lustratus

Research

A Competitive Review of SOA Appliances

Comparing SOA appliances from IBM, Layer 7 and Intel

Author: *Steve Craggs*

Version 1.00
March 2010

Table of Contents

Executive Summary 3
Introduction 4
- Why appliances? 4
- Competitive assessment approach 4

Why SOA Appliances? 4
- SOA Background 5
- How can appliances help SOA? 5

SOA Appliance Offerings 7
- IBM DataPower 8
  - Background 8
  - What is the IBM WebSphere DataPower portfolio? 8
- Intel SOA Expressway 11
  - Background 11
  - What is Intel SOA Expressway? 11
- Layer 7 SecureSpan SOA Appliances 13
  - Background 13
  - What is in the Layer 7 SecureSpan XML appliance range? 13

SOA appliances – Competitive assessment 16
- Improve SOA performance/predictability/resource usage 16
  - Setting the scene 16
  - Competitive assessment 17
- Enhance SOA security and governance 19
  - Setting the scene 19
  - Competitive assessment 19
- Reduce SOA complexity / total cost of ownership (TCO) 20
  - Setting the scene 20
  - Competitive assessment 20
- Miscellaneous observations 21
- Competitive summary 21

Conclusion 22

Disclaimer

Whilst reasonable care and skill has been taken by Lustratus Research Limited (the company) in the preparation of this report no liability is accepted by the company (except in the case of death or personal injury caused by the company's negligence) by reason of any representation or any implied warranty condition or other term or any statutory or common law duty or otherwise howsoever arising for any direct or indirect general special or consequential damages or loss costs expenses or other claims (whether caused by the negligence of the company or otherwise) which come out of the provision of this report or its use.

All trademarks are acknowledged as the property of their respective owners.

Executive Summary

The idea of appliances is not new. Packaged, self-contained, specialized servers have been performing tasks such as network gateways, firewalls and email cleansing for years. The attraction of an appliance is that access to the internals is restricted by the hardware form factor, and its specialized role enables hardware and software efficiencies that would not be possible in a general purpose server environment. As a result, appliances have the reputation of being tamper-proof, easy to install and configure and ideal for mechanical and repetitive operations.

Meanwhile, service oriented architecture (SOA) continues to grow in popularity, being adopted across more and more of the enterprise and partner value chain as companies seek greater agility, visibility and closer alignment of IT to business needs. As a result SOA network traffic, based around the self-defining XML data format, is growing exponentially and broadening to touch more and more domains and environments. This makes areas such as security, traffic management and the overhead of XML processing major concerns. In addition, the constantly growing SOA infrastructure continues to get more complex as more moving parts are added.

SOA appliances were introduced to address precisely these concerns. The idea is to offer a dedicated, fixed-purpose environment of specialized and highly optimized hardware and software in a robust and secure package. This environment will not only handle SOA and XML security, processing and governance needs, but will also mitigate SOA risk, reduce costs and increase efficiency. The market is growing, and a number of SOA appliance vendors have emerged; some are the usual SOA suspects like IBM and TIBCO, while others are specialist appliance vendors like Layer 7. Even Intel has decided to enter the fray with a rather unusual software version of the SOA appliance model, which seems a contradiction in terms.

This assessment takes a look at the SOA appliances being offered by three of these vendors, and considers where these offerings best fit in addressing SOA needs. The TIBCO appliance does not really fit in the SOA appliance category since it only offers a hardware implementation of the TIBCO Rendezvous messaging product, and so TIBCO is not included in this review. Summarizing the conclusions of this assessment, for general SOA needs the most comprehensive SOA appliance portfolio with the maximum opportunity for benefit comes from IBM. The Layer 7 range competes in the areas of security and governance, while the Intel ‘soft appliance’ may be of interest to organizations not wanting the more robust hardware form factor. However, whichever supplier is selected, the SOA appliance will most certainly be taking its place as an important element of an overall SOA deployment. While not suitable for all SOA needs, the efficiency, security, performance and simplification offered by SOA appliances makes them something that all SOA adopters should take into close consideration.

Introduction

The purpose of this paper is to provide independent guidance for companies thinking about purchasing SOA appliances – dedicated servers designed to help with the challenges thrown up by adopting a service-oriented architecture. After setting the scene with a discussion about appliances and their role in SOA, the focus will be turned on three SOA appliance candidates; IBM's DataPower range, Intel SOA Expressway and the SecureSpan range from Layer 7. Each offering will be summarized and then the three offerings will be compared against each other to identify the pros and cons of each solution.

Why appliances?

The appliance concept has been around for many years. At its most basic, it represents the idea of taking a specific set of functions and embodying them in a dedicated piece of hardware – the appliance. There are a number of reasons this may be appropriate. Firstly, a dedicated piece of hardware has better security characteristics than software running in the general corporate processing environment. If functionality is embedded in hardware, then it is much more tamper-proof than normal software, and in addition the fact that the appliance offers a dedicated set of services limits the scope for unwarranted intrusion affecting the rest of corporate operations. Implementing software in electronics also enables a much higher speed of execution, with less scope for human error, and allows the use of specialized availability measures such as duplicate resources. Then there is a price/performance consideration; moving processing activity to a purpose-built appliance may offer a cheaper processing alternative than using valuable processing capacity in the main corporate IT platform. There is also an advantage to be gained from a higher degree of standardization imposed by the fact that appliances often come pre-loaded and pre-configured, leaving only a prescribed set of customization options. The result is a more uniform infrastructure with fewer skills demands and less opportunity for mistakes.

Of course, appliances don't fit every need. In areas where significant amounts of custom coding are required, for instance, software may be more appropriate choice. But appliances appeal strongly where a cost-effective workhorse is required to repeatedly execute a fixed range of functionality, or where security is paramount. It is therefore no surprise that historically, one of the first uses of the appliance concept was in providing network security gateways. The secure nature of the appliance makes it ideal for deploying in the DMZ, as a protective shield around the corporate network, and in this role it also provides another very useful facility by offering a single point of management and control for all traffic coming in and going out of the enterprise.

Competitive assessment approach

The remainder of this paper assesses three of the main vendors of SOA appliances; IBM, Intel and Layer 7. The structure is laid out as follows:

1. Take a look at the key functional areas SOA appliances can deliver to establish a framework
2. Provide a high-level summary of functionality offered by each vendor against this framework
3. Set out the key drivers for purchasing SOA appliances
4. Consider and contrast each supplier's functionality in the light of these drivers

Why SOA Appliances?

So how does the appliance concept relate to service-oriented architecture (SOA)? Why is there a need for appliances in this software-dominated area? The answer is that the nature of SOA throws up some specific challenges for organizations, and some of these map precisely onto the characteristics of appliances discussed above.

SOA Background

Most IT professionals have at least a general idea of SOA now. The idea behind SOA is that the monolithic programs driving many corporate IT applications are broken up into a pool of shared business services which each perform some well-defined business activity, such as 'Get Customer Details' or 'Raise Purchase Order'. Applications now become flows of linked services combined with any remaining application-specific logic. Connectivity between these services and components is almost always based around the XML standard of data description which removes the need to know the source of the information before being able to understand it. These services may not reside in local IT systems, but may be spread across the enterprise or partner systems.

SOA delivers many benefits, including agility, reliability, business visibility and cost efficiency; but it also generates some important side-effects. For example, SOA is turning IT applications into a collection of services that can be accessed across the network or internet, and therefore an immediate concern is security. These services may represent key business activities, and it would be most damaging if unauthorized users could access or affect them. Another problem is that XML traffic is both verbose and unreadable to ordinary network security solutions. As a result, existing network firewalls and gateways cannot unpick the XML data streams to identify threats or other problems, and in addition the switching to and from XML formats and the XML parsing all increase the drain on processing capacity.

As well as these operational issues, SOA tends to lead to applications that extend across multiple environments, requiring an extensive and distributed infrastructure. As SOA adoption expands, this can create an increasing load in terms of implementing, administering and managing this infrastructure. These are all areas where judicious use of appliances can help.

How can appliances help SOA?

As SOA adoption has increased, a range of appliances have appeared in the market to provide additional options and capabilities within an SOA environment. Sometimes these appliances are classed as XML rather than SOA appliances, but the XML appliances are almost always deployed to help SOA implementations, so it makes sense to regard all of these under the banner of SOA appliances. There are five prime areas of functionality that SOA appliances deliver, as summarized below.

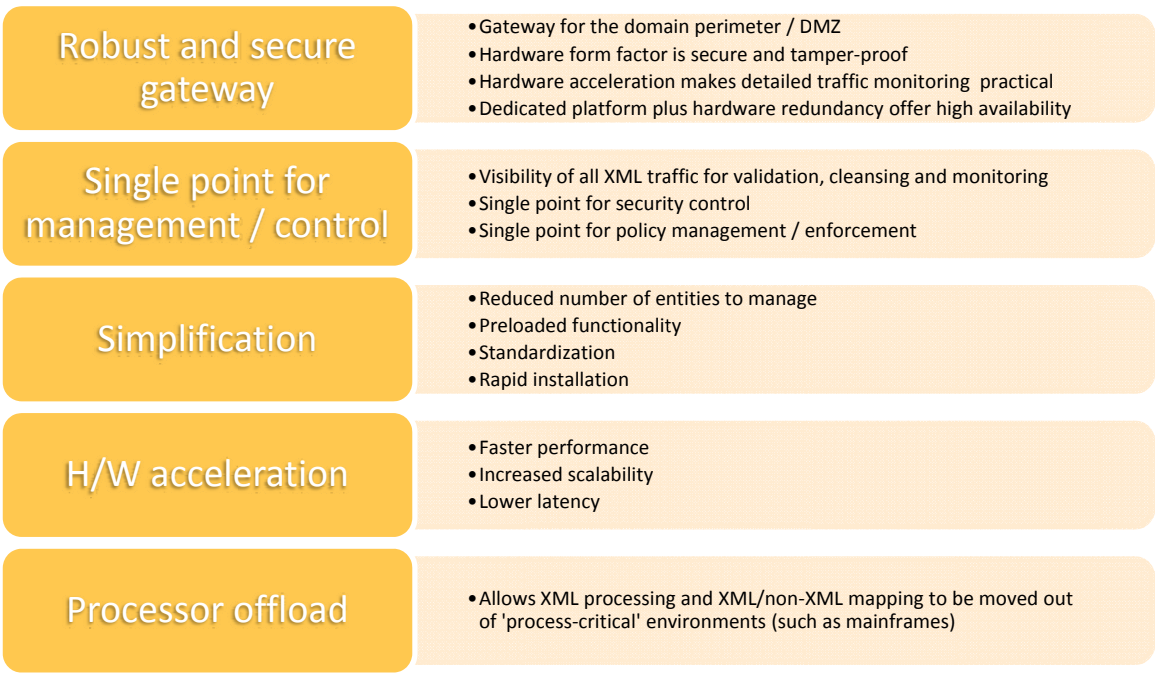

Figure 1: The five main functional areas delivered by SOA appliances

Anyone who has dealt with networks knows the value of having a security firewall / gateway to preserve network integrity and provide protection from unauthorized access or other external threats. The added advantage of supplying this capability in the form of an appliance is that a self-contained hardware unit offers less opportunity for either accidental or malicious tampering, while the dedicated platform combined with built-in hardware redundancy offers excellent availability. But network owners are now well aware that traditional network firewalls struggle with SOA traffic, because often the internal messages are encrypted and the firewalls are not familiar with XML flows anyway. Most network firewalls are therefore blind to SOA traffic. The SOA appliance is specifically designed to deliver the same level of protection for SOA and XML as is present today for standard network use.

Following on from the concept of an SOA appliance as a gateway, it is natural for the appliance to offer functionality to monitor, manage and police the XML traffic. The single point of control offered by the SOA appliance enables it to take responsibility for monitoring, validating, cleansing and controlling traffic content and speed, thereby removing the need for every other part of the infrastructure to do the same. Most SOA appliances therefore provide functionality in these areas, often supporting policies that offer an easy and enforceable way for organizations to ensure proper management and control of the SOA network and services. A key factor here is that because appliances can leverage hardware acceleration and can therefore execute processing much more quickly, it becomes practical to carry out this traffic management without undue overhead. Without faster, hardware-assisted processing, extensive analysis of traffic flows would put considerable strain on overall system performance.

Simplification is another key area of SOA appliance functionality. The principle is that by consolidating some SOA infrastructure functionality into a dedicated appliance, the system landscape can be simplified with an associated reduction in total cost of ownership (TCO). Some of the simplification capabilities come without the need for any extra functionality – for example, by collecting all the security functionality into one place, updating and maintaining it only requires one set of changes in one place. Similarly, the single point of control functionality already mentioned means there is one place to manage and monitor SOA traffic and policies, again simplifying the overall SOA management task. Then there is the benefit of standardizing functionality in a uniform, pre-configured platform, also reducing support requirements and making installation quicker and less complex.

However, specific appliance functionality is required to gain the best levels of simplification, which is delivered in primarily two areas. The first is that because the SOA appliance is a dedicated environment and does not need to consider general purpose processing needs, it can include functionality designed to optimize SOA and XML processing. This optimization can be achieved through specialized software design/execution and the use of hardware acceleration, discussed in more detail later. The result is that it may be possible to replace multiple servers in the SOA infrastructure with a single appliance, thereby considerably reducing overall costs at both a capital and operational level. The second area where SOA appliance functionality can deliver more scope for simplification is in the range of SOA infrastructure functions it provides. For example, an appliance might be designed just to provide security gateway services, or it could be extended to provide major pieces of SOA functionality such as ESB (Enterprise Service Bus) capabilities. Additional appliance options extend the opportunity to simplify SOA to a wider level.

This leads on to the area of hardware acceleration. A prime area of benefit from appliances is the fact that parts of the software can be implemented in electronics, giving performance approaching wire-speed. In addition, since the appliance is a dedicated environment, it is not even necessary for it to have the overhead of running a general purpose operating system. Specifically in the case of SOA, XML messages are frequently sent between heterogeneous domains that require transforming in order to be understood by the recipient. In addition, XML needs to be parsed at every stage to understand what is required, and all of these XML processing activities take time and resources. By designing processing logic specifically for this restricted usage, and taking advantage of hardware implementation, the SOA appliance can offer dramatic improvements in performance and capacity, delivering faster response times and leading to greater simplification through consolidation. It is

worth noting here, however, that just accelerating XML processing and transformation only addresses part of the problem; in an SOA environment it can be just as important to optimize non-XML / XML conversions too.

The fifth key functional area for SOA appliances relates to scenarios where general-purpose processor power is at a premium. For example, many users keep a very close eye on anything that may increase the demand for mainframe MIPS. In this respect, SOA and XML in particular are especially troublesome, because very few mainframe applications are designed to work with native XML formats, and as such there is often a very high load of transformations required between mainframe and XML formats as messages fly to and fro. SOA appliances address this problem by providing a more efficient platform for these calculations that places minimal drain on general-purpose resources. But to achieve this, the appliance needs to support interoperation with these environments to ensure it does not add to the problem or negatively impact performance.

SOA Appliance Offerings

Having identified the key areas of functionality for SOA appliances, this now establishes a functional frame of reference for looking at SOA appliances. However, it is important not to limit this framework to purely technical features. Instead, there are a number of ancillary aspects that need to be taken into account, such as how much time and effort will be required to deliver the expected benefits, how these SOA appliances are likely to affect overall total cost of ownership (TCO) and what level of flexibility the appliances offer. This section will therefore consider SOA appliances in two categories; functionality in the five key areas, and added-value features. The table below summarizes some of the factors considered in each area.

Basic functionality	Value-Add
Robust / secure gateway ■ Protection from XML-based threats and intrusion ■ High availability ■ Secure environment ■ Throttling and control of traffic flows **Single point for management / control** ■ SOA service authentication, authorization and audit ■ Service policy management and enforcement **Simplification** ■ SOA processing design efficiency ■ Breadth of SOA functionality available ■ Single point of control ■ Hardware acceleration **Hardware acceleration** ■ Areas covered ■ Acceleration effectiveness **Processor offload** ■ Integration with general-purpose environments	**Ease of Use** ■ Standards usage ■ Tools ■ Ease of customization **Manageability** ■ Monitoring and reporting ■ Administration ■ Interaction with other management frameworks ■ Maintenance / upgrade facilities **Flexibility and extensibility** ■ Partner ecosystem ■ Additional deployment options **Time to Value** ■ SOA experience / availability of skills ■ Skills requirements ■ Pre-packaged configurations and options **Miscellaneous** ■ Green credentials ■ Special offers

Figure 2: SOA appliances functional capabilities framework

With this framework in mind, the SOA appliance solutions for each of the three target vendors will be summarized, and then their competitive positioning will be discussed. The three vendors covered, in alphabetical order, are IBM, Intel and Layer 7.

IBM DataPower

Background

In late 2005, IBM acquired DataPower, a US-based provider of appliances designed to improve security and performance of XML web services processing. DataPower was a pioneer in XML appliances, approaching the issue from the perspective of leveraging the hardware appliance model to drive better security and performance, and as such DataPower offerings are designed to take advantage of hardware mechanisms such as application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs). IBM has since embraced the appliance approach, expanding the DataPower portfolio of offerings to cover wider SOA needs, rolling it under its SOA-leading WebSphere brand. Beyond SOA, IBM has seen considerable activity for its DataPower appliances as a general purpose, hardened proxy for the DMZ handling different forms of traffic such as REST and other Web 2.0 protocols. In addition, IBM has continued to develop new appliance offerings in other areas, such as the IBM WebSphere Cloudburst appliance.

Importantly, the IBM acquisition of DataPower has not led to any attempt to restrict DataPower applicability to the IBM fold. While DataPower now lives within the IBM WebSphere family, it remains just as relevant to non-IBM environments like Oracle, SAP and webMethods.

What is the IBM WebSphere DataPower portfolio?

IBM inherited a number of SOA appliances when it acquired DataPower, and this range has been expanded since the acquisition, demonstrating IBM's commitment to SOA appliances. Key members of the DataPower SOA appliance portfolio include:

IBM WebSphere DataPower Appliances	
WebSphere DataPower Integration Appliance XI50	Simplified ESB/application integration, deployment and hardened security
WebSphere DataPower XML Security Gateway XS40	Secure XML web services gateway
WebSphere DataPower B2B Appliance XB60	Secure B2B and file transfer gateway
WebSphere DataPower Low Latency Appliance XM70	Low-latency messaging
WebSphere DataPower XML Accelerator XA35	High-speed XML processing

Figure 3:- IBM WebSphere DataPower appliances coverage

The XA35 provides the hardware-accelerated XML processing foundation for the range, and is included in each of the other DataPower SOA appliances. The XS40 is the classic XML-based network security/firewall offering, servicing the same sorts of needs for XML / SOA that a network gateway with firewall serves for general network traffic. The XI50, which is IBM's biggest seller of the range, adds much more extensive SOA infrastructure capabilities on top of the XS40/XA35, bringing the power of an ESB (Enterprise Service Bus) implementation to the range. The last two SOA appliances extend the XI50 capabilities, with the XB60 adding B2B-specific capabilities such as partner profile management and the XM70 delivering a low-latency messaging solution. This is not the complete range of DataPower appliances – for example the WebSphere Cloudburst Appliance directly targets cloud adopters – but these are the ones most relevant to this analysis.

Basic SOA appliance functionality

As stated above, the XS40 offers robust, secure XML and web services gateway functionality, and this functionality is also included in the XI50, XB60 and XM70. The device acts as an XML firewall, detecting XML-borne threats and attacks such as denial of service, and identifying and protecting from incoming viruses. It provides this functionality within a reliable appliance form factor, with hardware redundancy, clustering support and optional mirrored disk drives for high availability. The XS40 offers comprehensive security features that are tightly integrated with related standards. Identity management can be done through integration with Tivoli Federated Identity Manager or similar third party policy managers, and federation of security tokens is also supported. This support is WS-Trust and WS Federation standards compliant. The XS40 also offers Public Key Infrastructure (PKI) and FIPS 140-2 Hardware Security Module (HSM) support.

XML and services security support includes XML validation, encryption and digital signature, with security at both XML field and message-level. The XS40 embraces WS-Security and WS SecureConnection, and can handle Kerberos, RADIUS, LDAP, Microsoft Active Directory, XACML and SAML queries. Specifically for web services, the XS40 implements standards based security compliant with a wide range of WS-* industry standards.

The XS40 has a wide range of options for policy management and enforcement. While simple proxy functions can be built with the Web GUI, the XS40 also supports the use of more sophisticated policies that can control access to applications, services and data. These customizable policies can be role-based, and the XS40 also allows integration with other policy managers and service registries that support WS-SecurityPolicy and WS-Policy. Service-level monitoring is also supported, for instance by traffic type, user class or identity.

In terms of simplification, one of the strengths of the DataPower range is its breadth, with appliances available for a number of different needs such as security gateway, B2B and file transfer gateway, ESB and low latency messaging. Combined with XML and non-XML processing efficiencies, this provides lots of opportunities for functional consolidation and simplification. Apart from this, the single point of management control provided through a web GUI offers a comprehensive set of administrative and monitoring capabilities, such as policy management, service level management, logging and alerting. SNMP support is also included, allowing alerts to be shared with enterprise management frameworks.

IBM DataPower SOA appliances all offer comprehensive hardware acceleration. XML Parsing, XSLT, XPath and other XML operations are carried out at close to wire speed, and a range of XML processing options are also supported including XML pipeline processing, compression and caching. But the DataPower range does not focus solely on XML processing acceleration; there is hardware acceleration for other formats too, such as non-XML / XML transformation, and hardware assistance is also provided for cryptographic operations such as encryption / decryption and digital signature handling. A full range of processing statistics is provided, including throughput rates, transaction counts and errors.

In general, the DataPower range is well integrated with general purpose solutions to aid processor offload scenarios. In particular, the XI50 provides full ESB support, making it easy to hook the DataPower appliances into just about any general purpose system.

Value Add functionality

The entire DataPower range features broad support for industry standards. This makes it much easier to integrate appliances with other third party offerings, such as identity managers or registries, and is one of the main reasons why there are so many deployments of DataPower in non-IBM environments such as Oracle, SAP and webMethods. The tooling for DataPower appliances is in the form of Eclipse-based web GUIs, although the command line interface is also supported. IBM has attempted to remove as much of the installation and configuration tasks as possible. For example, the XA35 is designed to drop in to an existing environment with minimal configuration required. The result is a substantial reduction in implementation and support effort.

The IBM WebSphere DataPower range is well integrated with other management and monitoring environments, both IBM's own Tivoli enterprise management framework and leading third party offerings. Audit facilities are built in, but information can also be shared with third party tools to make administration and management easier. In the security areas, administration is made easier with support for such facilities as single sign-on.

The breadth of the DataPower range, spanning security, high-speed XML, non-XML and message processing, B2B and ESB needs, significantly enhances its flexibility and applicability. In particular, the XI50 hardware ESB offers considerable value-add for SOA deployments, extending the advantages of a hardware appliance throughout the SOA network. While there will be situations where organizations will want to stay with a software ESB implementation, the XI50 is an attractive option for consideration, with a particular strength being its ability to speed up not just XML processing but non-XML too.

The XB60 B2B gateway may also appeal as a packaged way for delivering connectivity to business partners. It offers a secure B2B and file transfer gateway combining all the advantages of a secure gateway that insulates the enterprise from the partner systems and specific B2B functionality such as partner profile management and support for B2B messaging protocols and formats such as EDIINT. It also has other useful B2B functions such as a facility for storing and viewing transaction information, and even the capability to resend transactions if the partner has had a problem.

One added value option IBM offers for the DataPower range is the Application Optimization (AO) option. This is a powerful feature that enables the appliance to manage workloads dynamically and evenly, improving performance, reliability and resource efficiency. The principle is that just speeding up performance of one part of the SOA infrastructure, such as XML processing, does not address overall end-to-end performance and can even cause problems through shifting bottlenecks further downstream and thus overloading other parts of the network. The AO option allows a level of load balancing and throttling at both the front end and back end of appliance operations. So, incoming traffic can be queued or rejected based on current loads, while back end functionality can be routed based on a dynamic determination of the target with the most capacity.

On the upgrade side, one question often asked about appliances is what happens when you need a bigger or more technically up-to-date box. IBM offers regular in-place firmware upgrades to keep the technology current, while clustering support makes it a relatively straightforward task to add another DataPower appliance for more processing power.

One of the strongest points for IBM comes from its industry-leading experience with both SOA and appliances. Because IBM has been in the SOA game for a long time, it has built up extensive and pervasive SOA skills globally, which can be a great help when advising users on how to get the most out of SOA appliances. While areas such as XML security gateways may be on the fringes of this SOA knowledgebase, an appliance ESB is very much right in the middle. IBM's experience with ESBs as part of an enterprise-wide SOA infrastructure should be particularly helpful to users looking to deploy the XI50. On the appliances side, through its DataPower acquisition and subsequent market success, IBM has developed a solid business approach to the appliance marketplace, taking into account the challenges of adding new members to the range, maintaining a consistent focus and ensuring clients continue to get ongoing value. And on top of this experience in both SOA and appliances, IBM's decision to adhere to standards where possible helps to reduce user skills requirements.

Intel SOA Expressway

Background

Back in 2000, a Chicago-based start-up called Sarvega was born, based around the idea of providing security gateway appliances. As XML grew in popularity, Sarvega started to invest in building XML gateway appliances instead. A critical point for Sarvega was that unlike a number of other companies looking at XML and related web services needs, such as Cisco, Sarvega based its own solutions on general-purpose chipsets. Its idea was to remain agnostic to the chipset but to use smart architecture and techniques to deliver efficiency.

Intel became an investor in Sarvega, and in 2005 it decided to acquire the company. There were a number of conflicting reasons offered for this move including a claim that Sarvega had run out of money, hotly denied by Sarvega management. However, the truth of the story is probably that as Intel noticed other suppliers working on specialized chip-sets for networking, security and XML processing needs, it wanted to bring in a solution that it could lock into its own chipsets. Sarvega has now been recast as the Intel SOA Products division of its Software and Solutions Group (SSG), and the key deliverable is now Intel SOA Expressway, a software-based XML and security gateway designed to only run on Intel's latest Xeon multi-core servers.

What is Intel SOA Expressway?

Intel describes SOA Expressway (SOAE) today as an SOA 'software appliance' or soft appliance. As such, SOA Expressway is a software product that has been designed to run on any Intel Xeon Multi-Core server. Unlike a hardware appliance, SOA Expressway requires a general purpose operating system, with supported ones being Red Hat or SUSE Linux and Microsoft Windows 2003 Server. Since SOA Expressway is a single software package, manageable through a web interface, Intel claims that it is a software appliance, in that it can be administered and managed just like an appliance which is of course a single unit.

This idea of a soft appliance is controversial. Some agree with Intel that because SOAE is designed to be managed as a single unit, and carries out some of the functionality offered by other SOA appliances, then it can be classed as an 'appliance', or more correctly a 'soft appliance'. Others would say that SOAE is simply a software package, albeit one that has been designed to offer similar functionality to SOA appliances. Certainly, if one of the key performance benefits of a hardware appliance is that they are able to bypass layers of operating system software, then such a software appliance that runs on top of a general operating system starts with a performance disadvantage. This will be discussed further in the assessment section.

Basic SOA Appliance functionality

Functionally, however, Intel claims that SOAE delivers most, if not all, of the basic SOA appliance functionality. Because it is a single package, and can be configured to handle all incoming and outgoing traffic, it can offer single point of control and management capabilities. It also contains security software to handle areas such as user authentication, service authorization and threat protection, and its software has been designed to take maximum advantage from Intel Xeon multi-core processors to deliver optimum performance.

On the security front, much of the functionality has been inherited from the original Sarvega security gateway. So, Intel Expressway offers XML Firewall protection covering threats such as Denial of Service, XPath injection, Schema poisoning and many more. At the level of authorization and authentication, support is based around standards such as X.509 and SAML. In terms of communications security, SOA Expressway has once again followed the standards-based path with support for SSL, WS-Security and W3C XML encryption / signatures. Optionally, a range of cryptographic solutions for key handling can also be supported. It is worth noting, however, that because SOAE is just a software package running on a traditional operating system, it does not include any special high availability support or benefit from the added robustness of a hardware appliance.

In terms of single point of control and management, Intel SOAE offers runtime policy enforcement through the use of an embedded mediation engine that supports policy definitions in XML format and applies them in runtime service flows. These policies are limited to basic needs such as encryption, authentication and security.

More advanced governance facilities are theoretically possible through the mediation engine's support for native XML definitions, but this would require other governance components to work with policies in this format. Mediations are developed using an Eclipse-based tool.

Apart from policy handling, SOAE also offers a range of other management and monitoring facilities, although at a fairly basic level. Functions offered include message throttling and support for differing qualities of service. There is a web-based monitoring tool together with a dashboard view that can manage a single SOAE or an SOAE cluster. Primitive scripting support is available through a command-line interface. There is also SNMP support to allow interaction with other monitoring frameworks. Logging is to XML-based log files.

Performance is perhaps the most intriguing area, with most people instinctively believing that dedicated hardware will always beat even the fastest software. Intel claims that SOAE is actually 1-2 times faster than hardware XML accelerators. Intel's performance claims are based around the lightweight design of its SOAE mediation engine together with XML processing that employs an efficient binary representation which scales by leveraging Intel's own Multi-Core architecture. The claim is that this allows Intel to execute XML operations and mediation services such as XPath evaluations and XSLT transformations 'at wire speed'. However, in order to deliver this heightened level of performance, SOAE requires Intel Xeon multi-core processors in order to optimize its XML processing design. The net effect as far as Intel is concerned is that SOAE's SOA-specific design and processor utilization deliver the same or better levels of simplification and performance as hardware appliances.

Value-add areas

One area of added value offered by SOAE is nothing to do with the functionality, but instead relates to the fact that this functionality is delivered as software. This means that SOA architects and developers do not need to get used to using hardware appliances, but can instead stay within their familiar software environment. It also means that if problems appear, then the software can be relatively easily patched, but of course this is one of the reasons why a software implementation is by its very nature less secure and robust.

In the ease-of-use and management areas, Intel offers an Eclipse-based tool for defining applications, and this also supports testing in a single environment. Integration with enterprise management frameworks is achieved through SNMP support that allows alerts to be passed on. The web user admin interface can support individual SOAE implementations or multiples as a single cluster.

One feature that Intel is keen to stress is that it offers opportunities for third party exploitation through an optional JVM for AXIS2 and JBI-based services. Intel hopes that other vendors will support SOAE as a deployment platform, and Oracle has already taken advantage of this opportunity, implementing its own ESB on an Intel SOA Expressway base.

Finally, because SOAE is a software implementation of appliance functionality running on general purpose hardware, it offers other deployment options. One of the advantages of running on a general purpose platform is that if additional SOAE capacity is required, the current hardware platform can be easily upgraded. Alternatively, if a cluster of platforms are running SOAE and they are providing excess capacity, it is simple to remove a server and repurpose it. SOAE can also be deployed in a virtualized environment through its support for VMWare ESX. However, since SOAE's performance claims are based around use of a specific platform, namely Intel's Xeon multi-core technology, it is likely that any benefits of virtualization would be severely limited.

However, a major drawback for Intel is that it is not a specialist in the SOA field, and does not have extensive understanding of SOA in general. Users must therefore rely to a large extent on their own experience and understanding with SOA if they decide to use Intel SOA Expressway.

Layer 7 SecureSpan SOA Appliances

Background

Layer 7 Technologies was founded in 2003 to deliver a range of XML security gateways. The first delivery was an XML firewall, followed by a whole range of security and governance related gateways. As terminology has changed, Layer 7 has moved away from the 'gateway' positioning, and now describes itself as selling SecureSpan XML or SOA appliances designed to handle SOA, web services and Web 2.0 needs. Right from the start, the Layer 7 strategy has been to deliver appliances with pre-packaged software, following the standard gateway / firewall model. The key needs being addressed were to provide the additional security-based confidence of an appliance for use in the DMZ, and to concentrate the functionality into a specialized server to simplify XML implementation, reducing administration and management costs.

More recently, Layer 7 has stretched its product line to include Cloud Computing as an application area, once again in the gateway mould. It has also started to add some level of hardware implementation for things like XML processing through the use of application-specific integrated circuits, although most of its offerings are still software running in the appliance and not firmware engineering.

What is in the Layer 7 SecureSpan XML appliance range?

Before looking at the appliances that make up the SecureSpan range, there is a general point that needs to be cleared up to avoid confusion. Layer 7 creates some of this confusion by sometimes referring to its products as XML appliances, and sometimes SOA appliances. In reality, this shift in emphasis is simply marketing positioning, designed to ride the higher value wave of SOA rather than the more technical XML message. The fact is that everything about the SecureSpan range is geared to XML processing. Layer 7 forms the link to SOA by pointing out the XML handling serves overall SOA and web services needs, which it does of course. But this is the limit of SecureSpan's contribution to SOA. So, for example, Layer 7 has made no effort to deliver appliances with broader SOA infrastructure functionality.

Layer 7 offers a range of XML appliances covering areas such as XML Security Gateway, XML Acceleration, XML Firewall and more. The majority of products are hardware appliances pre-loaded with software or sometimes additional firmware acceleration as well. There is also a software appliance particularly for use in a virtualized scenario, and a software package for standard UNIX or Solaris environments – mimicking to a certain degree the Intel software appliance approach. The range of offerings is illustrated in the table below.

Layer 7 SecureSpan XML Appliances	Description
XML Network Gateway	WS-Policy based SOA/web services policy management and run-time enforcement across domains
XML Firewall	Centralized authentication, authorization and audit for SOA services across domains
XML Data Screen	Protection from XML-based threats and intrusion
XML Accelerator	Offloaded and optimized XML processing – eg parsing, transformation, validation, etc
XML Virtual Appliance	A software appliance implementation of the other SecureSpan XML appliances that can run on commodity hardware or virtualized platforms

Figure 4: The Layer 7 SecureSpan XML appliances

One observation is that although Layer 7 now refers to its appliance family as 'SOA appliances', they are actually all focused on XML. While this does not mean they are not relevant in SOA terms, it does point to Layer 7's background in XML rather than SOA, which in turn explains why the range has not been broadened to handle wider SOA needs.

The first four offerings form the foundation of the Layer 7 SecureSpan XML appliances family. The XML Network Gateway handles the policy management and enforcement needs, acting as a central enforcement point. XML Firewall provides the identity management, authentication and authorization services for the SOA or web services deployment, while XML Data Screen specifically watches for XML-based threats from the outside just as a regular firewall does for non-XML network transmitted ones. Finally, the XML Accelerator is the hardware-assisted XML processing optimization appliance used to either offload heavy-duty XML processing and/or deliver higher performance. In terms of packaging, the SecureSpan XML Networking Gateway is the all-round offering, supplying the policy-based governance support as well as a subset of the security functionality offered by the SecureSpan XML Data Screen and XML Firewall. SecureSpan XML Data Screen offers full function threat screening and protection, while SecureSpan XML Firewall provides the top level of XML and web services security.

Basic SOA appliance functionality

Looking at the threats side first, the XML Data Screen is specifically designed to cleanse XML traffic of threats, vulnerabilities and unauthorized content. Most common XML message formats are covered, including SOAP, REST, AJAX and Plain Old XML (POX). Policies can be set up to remove, block or transform inappropriate or illegal content. This XML content filter can also restrict or throttle traffic flow based on these same policies. Beyond this, the XML Data Screen also protects from malicious actions such as XML Denial of Service attacks.

More traditional XML / web service security is provided by the SecureSpan XML Firewall, spanning identity management, authentication, authorization, privacy and integrity. The XML Firewall has its own identity store, but also integrates with many other identity and access management systems such as IBM Tivoli, CA SiteMinder, LDAP and many more. Credential sharing provides federated identity capabilities, while there is strong support for SAML, keys and certificates. Key storage, encryption and signing operations can be handled through Federal Information Processing Standards (FIPS) 140-2 certified hardware in the appliance, or through an external module. A wide range of WS and WS-I security standards is also supported.

Layer 7 appliances are all designed for high availability and robustness, making use of dual power supplies and mirrored, hot-swappable drives. Appliances can also be clustered for failover support. In addition, the administration tool enables configuration files and policies to be backed up centrally, and then remotely restored in a disaster recovery scenario.

Application services governance is addressed with the SecureSpan XML Networking Gateway, which provides policy-based control based around security, compliance, SLAs and quality of service. Layer 7 offers both policy management facilities and also policy run-time enforcement through the SecureSpan XML Gateway. In particular, the support for throttling ensures that back-end services are not overwhelmed, and can be controlled with parameters such as time of day, quotas and per-user limits. Policies are created with a graphical policy editor tool based on the WS-Policy standard, and can be updated live across single appliances or clusters.

In terms of simplification support, the Layer 7 appliances claim to provide highly optimized XML parsing and processing as well as the option of hardware-based acceleration, resulting in consolidated XML handling to reduce the number of servers. However Layer 7 appliance functionality is basically limited to security, policy-based control and acceleration. It does not offer appliances with broader SOA infrastructure functionality.

On the performance side, all Layer 7 SecureSpan XML appliances offer optimized XML processing, but the specialized SecureSpan XML Accelerator is required to deliver the highest levels of performance. The XML Accelerator has a number of ASIC-based hardware accelerators for complex XML operations as well as the option of adding a hardware security model for SSL/crypto acceleration. Multiple XML Accelerators can be clustered, and managed from a single point or remotely. Message throttling support is available to control incoming message loads and avoid backend systems becoming overloaded, although there is no companion functionality for dynamically balancing loads across back-end systems apart from basic mechanisms such as round robin. Processor offloading is also enhanced by support for the standard communications mechanisms such as JMS and WebSphere MQ, assisting in the interoperation with legacy environments.

Value-add areas

Layer 7 SOA appliances all pay close attention to standards, which improves usability. The tools are graphical and cover not just configuration options and policy management, but also comprehensive monitoring and management support through the Layer 7 Enterprise Service Manager. This centralized tool can manage all Layer 7 appliances and clusters, and provides a range of reports and dashboards reflecting both current operations and historical performance data. It can monitor entire installations or individual services, reporting on such elements as service performance, policy violations and SLA conformance. It is also the central point for policy management, providing policy organization and views for management and the ability to roll out policies across any or all appliances.

There are no specific Layer 7 SOA appliance for additional SOA functionality – as noted earlier, Layer 7 is focused on XML rather than wider XML needs. However, Layer 7 does support a range of deployment options. While the hardware appliance is the standard form factor, Layer 7 also provides its appliance functionality in 'soft appliance' form, ready for virtualization with VMWare; as a software package for running on a regular Linux or Solaris server; and as an Amazon Machine Image (AMI) for running with the Amazon EC2 Cloud.

Layer 7 offers a number of aids to speed up time to value. For a start, it offers a range of out-of-the-box policy assertions, providing a sound base for users to customize to meet their own needs. It also offers an SDK for specifying unique policy requirements which is especially useful for partners. As an example, the SDK has already been used to provide custom policy assertions that work with a set of third party identity management products from companies like Sun, IBM, CA and Oracle.

On the skills and support front, Layer 7 has a lot of experience in the security area. Customers can expect help and assistance in planning this side of the solution implementation, in areas such as identity and policy management and the various security-based standards. However Layer 7 does not have the same extensive pedigree on the SOA side. It is extremely well versed in handling XML, but the bigger questions of broader SOA architecture tend to fall outside its skills domain.

SOA appliances – Competitive assessment

Having summarized the offerings from the three vendors under consideration, it is now possible to assess them against each other, in competitive terms. In order to make this assessment as relevant as possible, the basis will be the most common user-based drivers for adopting SOA appliances, namely:-

- Improve SOA performance/predictability/resource usage
- Enhance SOA security and governance
- Reduce SOA complexity / total cost of ownership (TCO)

Of course, prospective buyers of SOA appliances are often looking to enjoy a combination of these three benefits, and may have other aims too, but these are the most commonly found drivers. On this basis, the competitive assessment is grounded around these three areas.

Improve SOA performance/predictability/resource usage

Setting the scene

These three benefit areas are combined because they are all interlinked. Improving performance is part of using resources more efficiently, and the two combine to help avoid load-related response time issues. Essentially, however, underpinning this benefit area is better, smoother and more cost-effective performance. But there is an important point to note here – SOA performance is NOT just about making the XML processing faster. There are plenty of examples where organizations have decided to implement hardware acceleration for XML processing only to find that end-to-end performance across the SOA infrastructure does not achieve the desired goals.

The reason lies in the fact that it is the end-to-end performance that matters; that is, the perceived response profile experienced by the user of the SOA-based application or service. As a simple example, it might seem obvious that if XML parsing and transformations are speeded up, then response times will improve. But if the rapid processing of the XML simply shifts the bottleneck further downstream towards the backend systems, then the result will be unpredictable performance that might sometimes be quicker but might also clog up or even cause the desired service to fail. For the best results, it is necessary to focus on the overall performance picture. This will involve throttling the front end work submission, processing XML activities faster and then ensuring the backend servers are used to maximum XML processing efficiency by load-balancing across them.

Of course there may be specialized performance issues to be addressed. As mentioned earlier, for instance, there are some applications such as algorithmic trading in the finance industry that demand the lowest possible messaging latency. In this scenario, the end-to-end performance issue is thrown to the user to solve, but the specific need for ultra-low latency may be addressed by hardware implementations, highly optimized software or a combination of the two. But these specialized cases are the exception rather than the rule, and may not even fall into the SOA category.

The link to efficient resource usage relates to more efficient processing, and the flexibility to use more cost-effective processing power where possible. Many IBM mainframe users struggle with the demands of XML processing in an SOA environment because mainframe data-flows do not natively use XML, and therefore everything has to be transformed constantly from non-XML to XML and back. The situation is made worse by the fact that these same users are always keen to keep precious mainframe processing power for the things that absolutely must run there. Some data centre staff talk of there being ‘Smart MIPS’ and ‘Stupid MIPS’ to

delineate between workloads that need the smarts of the mainframe and those that could run anywhere without a loss of service quality. In this terminology, XML processing is definitely in the 'Stupid MIPS' category; it is mechanical, repetitive and processor-intensive. Another example is cryptographic processing, a heavy drain on processor power that is ideally suited to hardware acceleration. Functionality to allow these MIPS to be offloaded as transparently as possible while also ensuring that performance and efficiency is such that the number of offload devices is limited is highly desirable.

Competitive assessment

Perhaps the purest performance driver for an SOA appliance is the requirement for high-speed messaging that can overcome current performance restrictions. This is a small niche in the market, and only just squeezes into the overall SOA category, but it is an area where certain users have an immediate need for a solution. Because it is such a specialized market segment, vendors like Layer 7 and Intel do not even have offerings in this area. The only one of the three vendors under consideration that does specifically respond to this need is IBM with its IBM WebSphere DataPower Low Latency Messaging XM70 offering. Admittedly this is the one area that TIBCO does play in, with its implementation of TIBCO Rendezvous in hardware, but since TIBCO does not offer any other SOA appliance functionality it is outside the scope of this report.

IBM's XM70 is based on the IBM MQ LLM (Low Latency Messaging) offering, but it can also support different messaging protocols and environments such as TIBCO Rendezvous and EMS, WebSphere MQ, JMS and HTTPS. This makes it very flexible for serving a variety of low-latency messaging needs. On top of this, the XM70 does not limit its support to delivering faster message response time but also has sophisticated congestion and traffic rate control to provide a more consistent, predictable level of overall performance. On this basis, the obvious conclusion is that for high-speed messaging needs, IBM is the only one of the three vendors being considered to offer a viable low-latency messaging solution.

In the more general market for SOA appliances, Layer 7, Intel and IBM all have performance functionality. Frequent performance claims are made showing how each vendor can outperform the other. Perhaps the first observation to make is that by choosing a 'soft appliance' route, Intel's SOA Expressway can never put instructions into hardware by definition. However, Intel has tuned the software as closely as possible to its Xeon multi-core processors, and has also come up with a highly optimized XML processing architecture. As a result it claims a level of acceleration at the 'pure' level of XML processing execution.

In contrast, both IBM and Layer 7 have combined optimized XML processing approaches and hardware acceleration in their SOA appliance ranges, giving them both strong XML processing figures. Indeed, it is interesting to note that while Layer 7 has taken a similar route to Intel in optimizing XML processing in software, it still built hardware acceleration for the most demanding performance needs, and this is an option that will never be open to Intel with its 'soft appliance' model.

In simple XML deployments, the differences between these three offerings may be relatively small, with performance claims being highly dependent on test system configuration and task complexity. But in these simpler cases, it is unlikely that the prospective SOA appliance buyer would be focused on super-fast performance anyway. In the more extensive SOA deployments, however, the end-to-end performance picture is likely to be the real concern, with users looking for increased capacity with faster response times and predictable results. This swings the focus onto the added value capabilities built around the core XML processing acceleration.

In the case of the Intel SOA Expressway (SOAE) soft appliance, the Intel performance claims are based around three points; the speed of the optimized SOAE XML processing design, the fact that SOAE includes a mediation engine as well, to speed up the whole XML traffic handling exercise, and the ability to scale up the SOAE server as required. This last point is the most relevant, picking on one potential weak spot of a hardware-based appliance. If software is struggling, it is relatively easy to wheel in a bigger server for it. Upgrading the power of a hardware appliance is not quite as simple, although since most hardware SOA appliances support clustering it

is still only a matter of adding another server. However it must be remembered that in the case of SOAE the required server environment is not just any general purpose server, but must be a Xeon multi-core system, so the result is the user may well be forced into another hardware acquisition anyway.

Apart from this point, there is nothing stunning about the Intel performance picture – even Intel itself only claims speeds of 'one or two times faster than hardware appliances' and to be honest, performance claims are often highly artificial. Regardless of Intel claims, the simple fact is that with the best design in the world, software can NEVER run as fast as hardware – it is just a physical impossibility. A software instruction running on a general purpose operating system cannot compete with an electrical signal on a wire. But the real problem is that SOAE does not pay much attention to the wider end-to-end performance issue. While there is some basic throttling for incoming messages based on quality of service parameters, there is little dynamic performance and workload management support. This is not really too surprising, because of course Intel does not have extensive experience with SOA deployments. And of course, in terms of providing a reliable level of performance, the SOAE software implementation does not have the same ability to build in the levels of hardware redundancy that the other appliances offer, resulting in a lower level of availability. The only hardware option it does exploit directly is use of hardware-accelerated cryptography.

The Layer 7 SecureSpan XML Accelerator's support for faster XML handling, through its use of ASICs and an optimized design for XML processing, generates some reasonably impressive performance figures, although once again vendor-published figures never offer the most balanced of pictures. One source of XML processing speed is the hardware-assisted support the XML Accelerator offers for message searching, element detection and filtering. The clustering support, all managed as a single entity, offers a level of scalability to support increasing capacity demands, and the appliance also offers some limited caching facilities. The inclusion of automated failover support across the cluster also improves service reliability. All of this functionality ensures that Layer 7 can offer a good story on straight XML processing. However, it has also given at least some attention to the wider performance issue, supporting throttling of incoming requests to avoid overloading backend systems and providing some rudimentary, if rather static, load balancing options to improve the efficiency of back end resource usage. On the offload side of the performance equation, Layer 7 SOA appliances can interoperate with WebSphere MQ and any JMS-compliant ESB, and as far as reliability is concerned all Layer 7 SOA appliances support redundant hardware and mirrored files.

The IBM response to performance requirements is built around the hardware acceleration provided to the whole range by the XA35, and also the broader capabilities of the XI50. The DataPower range therefore combines smart XML processing design and hardware circuits to deliver rapid and efficient XML processing. As well as handling XSLT and XPath operations optimally, the IBM support for XML pipeline processing, caching and compression all add to the overall processing efficiency. In fact, IBM has even developed its own XG4ng chipset specifically for optimized handling on XML needs. Outside of specific XML processing needs, IBM's DataPower appliances also offer other significant advantages, such as hardware support for encryption/decryption operations, digital signature handling and SSL processing. But it is the Application Optimization option that is the real differentiator at this level, especially in terms of end-to-end performance. This ability to handle both the throttling of incoming messages and dynamically load-balance work over the back-end systems delivers not just a strong XML processing story but also a smooth, consistent and predictable quality of service.

On top of this, the ESB implementation in the XI50 provides another boost to processing efficiency, particularly since it allows offloading of not just XML processing but also ESB operations, and the connectivity brought about by using ESB technology makes the XI50 relatively easy to include in a wide range of technical environments. An important advantage of this approach is that the XI50 offers performance acceleration not just for XML processing, but for non-XML formats too. A common requirement in an ESB deployment is to support transformations of non-XML formats into XML and back again. These transformations can be extremely complex, and the ability to accelerate them is very welcome. Most other SOA appliances speed up the XML handling but do nothing for the wider processing needs, weakening their SOA performance story considerably.

Enhance SOA security and governance

Setting the scene

Most SOA infrastructures have reasonably strong support for security, and many also offer governance options for controlling the creation, deployment and operations of SOA services. However, the perceived exposure is not so much the internal SOA network but rather the touch points between the network and other domains, such as other departments, partners or the internet. As SOA becomes more and more important, and connectivity becomes more and more ubiquitous, organizations start to worry a lot more about exposure to hackers or other external sources of threats, and whether everyone is following the agreed corporate policies as traffic flies around the SOA network. In particular, organizations often worry about putting software out in the DMZ – the view is that if you have to put a security gateway out there, it should be tamper-proof hardware and not easy-to-get-at software. Problems can arise from non-malicious SOA services too. Popular services that are accessed by many systems can also negatively impact end-to-end SOA performance. A means to detect excessive usage and to then govern access to such services is needed to ensure performance is maintained and SLAs are met.

Competitive assessment

The Intel SOA Expressway 'soft appliance' contains comprehensive threat identification software to handle XML-borne threats coming in from external sources, and also has the full range of authentication and authorization features with general adherence to industry standards such as X.509 and SAML. It also works with CA Site Minder and Oracle Access Manager. The built-in service mediation engine provides the basis for the SOAE policy management and enforcement. However, the issue for SOAE in terms of security is not so much a functional one as an emotional one. In the end, there is no getting away from the fact that SOAE is software, running on a general purpose operating system in a 'standard' server environment. With the best will in the world, and the best security software, many organizations will not accept that this form factor can possibly have the same tamper-proof, hardened security characteristics as a physical appliance. Indeed, some organizations operate a policy that forbids the use of general software in the DMZ, insisting that all functionality there is hardware appliance based. For example, the defence industry often demands all systems to be hardened from top to bottom before deployment in the DMZ, and this is a challenge that the Intel soft appliance approach would be totally unable to meet.

Security is where Layer 7 started out, and as a result the SecureSpan range delivers strong security functionality. The threat screening offered by SecureSpan Data Screen ensures that all XML traffic entering the network has been cleansed, and also protects from a wide range of malicious XML-based attacks. SecureSpan XML Firewall's support for identity management, authentication, authorization, privacy and integrity is heavily standards based, leveraging the appliance's own identity store although third party ones are supported too. All aspects of security from key handling to credential sharing are covered, and all in a hardened, highly available, tamper-proof hardware form factor. Policy management and enforcement is handled by the SecureSpan Networking Gateway, supporting policies that cover such areas as SLAs, quality of service and security requirements.

The WebSphere DataPower Security Gateway XS40 appliance provides the security and governance functionality for IBM. In essence, support covers much the same areas as the Layer 7 SecureSpan appliances, and is perhaps even more strongly wedded to standards than the Layer 7 offerings, with comprehensive support of WS-* standards as well as the more general security related ones like SAML and XACML. However there are one or two important differences. For instance, the IBM security appliance allows XML security at both message and field levels, and it has wider connectivity to third party environments than Layer 7, covering technologies such as Kerberos, LDAP and Microsoft Active Directory. Also, on the policy side, IBM's support includes the ability to define role-based policies. This provides a little more flexibility in building an effective governance solution.

Reduce SOA complexity / total cost of ownership (TCO)

Setting the scene

The issue here for many organizations is that as SOA becomes more heavily embedded in their operations, the SOA network and supporting infrastructure can expand rapidly, across many different domains and nodes. In simple terms, the SOA infrastructure becomes a collection of many moving parts – ESB nodes, XML servers, security components in servers in every domain, and so on. The SOA appliance idea produces a way of reducing the number of moving parts, enabling sets of them to be consolidated into single appliances. These appliances all look the same, have the same interfaces, and implement the same standards, and as such they make the infrastructure more uniform. The result is that as the number of entities and the extent of variations to be supported decreases, the people costs to support them falls. Putting a new appliance in place becomes a repeatable process, particularly since appliances tend to come more or less preloaded with limited customization required. Supporting functionality in one place makes maintenance cheaper and more reliable, and being able to look in one place to get a picture of system activity and performance also reduces time an effort. And there is another side effect of appliance adoption – the greater efficiency reduces the number of servers that require cooling, space and power.

This whole area of simplification with the corresponding reduction in TCO is perhaps the most powerful of all the factors driving SOA appliance purchases.

Competitive assessment

Intel SOA Expressway purports to offer consolidation of XML processing, security and governance needs, claiming that its highly optimized XML processing design combined with utilization of the capabilities of its Xeon multi-core processors deliver a level of efficiency that significantly reduces the number of servers required. This will clearly help to reduce complexity, and SOAE's close adherence to standards will improve this by bringing a level of uniformity. There is also the fact that because SOAE is just a software package running on a standard operating system, there are less new skills to be learnt to deploy and support it, which will make it instantly familiar to software architects, all of which will contribute to further lowering costs. Maintenance of software is also generally easier and therefore less costly for software than for hard appliances. Applying a software patch is always going to be easier than updating firmware, although with modern appliances these firmware updates can be done in a matter of minutes. However, with ease of patching also comes increased security risks, and there is also a cost that must be taken into account when using software loaded onto a general server. For example, when deploying this to remote locations, it is difficult to be sure that the same software configuration options are taken.

In comparison, the hardware appliance offerings offer a much stronger level of uniformity, with less opportunity for unauthorized or accidental change. Deploying a hardware appliance is almost a matter of wheeling a box into the new department, cabling it up and plugging it in, and with clustering support it is just as easy to upgrade processing capacity by adding another appliance. Remote management is pretty standard for SOA appliances, removing any need for customization from the local team.

Layer 7's SecureSpan SOA appliances offer additional advantages in reducing support work. For instance, the configuration information and policies can be backed up locally and then restored remotely in a disaster recovery scenario. In addition, Layer 7 has the Enterprise Service Manager which not only provides a graphical environment for specifying configuration options and policies, but also offers comprehensive management and monitoring support from a single point of control for all Layer 7 SOA appliances. The pre-supplied dashboards and reporting facilities combined with monitoring all the way from individual services to entire installations make the support task much easier, reducing costs further. The out-of-the-box policy assertions also reduce implementation effort. At a more general level, SecureSpan offerings enable simplification due to consolidation of security functionality in one gateway, and the greater efficiency from the optimized XML processing that reduces the number of servers required.

While IBM's DataPower range offers broadly the same sort of simplification opportunities as Layer 7, IBM has another important card to play. While Layer 7 is focused exclusively on XML processing and security, IBM's DataPower range extends appliance functionality to other parts of the SOA infrastructure such as Enterprise Service Buses (ESBs) and Business-to-Business (B2B) gateways. This extends the opportunity for simplification to a greater part of the overall SOA infrastructure. While it may not be appropriate to replace every instance of an ESB with an appliance, there are bound to be many scenarios such as edge ESB or inter-domain nodes that would benefit from the simplicity of a hardware implementation. Since ESBs tend to be quite complicated, with many options, the standardization and uniformity offered by the XI50 could significantly reduce complexity and hence TCO. Similarly, B2B is an ideal area for simplification. For example, if an SOA is being extended to a partner who is new to the whole SOA area, the appliance form factor offers a way to enable connectivity without throwing the partner a whole load of new software.

The IBM DataPower AO feature for optimizing end-to-end performance also has a contribution to make in terms of complexity reduction. As discussed previously, this capability manages performance by smoothing loads and volumes and balancing them, at both the front end and the back. The result is that IBM DataPower appliances can often reduce the need for load-balancers across the network, with a corresponding reduction in network topology and ownership costs.

Miscellaneous observations

Although the three areas outlined above are the main factors likely to be driving an SOA appliance purchase, there are other differences between the three appliance ranges covered in this review that are relevant in comparative terms. The first such consideration is the availability of SOA expertise. Anyone looking to address SOA issues, or implement a new SOA, will benefit from working with a supplier who understands SOA. SOA is a complicated concept, and because it tends to be so widespread, crossing many domain boundaries, it can be hard to appreciate all of the inter-relationships between the different parts. In this area, IBM is the clear leader over the other vendors. Layer 7's area of expertise is XML security rather than SOA in general, and Intel does not have much SOA experience at all.

Another factor to consider is the impact of virtualization on SOA appliance plans. This is an area where the hardware appliance may seem less flexible than software. Indeed, Intel makes a big fuss about the fact that SOAE, being simply a software stack, can easily be deployed in a virtualized environment with its VMware support, and Layer 7 now offers a 'soft appliance' version of SecureSpan. In fact, Layer 7 even offers a pure software stack for running on general purpose operating systems if the buyer wants it. On the face of it, these options do appear to offer flexibility, but of course some of the benefits offered by the hardware appliance will be lost. Actually, the whole premise of a virtualized appliance that can run on any hardware seems a bit bizarre. One of the appeals of an appliance is its ability to leverage hardware for performance, and even Intel's soft appliance claims performance gains by working closely with the Xeon chipset. Another is the security benefits of gathering all the functionality on a known hardware platform. By virtualizing the appliance software, it will be run on any hardware in the pool and hence all these benefits are thrown away, which seems to defeat the object of having the appliance in the first place.

Competitive summary

The table below summarizes to what extent the three selected SOA appliance vendors address the three main areas of interest for SOA adopters.

	Performance / Resource usage	Security and Governance	Reduction in Complexity / TCO
IBM	■■■■■■■■□□	■■■■■■■■□□	■■■■■■■■□□
Layer7	■■■■■■□□□□	■■■■■■■■□□	■■■□□□□□□□
Intel	■■■■□□□□□□	■■■■□□□□□□	■■■■□□□□□□

Figure 5: SOA Appliances – Competitive Assessment Summary

Conclusion

Appliances have been serving business needs for many years, particularly as security gateways in the DMZ, and now they are expanding their influence into the field of service oriented architecture (SOA). With SOA making heavy use of XML-based connectivity between different environments across the enterprise and beyond, appliances have quickly fitted in as gatekeepers to the SOA network, but have also emerged as a cost-effective and efficient means to perform the mechanical and repetitive calculations required to process XML traffic. In the former case, the hardened, tamper-proof nature of an appliance makes it an ideal security measure, while in the latter its ability to focus purely on XML processing tasks, combined with specialized hardware acceleration, enables improved performance and throughput without consuming critical processing capacity elsewhere in the enterprise. But there is another important aspect of SOA appliance usage that is not so immediately obvious. By consolidating parts of SOA processing into pre-loaded, pre-configured, uniform devices, appliances can considerably simplify the SOA infrastructure. This simplification delivers on-going benefit, reducing the cost of owning, operating and supporting an SOA implementation.

A number of vendors have stepped up to supply SOA appliances. Some have come from the appliance marketplace, while others have an SOA background. Of these vendors, three deserve closer consideration; traditional SOA vendor IBM and appliance vendor Layer 7 have both moved to deliver hardware appliances in the SOA space, while Intel has come up with an unusual software-based approach to address the SOA appliance needs. Each of these solutions has its own advantages and disadvantages, as discussed throughout this assessment, but there are a few general conclusions that have emerged.

Although TIBCO does offer a messaging appliance, its lack of any other presence in this market rules it out of general consideration as an SOA appliance vendor. The Intel option is an interesting idea, based around the oxymoron of a software appliance, and it will probably appeal to software technicians who may feel uncomfortable with an enclosed, hardware-based product, but the very flexibility it introduces based on its software approach makes it less secure and more easily compromised. In essence, the software model relies on self-regulation by the programming community, while the hardware form factor enforces regulation upon it. The software form factor also limits any opportunity to leverage specialized hardware for additional performance.

Layer 7 has a lot of experience in delivering appliances, and has a strong contender to play the role of security gateway and XML traffic manager. However the vendor is much less experienced in SOA than it is in XML, and as a result its appliances fit best in the world of XML data exchange and web services. Unsurprisingly, the most comprehensive range of SOA appliances is offered by IBM. As the leading SOA vendor, this was to be expected. The IBM range covers the same XML security and traffic management needs as Layer 7, but it also offers appliances that embody broader sections of the SOA infrastructure, thereby expanding options for simplification and cost savings.

As SOA continues to tighten its grip on the corporate IT marketplace, SOA networks will grow exponentially, with a corresponding increase in XML-based traffic passing between more and more locations and environments. SOA security and governance will become even more important, while the growing demands on the SOA infrastructure will place it under much strain, particularly in the areas of performance and management. SOA appliances form a valuable addition to the IT armoury, providing a way to secure and simplify the infrastructure while delivering greater efficiency and performance. As a result, there can be little doubt that, although SOA appliances are relatively new, they are definitely here to stay.

About Lustratus Research

Lustratus Research Limited, founded in 2006, aims to deliver independent and unbiased analysis of global software technology trends for senior IT and business unit management, shedding light on the latest developments and best practices and interpreting them into business value and impact. Lustratus analysts include some of the top thought leaders worldwide in infrastructure software.

Lustratus offers a unique structure of materials, consisting of three categories—Insights, Reports and Research. The Insight offers concise analysis and opinion, while the Report offers more comprehensive breadth and depth. Research documents provide the results of practical investigations and experiences. Lustratus prides itself on bringing the technical and business aspects of technology and best practices together, in order to clearly address the business impacts. Each Lustratus document is graded based on its technical or business orientation, as a guide to readers.

Terms and Conditions

Lustratus Research Limited
St. David's, 5 Elsfield Way, Oxford OX2 8EW, UK
Tel: +44 (0)1865 559040

www.lustratus.com

Ref STC/LR/96018175/V1.0