



Highlights

- Improve management with intelligent workload balancing and dynamic control of service levels
 - Support compliance with robust data protection and auditing capabilities
 - Mitigate risks with DMZ-grade security for mission-critical applications, services and data
 - Increase trust in existing services with highly secure hardware for run-time governance and policy enforcement
 - Control access to applications, services and data based on customizable roles and rights
-

IBM WebSphere DataPower XML Security Gateway XS40

Enforce policies and secure services, applications and data with customizable, scalable and automated service visibility and governance

Today's dynamic business environments require organizations to work smarter to remain competitive and respond to changing customer demands. In order to achieve these goals, organizations need to eliminate costly redundancies, promote reuse of existing services and make sure these services are secure, reliable and of high quality. IBM WebSphere® DataPower® SOA Appliances offer customizable, scalable and automated service visibility and governance solutions enabling enterprises to better manage, trust and secure their services, applications and data. By consolidating their service-oriented architecture (SOA) security and governance in a centralized, purpose-built appliance, organizations can rapidly bring new services to the market, reduce business application risk, increase staff productivity, and lower maintenance costs while maximizing return on their assets.

Why an appliance for service visibility, governance and security?

With an increasing number of SOA applications using services offered by external entities, it is vital that companies provide secure SOA services that are scalable and cost-effective without sacrificing performance. The award-winning IBM WebSphere DataPower XML Security Gateway XS40 (Figure 1) is a complete, purpose-built hardware platform for delivering highly manageable, more-secure and scalable SOA solutions. As a hardened SOA appliance, WebSphere DataPower XML



Security Gateway XS40 offers an advanced XML threat-reduction and security-enforcement layer for XML messages and Web services transactions. It meets the demand for fast, reliable XML processing in a consumable appliance that transforms back-end disparate message formats to XML while applying message-level security and service policies. WebSphere DataPower XML Security Gateway XS40 streamlines your SOA deployment in a security-rich environment, requiring minimal configuration, customization and management. The device helps protect SOA traffic by implementing XML threat-protection and Web-services security functions, as well as integrating with security and identity management software, such as IBM Tivoli® software.



Figure 1 - WebSphere DataPower XML Security Gateway XS40

WebSphere DataPower XML Security Gateway XS40 is a 1U (1.75-inch) rack-mountable network device designed to fit into industry-standard racks. Attachment to the network is through Ethernet. The device is virtually tamper proof and cannot be taken apart and deployed within other servers. You

gain business value without having to change your network or application software. As a result, proprietary schemas, coding or application programming interfaces (APIs) are not required to install or manage the device. Because of its versatility and ease of deployment, the appliance form factor of WebSphere DataPower XML Security Gateway XS40 is a cornerstone of a resilient infrastructure. It appeals to a variety of groups with stakes in successful SOA deployment, such as enterprise architects, network operations, security operations, identity management and Web-services developers.

Improve management with intelligent workload balancing

In today's distributed application environments, which increasingly cross ecosystems between enterprises and their customers, partners and suppliers, business success requires moment-by-moment feedback from and management of resources. Incoming network traffic needs to map to the most appropriate resource available. IBM WebSphere DataPower Appliances' Option for Application Optimization (AO) is designed to provide dynamic, intelligent load-balancing functions for today's most demanding environments, improving efficiency and minimizing critical outages. By evenly distributing workloads across appliances and onward to load-selected servers, AO enhances uptime, user visible responsiveness, and resource usage (Figure 2).

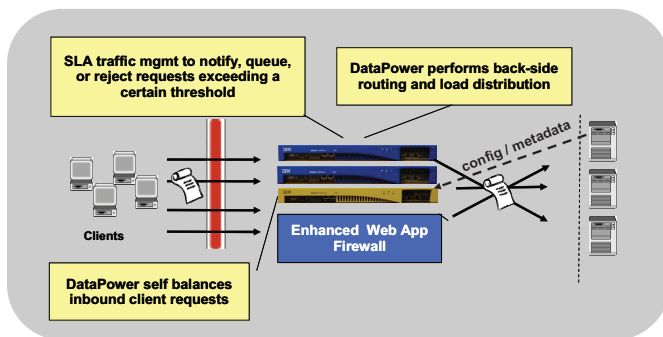


Figure 2 - Option for Application Optimization includes self-balancing across appliances and intelligent load distribution to back-end environments.

With support for Web Services Distributed Management (WSDM), Universal Description, Discovery, and Integration (UDDI), Web Services Description Language (WSDL), Dynamic Discovery, and Service Level Management (SLM) configurations, the XS40 offers a native Web services management framework for the efficient management of distributed Web service endpoints and proxies in heterogeneous SOA environments. The XS40 also offers SLM alerts, logging, and pull-and-enforce policies, which help enable broad integration with third-party management systems and unified dashboards, in addition to support and enforcement for governance frameworks and policies. When combined with its AO capabilities, the XS40's message routing, service level management, content inspection and security features provide another avenue to reducing complexity in the IT environment, while simultaneously improving service.

Support compliance with robust data protection and auditing capabilities

The XS40's powerful Authentication, Authorization, and Auditing (AAA) Framework allows the device to use a broad variety of methods for extracting user passwords, security tokens and other identity information from incoming

requests. Authentication and authorization steps are also fully modular and can be based on either on-board or off-board repositories, and the Audit & Accounting processing is fully extensible. This unique framework enables the XS40 to integrate with a wide variety of identity management solutions, as well as allowing customers to integrate proprietary, in-house Single Sign On (SSO) systems with their Web services security architecture. The XS40 also selectively shares information through encryption and decryption and signing and verification of entire messages or of individual XML fields. These granular and conditional security policies can be based on nearly any variable, including content, IP address, host name and other user-defined filters. These are among many of the XS40's robust data protection, policy enforcement, and auditing capabilities that help organizations around the world achieve and maintain compliance with such industry and/or regulatory requirements as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

Mitigate risks with DMZ-grade security for mission-critical applications

As a hardware device that delivers advanced XML and Web services access controls without complex configuration or custom code, the WebSphere DataPower XML Security Gateway XS40 offers the higher levels of security-assurance certifications that are required by such enterprises as financial services and government agencies, including Public Key Infrastructure (PKI), Federal Information Processing Standard (FIPS) 140-2 Hardware Security Module (HSM), General Services Administration (GSA) eAuthentication, Homeland Security Presidential Directive (HSPD)-12, and Common Criteria Evaluation Assurance Level (EAL) 4+. The combination of the high performance of hardware acceleration with simplified deployment and ongoing management reduces complexity and lowers costs of securing mission-critical services, applications and data. The reduced need for SOA programming skills means faster time-to-market for SOA benefits, without sacrificing security.

Increase trust in existing services with run-time policy enforcement

The unmatched performance of the XS40 enables enterprises to centralize security and governance functions in a single drop-in device that reduces ongoing maintenance costs (Figure 3). Simple firewall and Web-services proxy functions can be configured using a Web GUI, and run in minutes. Or, using the power of Extensible Stylesheet Language Transformation (XSLT), the device can also create sophisticated security and routing rules. WebSphere DataPower XML Security Gateway XS40 is an excellent policy-enforcement and execution engine for securing next-generation applications, enabling enterprises to control access to applications, services and data using customizable roles and rights. The XS40 integrates with leading policy managers and service registries, and supports such standards as WS-Security, WS-SecurityPolicy, WS-ReliableMessaging and WS-Policy. Manageable locally or remotely, the device supports Simple Network Management Protocol (SNMP), script-based configuration and remote logging to integrate seamlessly with leading management software.

Drop-in, standards-based security and governance for Web 2.0 applications

Modern Web applications are evolving from static pages and forms into interactions that rival native desktop programs like e-mail clients, street mapping software, and customer relationship management systems. Customers and partners across all industries demand the same level of interactivity and data access for their information as well. Unfortunately, critical business data are often locked away in legacy applications that weren't designed for this kind of usage. With its native support for JavaScript™ Object Notation (JSON) and REpresentational State Transfer (REST), the IBM WebSphere DataPower XML Security Gateway XS40 bridges Web 2.0 applications to more formal enterprise standards like WS-*. This allows businesses to engage in emerging spaces like social networking, cloud computing, and Software as a Service (SaaS).

Middleware appliances from the middleware experts

IBM WebSphere DataPower SOA Appliances combine IBM's long-standing industry leadership and expertise in SOA middleware with highly consumable, dedicated appliances that combine simplified integration, superior performance and hardened security for SOA implementations. Meticulously designed to augment all phases of the SOA life cycle and implementation, these highly specialized devices offer a host of essential SOA functions in specialized appliances for easy consumption, deployment, management and service delivery.

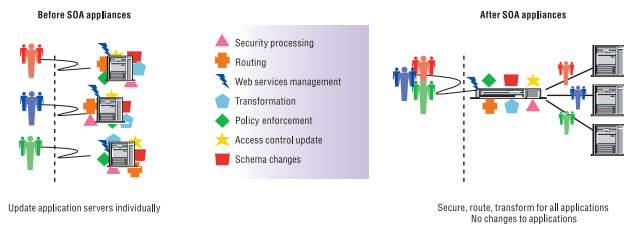


Figure 3 - WebSphere DataPower XML Security Gateway XS40 centralizes and simplifies Web services management and SOA governance.

IBM WebSphere DataPower XML Security Gateway XS40 at a glance

XML:

- XPath
 - XSLT
 - XML Schema
-

Optimization:

- Compression
 - Multistep flow processing and mediation
 - Wirespeed XML and XPath processing; XSLT
 - Quality of service (QoS) and service prioritization
-

Enterprise messaging and integration:

- HTTP, Secure HTTP (HTTPS)
 - Routing (XPath, WS-Routing and XML)
 - Message logging
-

Data security:

- Data validation (XML Schema, Web Services Description Language [WSDL] and SOAP filtering)
 - XML encryption and digital signature
 - WS-Security
 - WS-SecureConversation
 - Field- and message-level XML security
 - Internet Content Adaptation Protocol (ICAP) integration (anti-virus)
-

Security policy enforcement for XML and Web services:

- Authentication of Web services messages using WS-Security and Security Assertion Markup Language (SAML), Version 1.0, 1.1 and 2.0
 - XACML
 - Authorization for XML messages
 - Support for Kerberos, RADIUS, Lightweight Directory Access Protocol (LDAP), Microsoft® Active Directory and SAML queries
 - Ability to process Liberty Alliance ID-FF, WS-Trust and WS-Federation messages when configured with Tivoli Federated Identity Manager or a similar policy manager
 - Federal Information Processing Standard (FIPS) 140-2 Hardware Security Module (HSM) option
 - Federation of security tokens when configured with Tivoli Federated Identity Manager or a similar policy manager
-

IBM WebSphere DataPower XML Security Gateway XS40 at a glance

Web services:

- SOAP 1.1 and 1.2
- WSDL
- WS-SecurityPolicy
- WS-Policy Framework
- Registry integration (UDDI V2/V3, UDDI V3 subscription, WebSphere Service Registry and Repository)
- WS-Trust
- WS-ReliableMessaging
- WS-I Basic Profile
- WS-I Basic Security Profile
- WSDM
- WS-Management
- Support for JavaScript™ Object Notation (JSON) and REpresentational State Transfer (REST) applications

System and service security:

- Service virtualization
- XML and SOAP firewall
- XDoS protection

Management:

- Web GUI
- Command-line interface (CLI)
- Simple Network Management Protocol (SNMP)
- SOAP management interface
- Integrated development environment (IDE) integration through Eclipse and Altova XML Spy
- Service-level management (to configure, enforce and monitor qualities of service)
- Logging, drill down and alerting (on-box, off-box or centralized)
- Device partitioning and role-based management

Transport Layer Security (TLS):

- SSL and HTTPS, hardware-accelerated

Reliability:

- Virtual Router Redundancy Protocol (VRRP)
- Single firmware image

Optional features:

- Application Optimization
 - Tivoli Access Manager integration
 - Mirrored RAID 1 Disk Drives
-

For more information

To learn more about IBM WebSphere DataPower SOA appliances, contact your IBM representative or IBM Business Partner, or visit: ibm.com/software/integration/datapower/

To join the Global WebSphere Community, visit:
<http://www.websphere.org/>



© Copyright IBM Corporation 2009

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
December 2009
All Rights Reserved

IBM, the IBM logo, ibm.com, DataPower and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

Other product, company or service names may be trademarks or service marks of others.



Please Recycle
