Blade Solutions

IBM - Layer 7 - Tarari XML Security in a Box White Paper

Introducing the SecureSpan™ XBlade

By Mark Litten - IBM, Phil Walston- Layer 7 Technologies, John Bromhead - Tarari

This page intentionally left blank

Table of Contents

This page intentionally left blank

Executive Summary

XML and XML-based Web services are gaining broad adoption inside the enterprise by providing a common, standards-based framework for exposing APIs and exchanging data. While XML and Web services simplify information integration, they also require new approaches to securing interactions.

To address security at an application level, dedicated XML firewalls are often used to enforce fine-grained, message-level security. But processing XML is computationally intensive and deploying or scaling architectures utilizing Web services depends on the ability to rapidly process XML and enforce security at or near wire speeds. This requires a high-performance XML security solution that is both scalable and cost-effective.

The "XML Security in a Box" solution from IBM, Layer 7 Technologies and Tarari makes it easier to secure and deploy XML-based Web services without performance trade-offs. SecureSpan™ XBlade combines the IBM eServer® BladeCenter™ platform and Layer 7 Technologies SecureSpan with the Tarari® XML RAX Content Processor to deliver the security, speed, scalability and reliability required to deploy real-world XML and Web services applications.

1) The demand for processing transactions in XML is increasing.

2) XML processing brings with it a new array of security concerns.

3) SecureSpan XBlade offers a unique, combined solution from IBM, Layer 7 and Tarari.

This paper explains the XML Security in a Box solution by describing:

- how IBM, Layer 7 and Tarari combine to form the SecureSpan XBlade, the cornerstone of XML Security in a Box
- each component of SecureSpan XBlade
- the performance benefits of SecureSpan XBlade

Solution Overview

XML Security in a Box is designed as a drop-in solution for enterprise data centers that accelerates the process of parsing XML and keeping XML-based transactions secure. At the heart of XML Security in a Box lies the SecureSpan XBlade, which combines several best-of-breed products:

- The IBM eServer BladeCenter is the platform on which the solution rests. Its chassis accommodates multiple server blades and communicates via midplane to system management, cooling and switching modules. BladeCenter offers the ease of management, capacity on demand, high availability and fault-tolerance ideal for the growing needs of Web services.
- Layer 7 Technologies' SecureSpan is a XML firewall and gateway that comprehensively prevents attacks against infrastructure, applications and transactions, while enforcing security, authentication, authorization, privacy, integrity, SLA and audit requirements.
- The Tarari XML RAX Content Processor (RAX-CP) is a silicon component that uses reconfigurable logic inside the SecureSpan XBlade to offload the processor-intensive work of parsing XML traffic from the Intel Xeon processors and to accelerate XML throughput to network speeds. RAX-CP fits in the PCI slot of the blade to accelerate XML processing as well as freeing up a significant percentage of the blade's processing power – otherwise taken up by software-only processing – for other tasks.

SecureSpan XBlade brings accelerated, robust protection to applications such as enterprise integration projects, the deployment of Service Oriented Architectures, B2B or B2C applications or any integration spanning heterogeneous platforms, operating systems or programming languages. Its flexible architecture supports SSL, WS-Security, WS-Trust and other standards while allowing growth and migration to evolving market needs and hardware options.

More-robust protection with SecureSpan XBlade means enterprises and data centers can exploit the promise of XML and Web services without enduring the performance trade-offs that have hampered acceptance of these burgeoning technologies until now.

The Problem

By providing a flexible way for expressing almost any type of information, XML has rapidly grown in prominence inside the corporate IT environment. Research from ZapThink indicates that XML traffic is expected to increase from under 15% of all network traffic on the network in 2004 to nearly 48% of all LAN network traffic by 2008. The adoption of XML Web services as an integration technology will only accelerate the use of XML as both a messaging format and a common interface into applications. But security in XML and Web services applications presents some unique problems.

Unlike traditional IP firewalls, XML and Web services require that security be enforced at the application level, rather than at the packet level. This requires complex processing to determine the content of messages, requested operations, user permissions and other factors affecting the trustworthiness of traffic. Securing XML also requires the rigorous filtering of new kinds of threats and risks due to the unique nature of how XML is structured, processed and composed into a Web services transaction.

But processing XML is computationally intensive. Since XML is at the core of Web services, building real-world architectures utilizing Web services depends on the ability to rapidly process XML and perform message-level operations like threat scanning, message inspection and routing at or near wire-speed. Since the growth of Web services is so rapid, this also requires the ability to scale message processing as traffic volumes increase, while still meeting enterprise-grade service level expectations.

Some typical application scenarios:

- A large provider of IT systems for processing secure brokerage transactions and securities data needs to support as many as 50,000 transactions per minute. The current generation of XML technology falls far short of this goal.
- A large bank could not maintain acceptable service levels after introducing XML to its workflow. Average response time per XML transaction skyrocketed by a factor of 10.
- A life science company receives and produces XML documents between 10MB and 500MB in size. The demands on their server caused by XML processing left the company unable to include these documents in their system.

As the system administrators and analysts in these scenarios wrestle to bring throughput and response times into acceptable ranges, they must endure trade-offs in performance when they try to have their XML cake and secure it, too.

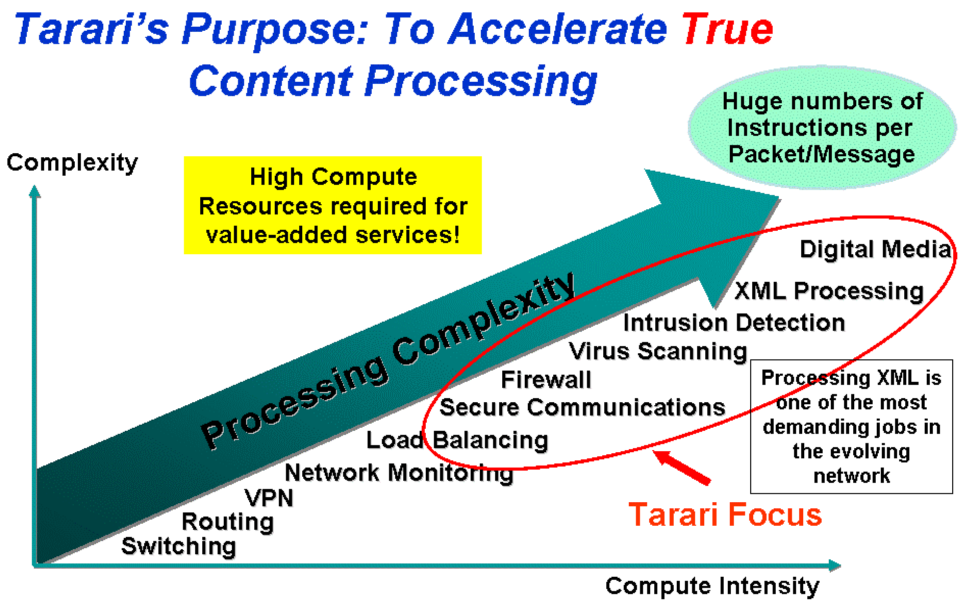

Tarari's Purpose: To Accelerate True Content Processing
Huge numbers of Instructions per Packet/Message
Complexity
High Compute Resources required for value-added services!
Processing Complexity
Digital Media
XML Processing
Intrusion Detection
Virus Scanning
Firewall
Secure Communications
Load Balancing
Network Monitoring
VPN
Routing
Switching
Processing XML is one of the most demanding jobs in the evolving network
Tarari Focus
Compute Intensity

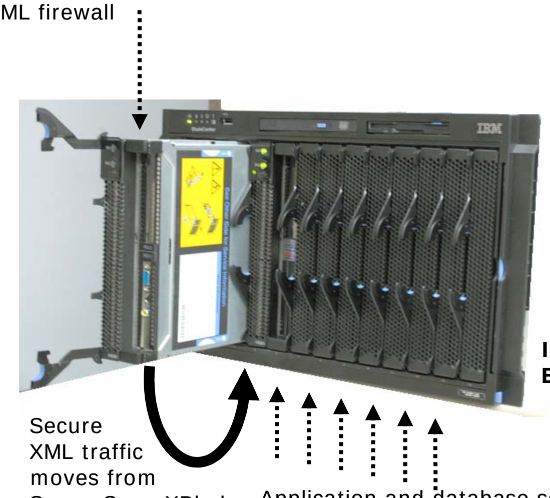
Figure 1 - Why XML Security?

SecureSpan XBlade offers the consolidation, power and manageability of BladeCenter with Tarari's years of experience in acceleration technology and Layer 7's expertise in perimeter XML firewalling for the first, over-arching solution to the problem of securing XML transactions while preserving acceptable levels of network throughput.

Solution Outline

The IBM-Layer 7-Tarari SecureSpan XBlade

SecureSpan XBlade – Hardware-accelerated XML firewall



IBM eServer BladeCenter

Secure XML traffic moves from SecureSpan XBlade through BladeCenter

Application and database server blades (HS20's, HS40's, etc.) running apps on XML-based transactions

In a typical solution, SecureSpan XBlade resides in the BladeCenter alongside server blades running a variety of applications. As XML traffic enters the BladeCenter, it flows through the SecureSpan XBlade for inspection. SecureSpan, running on the blade's main CPU, hands off the parsing of the XML messages to the Tarari RAX-CP, which returns results to SecureSpan. SecureSpan then applies any other aspects of the security policy and accepts, cleans or rejects the traffic, then passes it on to the applications running on other blades in the BladeCenter.

This means that only secure XML messages compliant with security policy will pass the XML firewall/gateway and reach the applications.

SecureSpan XBlade – Solution and Components

The following sections provide an overview of the SecureSpan XBlade solution, and a brief description of the main components:

- IBM eServer BladeCenter HS20 blade
- Layer 7 SecureSpan running on Linux (RedHat Enterprise)
- Tarari XML RAX Content Processor (RAX-CP)

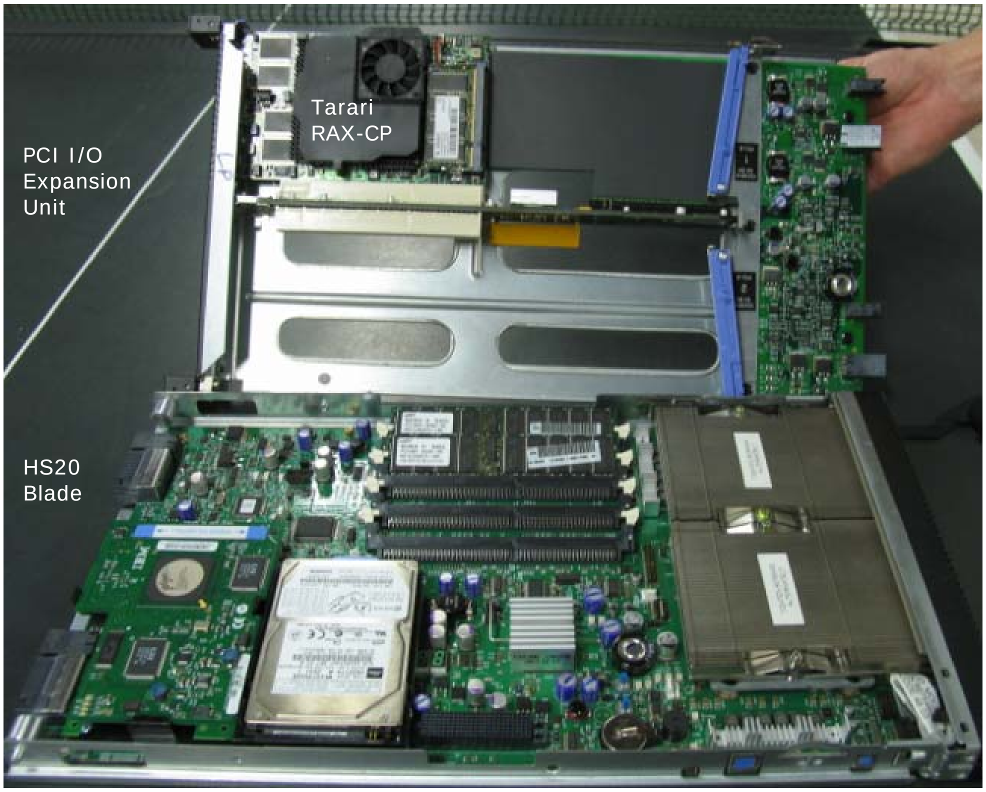


Figure 2 – SecureSpan XBlade – View of Components

IBM eServer BladeCenter HS20 blade

BladeCenter is a superior implementation of the blade server concept of physical consolidation of servers into a smaller, more manageable environment to achieve efficiency of operation. The BladeCenter design brings the client's computing resources into a cost-effective, highly reliable, modular form factor at up to twice the density of comparable 1U Intel® processor-based servers. Coupled with Intel® Xeon™ processors (at over 3GHz), modular Fibre Channel (FC) and Ethernet switches (Layer 2, and Layer 2-7) built into the BladeCenter chassis and advanced management of storage, networking, servers, and applications through IBM Director 4.2, organizations can take control of the computing environment and potentially reduce costs. Physical costs alone can potentially be reduced with a smaller footprint for multiple servers and up to an 83% reduction in cabling. BladeCenter supports IBM's TotalStorage® and networking solution in a common, fully managed architecture. Additionally, BladeCenter often takes less time to install, can require fewer people to manage and maintain, provides modular scalability and provides an environment with almost no single point of failure.

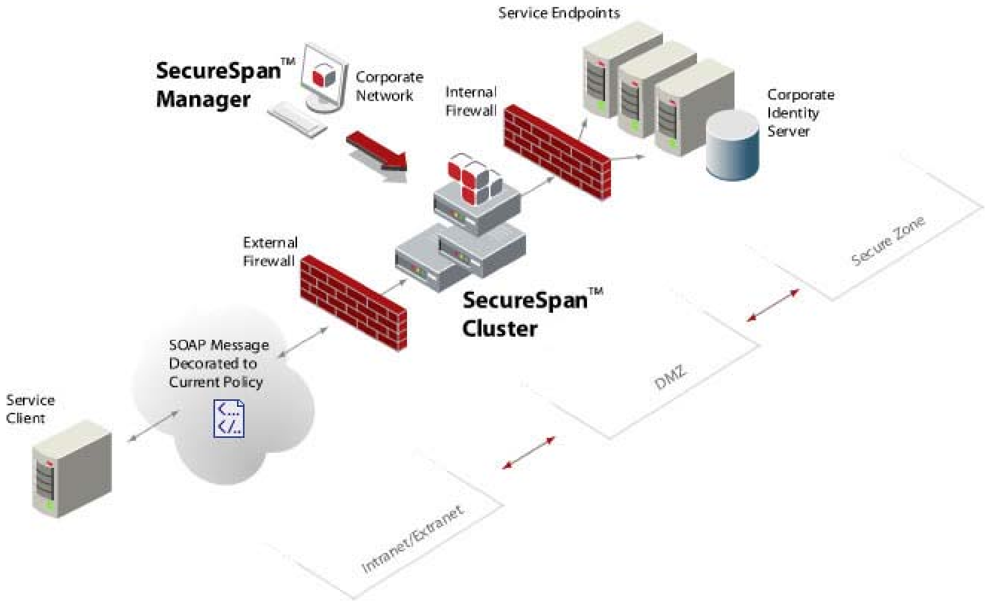
IBM BladeCenter HS20 Blade Features & Benefits

Feature	Benefits
Modular system delivering raw processing power	•Ultra-slim and powerful blade design delivers high density without sacrificing server processor performance •Up to 84 HS20 or 42 SecureSpan XBlades in an industry-standard rack, packing more performance per square foot and saving valuable central office and/or data center real estate •Hot-swappable, designed for adding or changing servers without disrupting the operation of other servers in the chassis
Supports up to two Intel Xeon processors with 800 MHz front-side bus	•Equipped with Intel Hyper-Threading and NetBurst® technologies, the Intel Xeon processor delivers server performance ideal for compute-intensive, next-generation network and IT application workloads
Up to 8GB of DDR ECC Chipkill™ memory	•Double data rate, error checking and correction, and Chipkill offer high performance with mainframe-inspired fault protection •Able to handle data-hungry applications with memory to spare
64-bit extensions	•Supports Intel® Extended Memory 64 Technology (Intel® EM64T) with embedded Intel Xeon 3.06 GHz processor(s) on HS20 blade model 8832-XXX •Provides 64-bit addressability while supporting both 64- and 32-bit applications, a smooth transition to 64-bit enabled applications while leveraging the price and performance of existing applications
Integrated dual Gigabit Ethernet connections	•Enabled to transmit large amounts of data at high speeds for high-performance network applications •Robust design supports teaming and failover
Two high-availability midplane connections	•Provides durable and reliable connections to all chassis resources
Integrated System Management Processor	•Increases server availability by continuously monitoring the system and sending notification of potential system failures or changes

Feature	**Benefits**
IBM Director and IBM Director Extensions comprehensive systems management tools	•Exploits hardware capabilities by returning pertinent system information, allowing automated response •Helps increase uptime, reduce costs and improve productivity via advanced server management capabilities •Provides intelligent system management for rock-solid reliability •Remote Deployment Manager simplifies and automates deployment and redeployment for efficient installation and startup of IBM eServer BladeCenter T
Operating System Support	•Red Hat Enterprise Linux
3-year on-site limited warranty[1] for parts and labor	•The IBM Global Services organization provides reliable, dedicated and skilled assistance when needed •Provides peace of mind for an extended period of time
Blade server interconnects	•Supports an optional 2-port (2Gb per port) FC Expansion Card (Host Bus Adapter) to deliver a high-performance, highly manageable Storage Area Network (SAN) •Supports an optional 2-port (1Gb per port) Gigabit Ethernet Expansion Card to enable additional Ethernet bandwidth and allows for connection to multiple LAN segments
Light path diagnostics self-diagnosis panel	•Provides quick and easy guide to troubleshoot server for higher availability and system uptime •Independently powered, allowing removal of the server from the chassis and persistent illumination of the light path LEDs
Predictive Failure Analysis™ (PFA)	•Helps save time and money by decreasing planned and unplanned downtime •Increases uptime by sending proactive alerts as much as 24-48 hours in advance

Layer 7 SecureSpan

SecureSpan is an advanced XML firewall that defends access to protected applications. In typical configurations SecureSpan resides between application servers and the DMZ, or on the boundary of departmental security, identity, or trust zones. Optimized for both XML and SOAP environments, SecureSpan provides administrators fine-grained control over how Web services and XML applications are exposed to and accessed by external applications, without programming.



SecureSpan performs the role of policy enforcement point, combining an intelligent message-processing engine with an XML firewall that enforces a set of user-defined security policies on every service provisioned through the SecureSpan Manager console application. SecureSpan identifies and processes each message under the policies created for a respective service. It shields access to internal services, ensuring that only those messages meeting all security requirements are forwarded to the destination service residing on an application server.

SecureSpan's patent-pending, policy-driven XML Stream Processor technology is specifically designed to screen out threats specific to XML and Web services and to enforce security policies, maintaining high service availability and reducing the impact of many attacks. XML and Web services threats fall into three broad classes:

1. Infrastructure Attacks
   - Operating system exploits that undermine a host's execution environment
   - Parser attacks that compromise Web services performance or operation
   - Denial of Service-type attacks that degrade availability of a Web service
2. Application Attacks
   - WSDL API scanning and address discovery
   - XML message content manipulation, injection and malformation
   - Message attachments carrying viruses
3. Transactional Attacks
   - Manipulation or inspection of data during transmission
   - Spoofing identity during a transaction
   - Hijacking a communication session

To effectively protect Web services against these threats, SecureSpan performs deep inspection of XML and Web services messages for potential risks, screening out attacks before they can do harm. This process combines Layer 7's proprietary processing technology with the acceleration provided by the Tarari XML RAX Content Processor to perform the complex XML operations required to parse, probe and compare XML messages at near wire speed. The result is accelerated protection against XML threats and fine-grained security with maintenance of the tough service levels demanded by internal stakeholders, business partners and customers.

As traffic volumes increase, SecureSpan is designed to meet increased needs by providing a high-availability, peered configuration that scales in a linear fashion simply by adding more blades. These form SecureSpan Clusters that process high volumes of service transactions, all administered through a common SecureSpan Manager.

Tarari XML RAX Content Processor

Tarari has developed the industry's first commercial implementation of Random Access XML (RAX): a breakthrough for XML processing which has been benchmarked at 40 to as much as 200 times the performance of conventional XML technologies. RAX provides direct access to the data needed by an application with near-zero parsing and other processing overhead.

Tarari's XML RAX Content Processor (RAX-CP), a device which has been designed to snap into the HS20 PCI I/O Expansion Unit, accelerates and offloads the XML processing from the main CPU and performs the parsing in specialized hardware. Not only is RAX-CP much faster than software, but it also leaves the CPU free for other tasks.

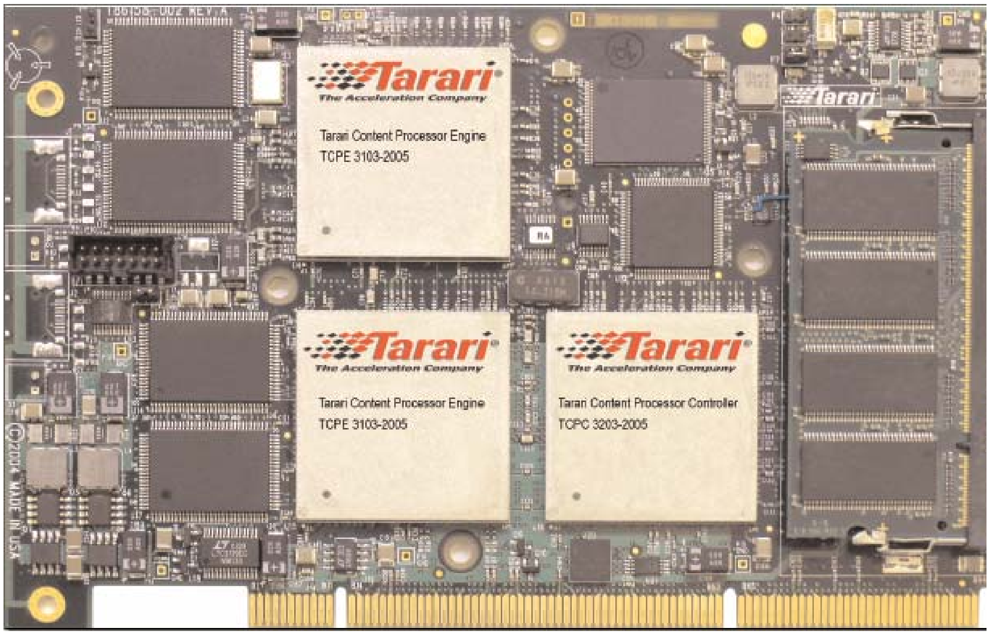
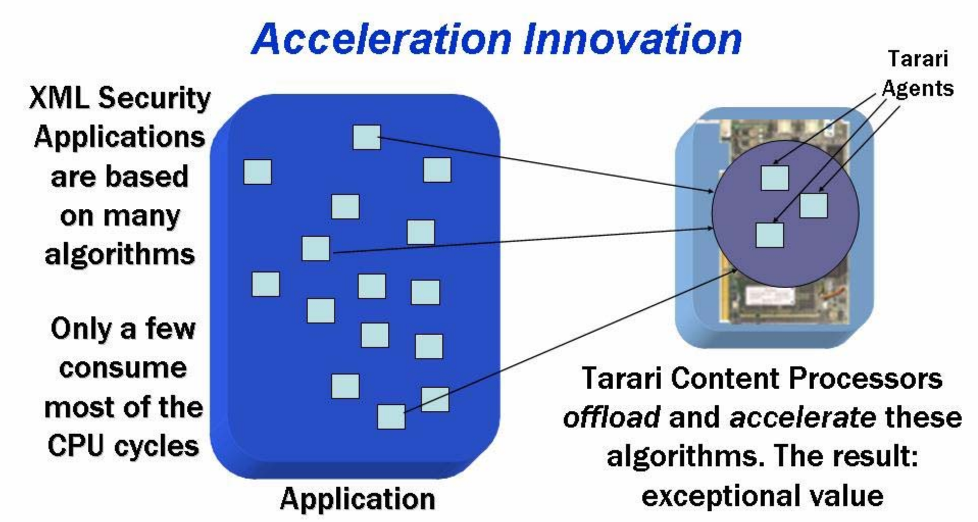


Figure 3 - Tarari XML RAX Content Processor (RAX-CP)

Tarari Acceleration Innovation

The silicon-based Tarari XML RAX Content Processor uses high-performance dedicated logic and customizable silicon to run Tarari agents especially designed to accelerate XML processing. RAX-CP uses silicon logic to accelerate the most processor-intensive algorithms, offload them from the general-purpose CPU, and execute them at accelerated speeds on the Tarari hardware. This frees up for other tasks those processor cycles typically consumed in software-only XML parsing. RAX-CP supports Random Access XML, simultaneous XPath, SOAP processing, schema validation and streaming XML transformation.


Acceleration Innovation
XML Security Applications are based on many algorithms
Only a few consume most of the CPU cycles
Application
Tarari Agents
Tarari Content Processors *offload* and *accelerate* these algorithms. The result: exceptional value

Installation

- SecureSpan XBlade

If the SecureSpan XBlade is already completely assembled, simply slide it into the BladeCenter chassis.

Otherwise, fit the Tarari XML RAX Content Processor into the PCI I/O Expansion Unit ("sidecar"), snap the BladeCenter HS20 closed, and replace it in the BladeCenter chassis. Then install Redhat Enterprise Linux and Layer 7 SecureSpan software onto the BladeCenter HS20.

- SecureSpan Manager

Install the SecureSpan Manager on any Linux workstation running RedHat Enterprise 4.0 and later. Set configuration options as required and create policies to protect services using the intuitive Manager user interface.

Optional: Install additional blades to meet higher requirements for sustained traffic volume.

Major Features and Benefits

- **Key enabler for adoption of XML / Web services**

As outlined above, the trade-off between acceptable performance and acceptable security has hampered the adoption of XML in some enterprises. SecureSpan XBlade bridges the gap between performance and security and does away with the trade-off.

- **Reduced cost per megabyte of content processed**

SecureSpan XBlade is more than technically interesting; it is also a compelling business case rooted in high performance. XML documents that previously took minutes to process can now be processed in fractions of a second. With 40-200x speedup over comparable software approaches, the cost of processing XML and exploiting Web services drops dramatically, and the opportunity to realize the promise of XML-based content rises correspondingly.

- **Reconfigurable assets**

SecureSpan XBlade is designed for flexibility and migration. As hardware and throughput requirements grow, the modular nature of BladeCenter allows for upgrades to processors, memory, storage and connectivity. As parsing needs change and Web services evolve, RAX-CP's reprogrammable logic accommodates in-field reconfiguration for performance improvements and new features in as little as 30 milliseconds, resulting in less downtime, less obsolescence of purchased hardware and lower inventory of spare parts.

- **Big advantage over competing approaches**

The alternative, “XML Security out of a Box,” features dedicated, proprietary network appliances that live outside of the HS20 and outside of the BladeCenter as security add-ons. These appliances, while they may play a role in standard network security configurations, do not lend themselves to integration with the BladeCenter model.

- **High-performance security with scalability**

SecureSpan XBlade uses the optimal combination of software, processor and co-processor to keep security-related XML message processing from impacting service levels or throughput. Also, as XML applications and Web services deployments continue to grow, these blades can be added to meet increased demands for throughput.

- **Simple network topology and integrated solution**

BladeCenter represents an investment not only in computing hardware, but also in form factor and IT strategy. SecureSpan XBlade is the first XML firewall and gateway to take full advantage of the scalability and manageability of the BladeCenter. The SecureSpan XBlade provides an integrated, drop-in XML security solution for rapid deployment of secured Web services in any corporate data center. Services can go live securely within minutes of deployment.

Performance

SecureSpan XBlade does the heavy lifting, keeping the XML processing work from bogging down other applications. This results in comprehensive threat protection and security, without unacceptable increases in message latency.

Applies dedicated hardware to compute-intensive processes

The SecureSpan XBlade is designed to execute key XML processing functions, such as schema validation, much faster than on general-purpose CPUs. The SecureSpan XBlade can also free other blades in the BladeCenter for other tasks, resulting in increased overall productivity.

Consumes much less power

The IBM BladeCenter offers 20-40% savings in power consumption over traditional standalone systems, according to the Gartner Power Usage Report[1]. This not only results in lower costs for raw electricity but also reduces the cooling requirements over traditional 1U servers, while offering higher availability and fault-tolerance. Furthermore, because of the Tarari RAX-CP, which consumes less than 20 watts, SecureSpan XBlades make for even lower power consumption. Seven SecureSpan XBlades in a BladeCenter chassis would deliver similar XML/Web services performance to over 35 normal BladeCenter HS20 blades; yet consume only about one-fifth the power of that configuration.

[1] Electrical Requirements for Blade Servers. Written by Jane Wright (G00120690) released April 24, 2004. Available from Gartner Research.

	1U server	**HP BL20p G2**	**IBM BladeCenter HS20**
Max config / rack	84 Xeon DP 3.2Ghz	96 Xeon DP 3.2Ghz	168 Xeon DP 3.2Ghz
Equalized rack fulfillment	36 servers, 72 processors	5 enclosures, 36 servers, 72 processors	3 enclosures, 36 servers, 72 processors
U space required	36U	30U	21U
Power requirement	15,912W	13,891W	**8,872W**
Heat output	54,260 BTU	47,365 BTU	**30,255 BTU**

Key Messages

1. SecureSpan XBlade brings unprecedented performance in an XML firewall to a new breed of Web services applications while delivering the density, high availability and scalability of the IBM eServer BladeCenter platform.

2. SecureSpan XBlade performs XML/Web services firewalling, using RAX-CP to offload and accelerate the compute-intensive work of parsing the XML.

3. SecureSpan XBlade consolidates the XML firewall, XML acceleration, processing and network functions required to protect and deploy XML and Web services.

4. SecureSpan XBlade provides the fine-grained, flexible control over security required to meet almost any XML or Web services deployment.

Summary

The IBM – Layer 7 – Tarari SecureSpan XBlade is the first XML firewall with accelerated threat protection designed specifically for deployment in IBM's eServer BladeCenter for high-availability, scalable XML firewalling in corporate data centers. The result is cost-effective, highly available, high-performing and scalable, on demand.

SecureSpan XBlade is designed to enable the end-to-end security and management of Web services and XML applications spanning departments or the globe.

SecureSpan XBlade brings to XML firewalling the dedicated hardware and acceleration needed to protect XML/Web services applications without adversely affecting performance and network throughput.

This integrated solution delivers high performance at a fraction of the cost of competing approaches. It delivers automated performance and response monitoring, system wide automated rollback, disaster recovery, replication and auditing.

Additional Information

IBM BladeCenter
ibm.com/servers/eserver/bladecenter

IBM eServer BladeCenter HS20 (8832-xxx)
IBM PCI I/O Expansion Unit (90P3721)

Layer 7 Technologies
Layer7-tech.com

Layer 7 SecureSpan

Tarari, Inc.
Tarari.com/rax

Tarari XML RAX Content Processor (RAX-CP)

Prices do not include tax or shipping and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Price may include applicable discounts. Reseller prices may vary. Unless otherwise specified, pricing information is current as of original publication of this document.

MB, GB, and TB = 1,000,000, 1,000,000,000 and 1,000,000,000,000 bytes, respectively, when referring to storage capacity. Accessible capacity is less; up to 3GB is used in service partition. Actual storage capacity will vary based upon many factors and may be less than stated. Some numbers given for storage capacities give capacity in native mode followed by capacity using data compression technology. Maximum internal hard disk and memory capacities may require the replacement of any standard hard drives and/or memory and the population of all hard disk bays and memory slots with the largest currently supported drives available. When referring to variable speed CD-ROMs, CD-Rs, CD-RWs and DVDs, actual playback speed will vary and is often less than the maximum possible.

IBM, the eight bar logo, the _`logo, xSeries, BladeCenter, Chipkill, ClusterProven, ServerProven, ServeRAID and TotalStorage are trademarks or registered trademarks of International Business Machines Corporation in the U.S. and other countries. For a list of additional IBM trademarks visit **ibm.com**/legal/copytrade.shtml.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation.
Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
Other company, product and service names may be trademarks or service marks of others.

Visit **ibm.com**/pc/safecomputing periodically for the latest information on safe and effective computing. Warranty Information: For a copy of applicable product warranties, write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services including those designated as ServerProven® or ClusterProven®. Telephone support may be subject to additional charges. For onsite labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician.

All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

This publication was developed for products and services offered in the United States.

IBM may not offer the products, services or features discussed in this document in other countries. Information is subject to change without notice. Consult your local IBM representative for information on offerings available in your area.

All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of a specific Statement of General Direction.

The examples given in this paper are hypothetical examples of how a customer can use the products described herein and examples of potential cost or efficiency savings are not based on any actual case study. There is no guarantee of comparable results. Many factors determine the sizing requirements and performance of a systems architecture.

IBM assumes no liability for the methodology used for determining the configurations recommended in this document nor for the results it provides.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements quoted in this presentation may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this presentation may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information in this presentation concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources.

IBM has not tested these products and cannot confirm the accuracy of performance, compatibility or any other claims related to non- IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.