zapthink zapnote

ZAPTHINK ZAPNOTE™

DATAPOWER XS40 XML SECURITY GATEWAY
COMPREHENSIVE XML & WEB SERVICES SECURITY ON A HARDENED NETWORK DEVICE

Analyst: Jason Bloomberg

Abstract

XML appliances have recently emerged as a category of network device that can address XML and Web Services security and performance issues that traditional network appliances cannot. To properly secure XML traffic, a device must operate on the content of the messages that pass through the network, and take appropriate action on parts of each message.

Clearly, such content-based operations are resource intensive, which is the primary reason for solving such problems on dedicated hardware devices like the DataPower XS40 XML Gateway. DataPower's XS40 appliance can handle a wide range of XML security, performance, transformation, and routing, functionality, all at wirespeed, in a security hardened appliance that requires little skill to install and administer.

Security Appliances at the Content Layer

As the use and proliferation of XML and Web Services spreads throughout the corporate IT environment, so too will the demands on optimizing the performance of the XML data and applying enterprise-wide XML policies. Increasingly organizations are seeking to find solutions that can transparently monitor XML traffic on the network and apply business rules or corporate IT policies such as security, routing, performance, management, transformation, and end-point connection provisioning without adversely impacting network performance or burdening their already overwhelmed IT departments.

Traditional network security appliances like IP-based firewalls and routers are not designed for the task of dealing with XML traffic, because they work at too low of a level in the seven-layer Open System Interconnection (OSI) model for networking architectures. In particular, the TCP/IP-based approach of traditional network hardware that focuses only on looking at where network packets come from and where they are headed misses the mark for handling metadata-rich, text-encoded XML traffic. Security at other layers, including Secure Sockets Layer (SSL), Transport Layer Security (TLS), or IP Security (IPSec), are good at preventing network snooping of traffic, but are wholly inadequate for the authentication, authorization, and other content-specific requirements for securing XML traffic.

The problem with XML traffic is that it is *content-oriented*, rather than protocol-oriented. A device responsible for securing XML traffic must make decisions based upon the content of the messages, rather than the protocols that underlie those messages. In other words, users require a layer on top of the OSI stack —the content layer—where a new class of XML appliances can operate. As a result, there is a new category of devices often called an *XML firewall* or, depending on functionality, an *XML/Web Services security gateway* that offers a range of content-based security features, including policy enforcement, malformed message protection, authorization and authentication, encryption and decryption, and schema validation. By incorporating this functionality into hardware, vendors are able to offer substantially higher performance over software-based solutions, and also offer security-hardened environments that prevent tampering as well as simplified administration. XML firewalls also free application developers from being responsible for protecting their applications from every possible type of attack, and focus them on the primary responsibility of building application logic.

DataPower XS40: Fully-Featured XML Security Appliance

One XML appliance focused squarely on solving content-oriented security issues is the *DataPower XS40* XML Security Gateway, which is a secure hardware enforcement point for XML security and access control. The 1U rackmountable hardware device performs authentication, authorization, audit and accounting based on the source, transport and content of incoming XML transactions. This device inspects all incoming messages, rejects and logs invalid requests, and ensures that only valid requests pass through to the back end.

The DataPower XS40 includes a patented hardware-based XML processing technology DataPower calls *XG3*. XG3 enables the XS40 to offer wirespeed XML processing capabilities orders of magnitude faster than the typical off-the-shelfsoftware-based XML processing solutions developers use today. With this network-speed performance, for instance, XML schema validation for every message becomes more feasible, reducing the risk from malformed XML messages. The XS40 is also a hardened appliance with no hard drive or extraneous ports or controls, allowing for simplified installation and administration. DataPower also incorporates patent-pending algorithms into the XS40 for the broadest security intelligence and functionality, including denial-of-service (XDoS) protection, SOAP filtering, access control, schema validation, digital signatures, and message or field-level encryption of XML content. Other features of the XS40 include WS-Security, SAML, XACML, XPath, XKMS, LDAP, and RADIUS compliance as well as XML/SOAP routing, SSL acceleration, service virtualization, and centralized policy management.

The DataPower XS40 offers critical functionality in four key areas:

➢ AAA framework – XS40's authentication, authorization, and audit (AAA) framework supports a variety of access control methods, and it can extract different types of identity information such as passwords or security tokens from incoming requests. Authentication and authorization steps are also fully modular, and the auditing process is extensible.

➢ Fine-grained authorization – The XS40's fine-grained authorization functionality allows it to interrogate each XML transaction and determine whether it should be allowed through based on payload content, security policy, and identity information. The appliance supports a broad variety of role-based and content-based policies.

➢ SAML and other Web Services standards support – The XS40 supports the Security Assertion Markup Language (SAML), WS-Security, and the eXtensible Access Control Markup Language (XACML) for connecting policy enforcement points like the XS40 to central policy repositories. The XS40 can consume SAML assertions, produce SAML assertions and make SAML queries to SAML servers.

➢ Wirespeed performance and hardened hardware – XS40's hardware approach allows for a high level of security, reliability, and performance. Excluding a hard drive also increases reliability, and the absence of a floppy drive or USB port eliminates the possibility of booting up the device with malicious software.

DataPower Products

DataPower XS40

Overview

The DataPower XS40 is a purpose-built, wirespeed XML security appliance that provides deep security capabilities for XML-based traffic. The product is a "drop in", rack-mountable network device that offers a broad set of security, performance, and agility benefits.

Description

The DataPower XS40 offers the following capabilities:

➢ XML firewall – filters traffic on any content or metadata variables

➢ Data validation – approves or rejects incoming or outgoing XML at wirespeed

> ➤ XML security at the field level – encrypts and signs individual message fields

> ➤ XML routing – simple or multi-step routing, as well as transport layer flexibility through protocol translation

> ➤ Service virtualization – abstracts back-end resources at transport protocol, HTTP, and SOAP header levels

> ➤ Integration with IBM WebSphere MQ and Tivoli, Computer Associates, Blue Titan, Nortel Networks, Sun Microsystems Identity Server, Netegrity, Oblix, RSA Security, and F5 solutions

Value Proposition

> ➤ *Reduced total cost of ownership and maintenance* – Instead of implementing access control in each XML application or providing software-based security solutions at less than wirespeed, the XS40 enables developers and network administrators to centralize access policy enforcement and increase the scalability of their security solutions.

> ➤ *Increased reliability and flexiblity* - The hardened hardware approach increases reliability, manageability, and security. And finally, specialized hardware and algorithms offer exceptional performance.

Key Differentiators

> ➤ *Breadth of Functionality*

> ➤ *Specialized Hardware Acceleration*

> ➤ *Diskless, Hardened Environment*

The ZapThink Take

The DataPower XS40's strongest differentiator isn't any one of its capabilities, but rather its sheer breadth of functionality. From its DataPower-engineered hardware-based wirespeed performance, to its broad security capabilities, to its routing, Service virtualization, and protocol translation capabilities, the DataPower XS40 will fill most customers' checklists of required functionality. Also to DataPower's credit is the fact that the company has been in business since 1999, providing advanced XML acceleration and network performance through several generations of technology.

DataPower originally focused on improving the performance of XML transformations, and that core ability to accelerate complex transformations serves the XS40 well. This transformation expertise finds its way into the XS40's pipeline approach to security. Security processing can contain several steps, including decryption, parsing, schema validation, XPath filtering, signature verification, and arbitrary transformations. Fundamentally, each of these operations is a transformation. DataPower's expertise in XML acceleration, combined with its XG3 processing technology and patent-pending algorithms, makes it a solid contender in the XML and Web Services security market.

Profile: DataPower	August 2004
Funding:	Seed Capital Partners, Venrock Associates, and Mobius Venture Capital
Chairman/CEO:	Jim Ricotta
Employees:	50+
Products:	DataPower XS40 XML Security Gateway DataPower XA35 XML Accelerator DataPower XI50 Integration Appliance
Address:	One Alewife Center, 4th Floor Cambridge, MA 02140
URL:	http://www.datapower.com
Phone:	1-617-864-0455
Contact:	Kevin Anderson kevina@datapower.com

Related Research

➤ *Service Orientation Market Trends* Foundation Report (ZTR-WS110)

➤ *XML Proxies* Foundation Report (ZTR-DI101)

➤ *F5 Networks: Leveraging the Network as an Integral Part of the Application* ZapNote (ZTZN-1158)

➤ *Xlipstream: Information Integration at Network Speed* ZapNote (ZTZN-1137)

About ZapThink, LLC

ZapThink is an IT market intelligence firm that provides trusted advice and critical insight into XML, Web Services, and Service Orientation. We provide our target audience of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

ZapThink's role is to help companies understand these IT products and services in the context of SOAs and the vision of Service Orientation. ZapThink provides *market intelligence* to IT vendors who offer XML and Web Services-based products to help them understand their competitive landscape and how to communicate their value proposition to their customers within the context of Service Orientation, and lay out their product roadmaps for the coming wave of Service Orientation. ZapThink also provides *implementation intelligence* to IT users who are seeking guidance and clarity into how to assemble the available products and services into a coherent roadmap to Service Orientation. Finally, ZapThink provides *demand intelligence* to IT vendors and service providers who must understand the needs of IT users as they follow the roadmap to Service Orientation.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOAs by vendors, end-users, and the press. They are in great demand as speakers, and have presented at conferences and industry events around the world. They are among the most quoted industry analysts in the IT industry.

ZapThink was founded in October 2000 and is headquartered in Waltham, Massachusetts. Its customers include Global 1000 firms, public sector organizations around the world, and many emerging businesses. ZapThink Analysts have years of experience in IT as well as research and analysis. Its analysts have previously been with such firms as IDC and ChannelWave, and have sat on the working group committees for standards bodies such as RosettaNet, UDDI, CPExchange, ebXML, EIDX, and CompTIA.

Call, email, or visit the ZapThink Web site to learn more about how ZapThink can help you to better understand how XML and Web Services impact your business or organization.

ZAPTHINK CONTACT:
ZapThink, LLC
11 Willow Street, Suite 200
Waltham, MA 02453
Phone: +1 (781) 207 0203
Fax: +1 (786) 524 3186
info@zapthink.com
www.zapthink.com