ;
- **Access control lists:** they enable granular access control to the functions of the various actors of a Web Service, can limit UDDI access to registry services based on the source's IP address or accessed functions.

A unique, differentiated solution

These features, which make rXML a unique product, translate into the following competitive advantages:

- **rXML can be deployed effortlessly and quickly, without impacting the SOA architecture,** it requires no changes to the application nor does it require a learning phase.
- **rXML is a true web application firewall,** protecting against attacks specifically targeting Web Services, but also against any **known or unknown Web application layer attack.**
- **rXML enables application scalability thanks to its active-active high availability mechanism.** Several rXML devices can run in parallel in order to ensure the continuity of your applications' security, including in case of a failure.
- **rXML offers unique evolution possibilities:** to meet the most demanding security needs, a simple license key will let you upgrade and take advantage of rWeb's advanced Web security features, including the White List, User Behavioral Tracking module and the Client Sanitization option.

With the introduction of rXML, Deny All demonstrates its ability to adjust to the evolving needs of enterprise and SMB customers. Any organization needing to secure both its legacy and modern applications will find a solution within Deny All's portfolio, which now includes three firewalls based on the same platform:

- **sProxy**, the plug and play WAF, especially adjusted to the needs of SMBs,
- **rWeb**, the next generation WAF, capable of securing the most critical applications,
- **rXML**, dedicated to securing Web Services-based SOA applications.

About Deny All

Deny All is the European leader in the Web Application Firewall (WAF) market. Our reverse proxy-based solutions secure and accelerate 30 000+ Web applications, XML/SOAP Web Services and FTP servers globally. Available as software or appliances, they provide a superior level of protection against known and unknown attacks, ensure application availability and simplify user authentication for customer-facing, transactional, extranet and intranet applications and Service Oriented Architectures. Deny All's flagship products are rWeb, a fully functional WAF, its XML Firewall option and sProxy, an entry-level solution. The offering also includes an application vulnerability scanning service, Edge, and a solution designed for securing FTP connections, rFTP.

Founded in 2001 and headquartered in Paris, France, the company has local teams in Germany, Spain and the Nordics and value-added partners across the globe. Deny All serves enterprises, SME's, outsourcers and cloud providers around the world, Our customers include large financial institutions, state and local governments, industry and services companies, media and e-commerce leaders.

Press contacts
Stéphane de Saint Albin +33 1 46 20 96 21 sdesaintalbin@denyall.com **www.denyall.com**