Secure your information flow

Organizations have to ensure interoperability among their applications to facilitate information sharing, data analysis and new market conquest. From this perspective the Web Services infrastructure is of prime importance. It lies at the core of information system interconnections and of migrations towards cloud computing. New means of protection are necessary to provide continuous interactions and secure, reliable Web Services exchanges, whether these address partners or the internal applications of a company.

The Web Services Firewall detects and intercepts any malicious content that is proper to Web Services. SOAP/XML or RESTful messages are deciphered, deep inspected and measured against access and filtering policy.

Assure service continuity

During application-to-application dialogues, the quality and reliability of information exchanged are paramount. The Web Services Firewall makes it possible to protect your application servers from receiving ill-formed messages and from traffic overload.

Instead of the denial of service that usually results from this kind of incident, your partners can expect reliable and ongoing service. Administrators receive qualified incident alerts as well as all the elements that enable them to determine the source of an issue.

Apart from protecting your applications, the Web Services Firewall can also be used to ensure that messages you transmit conform to standards, so that no unforeseeable occurrence (bug, network overload) disrupts the use of Web Services by your partners.

Regardless of whether Web Services are local, remote or hosted, the Web Services Firewall fulfils the requirements for protection, compliance and access management of Web Services. Message time-stamping and real-time performance assessment also make the Web Services Firewall an essential tool for information system governance.

About Bee Ware:

Bee Ware is a pioneering provider of secure web enabled delivery solutions. Bee Ware’s appliance-based products ensure security, high performance and business continuity for the world’s most demanding organizations.
i-Suite’s graphical interface displays all the parameters an administrator needs to watch. Truly ergonomic and user-friendly, it represents ongoing feedback from our customers over many years.

i-Suite generates graphical reports intended for technical and/or management perusal. They provide a rapid and synthetic view of the activity on protected servers.

i-Suite incorporates a wide range of enhanced complementary features (advanced log rotation, automated management of CRLs, conversion of SSL certificates, multi-user management console, Selective Back up & Restore ….) as well as an Application Delivery Controller that includes Load Balancing, Content Caching, Compression, Traffic Rewriting and other functions.

Following the lead of all Bee Ware products, the Web Services Firewall is based on a common platform, and makes use of administration and operational tools and the graphical interface that are common to all the other products in the range:

1. Adoption of security standards:
   Integrating security within the development environment of Web Services helps to save publication time. R&D and Production also share the same security speak.

2. Protection and routing:
   Web Services that address the enterprise or the Internet require deep message inspection due to the diversity and potential risk factor of the technologies that come into play. Different standards (XML, RESTful, JSON, etc.) need to be supported for application inspection and routing.

3. Quality of service:
   Messages addressing partners are checked by the XML firewall, in order to ensure that formats and frequency do not disrupt a partner’s Web Service.

4. Service Continuity:
   The XML firewall ensures the availability of Web Services for partners, making certain that an isolated production hitch (bug, accidental overload) does not interfere with the rest of the service.