WebSphere DataPower Appliance
The perfect XML/Web Services security gateway for SOA

Service security, service-level management, mediation & policy enforcement

Thomas KW Poon
Advisory IT Specialist
WebSphere
IBM’s acquisition of DataPower

An SOA Appliance…

Creating customer value through extreme SOA performance and security

- Simplifies SOA with specialized devices
- Accelerates SOA with faster XML/WS throughput
- Helps secure SOA XML/WS implementations

WebSphere DataPower SOA Appliances redefine the boundaries of middleware extending the SOA Foundation with **specialized, consumable, dedicated SOA appliances** that combine **superior performance and hardened security** for SOA implementations.
WebSphere DataPower SOA Appliance Product Line

**LLM Appliance XM70**
- High volume, low latency messaging
- Enhanced QoS and performance
- Simplified, configuration-driven approach to LLM
- Publish/subscribe messaging
- High Availability

**XML Accelerator XA35**
- Offload XML processing
- No more hand-optimizing XML
- Lowers development costs

**Integration Appliance XI50**
- Hardware ESB
- “Any-to-Any” Conversion at wire-speed
- Bridges multiple protocols
- Integrated message-level security

**B2B Appliance XB60**
- B2B Messaging (AS1/AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Exceptional performance
- Simplified management and configuration

**XML Security Gateway XS40**
- Enhanced Security Capabilities
- Centralized Policy Enforcement
- Fine-grained authorization
- Rich authentication

**LLM Appliance XM70**
- High volume, low latency messaging
- Enhanced QoS and performance
- Simplified, configuration-driven approach to LLM
- Publish/subscribe messaging
- High Availability

**XML Accelerator XA35**
- Offload XML processing
- No more hand-optimizing XML
- Lowers development costs

**Integration Appliance XI50**
- Hardware ESB
- “Any-to-Any” Conversion at wire-speed
- Bridges multiple protocols
- Integrated message-level security

**B2B Appliance XB60**
- B2B Messaging (AS1/AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Exceptional performance
- Simplified management and configuration

**XML Security Gateway XS40**
- Enhanced Security Capabilities
- Centralized Policy Enforcement
- Fine-grained authorization
- Rich authentication
### IBM SOA Appliance Product Line

*Specialized network devices simplify, help secure & accelerate SOA*

<table>
<thead>
<tr>
<th>XML Security Gateway XS40</th>
<th>Integration Appliance XI50</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Help secure SOA with XML threat protection and access control</td>
<td>▪ Transforms messages (Binary to XML, Binary to Binary, XML to Binary)</td>
</tr>
<tr>
<td>▪ Combines Web services security, routing and management functions</td>
<td>▪ Bridges multiple protocols (e.g. MQ, HTTP, JMS)</td>
</tr>
<tr>
<td>▪ Drop-in, centralized policy enforcement</td>
<td>▪ Routes messages based on content and policy</td>
</tr>
<tr>
<td>▪ Easily integrates with exiting infrastructure and processes</td>
<td>▪ Integrates message-level security and policy functions</td>
</tr>
</tbody>
</table>
WebSphere DataPower Deployment Patterns

1. B2B Gateway
2. Secure Gateway (Web Services, Web Applications)
3. Trusted Domain
4. Application
5. Application
6. System z
Simplify, Integrate and Centralize Core Functions

- Centralize - Route, transform, and help secure multiple applications without code changes
- Simplify - Lower cost and complexity
- Integrate - Enable new business with unmatched performance

Before SOA Appliances

Update application servers individually

After SOA Appliances

Secure, route, transform all applications instantly
No changes to applications
Why an Appliance for SOA

- **Hardened, specialized hardware for helping to integrate, secure & accelerate SOA**
- **Many functions integrated into a single device:**
  - Impact: connectivity will require service level management, routing, policy, transformation
- **Higher levels of security assurance certifications require hardware:**
  - Example: government FIPS Level 3 HSM, Common Criteria
- **Higher performance with hardware acceleration:**
  - Impact: ability to perform more security checks without slow downs
- **Addresses the divergent needs of different groups:**
  - Example: enterprise architects, network operations, security operations, identity management, web services developers
- **Simplified deployment and ongoing management:**
  - Impact: reduces need for in-house SOA skills & accelerates time to SOA benefits
XML Security Gateway XS40

- **XML/SOAP Firewall:**
  - Filter on any content, metadata or network variables
- **Data Validation:**
  - Approve incoming/outgoing XML and SOAP at wirespeed
- **Field Level Security:**
  - WS-Security, encrypt & sign individual fields, non-repudiation
- **XML Web Services Access Control/AAA:**
  - SAML, LDAP, RADIUS, etc.
- **MultiStep:**
  - Sophisticated multi-stage pipeline
- **Web Services Management:**
  - Service Level Management, Service Virtualization, Policy Management
- **Transport Layer Flexibility:**
  - HTTP, HTTPS, SSL
- **Web Application Firewall Capabilities:**
  - Additional security proxy, threat mediation & content processing services for other URL encoded HTTP-based applications
- **Easy Configuration & Management:**
  - WebGUI, CLI, IDE and Eclipse Configuration to address broad organizational needs (Architects, Developers, Network Operations, Security)
Integration Appliance XI50

- **DataGlue “Any-to-Any” Transformation Engine**
- **Content-based Message Routing:**
  - Message Enrichment
- **Protocol Bridging (HTTP, MQ, JMS, FTP, etc.):**
  - Request-response and sync-async matching
- **Direct to Database:**
  - Communicate directly with remote Database instances
- **XML/SOAP Firewall:**
  - Filter on any content, medata or network variables
- **Data Validation:**
  - Approve incoming/outgoing XML and SOAP at wirespeed
- **Field Level Security:**
  - WS-Security, encrypt & sign individual fields, non-repudiation
- **XML Web Services Access Control/AAA:**
  - SAML, LDAP, RADIUS, etc.
- **MultiStep:**
  - Sophisticated multi-stage pipeline
- **Web Services Management:**
  - Centralized Service Level Management, Service Virtualization, Policy Management
- **Easy Configuration & Management:**
  - WebGUI, CLI, IDE and Eclipse configuration to address broad organizational needs (Architects, Developers, Network Operations, Security)
Hardware Device for Improved Security

- **Sealed network-resident device:**
  - Optimized hardware, firmware, embedded OS
  - Single signed/encrypted firmware upgrade only, not arbitrary software
  - High assurance, “default off” locked-down configuration
  - Security vulnerabilities minimized (few 3 party components)
  - Hardware storage of encryption keys, locked audit log
  - No drives/USB ports, tamper-proof case

- **Third party certification:**
  - FIPS 140-2 level 3 HSM (option)
  - Under evaluation by Common Criteria EAL4

- **Large financial and government customers**

  “The DataPower [XS40]... is the most hardened ... it looks and feels like a datacenter appliance, with no extra ports or buttons exposed and no rotating media. "
  - InfoWorld
XML Threat Protection (Built-in supported by DP)

- XML Entity Expansion and Recursion Attacks
- XML Document Size Attacks
- XML Document Width Attacks
- XML Document Depth Attacks
- XML Wellformedness-based Parser Attacks
- Jumbo Payloads
- Recursive Elements
- MegaTags – aka Jumbo Tag Names
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Message Tampering
- Data Tampering
- Message Snooping
- XPath Injection
- SQL injection
- WSDL Enumeration
- Routing Detour
- Schema Poisoning
- Malicious Morphing
- Malicious Include – also called XML External Entity (XXE) Attack
- Memory Space Breach
- XML Encapsulation
- XML Virus
- Falsified Message
- Replay Attack
Performance Cost of XML Policy Processing

- Each security function requires XML processing
- Must implement all services without any compromise
- Need ability to scale as content and user base grows

* Representative of software-based systems. For demonstration only. Actual processing time varies depending on application.
Access Control

*Enforce Who can access Which Web service & When*

- Deploy as a high-speed access policy enforcement point
- Modular authentication/authorization architecture:
  - $x = \text{extract-identity}()$
  - $z = \text{extract-resource}()$
  - $zm = \text{map-resource}(z)$
  - $y = \text{authenticate}(x); \text{if } (y = \text{null}) \text{ reject}$
  - $ym = \text{map-credentials-attributes}(y)$
  - $\text{allowed} = \text{authorize}(ym, zm); \text{if } (!\text{allowed}) \text{ reject}$
  - audit-and-post-processing();

- **Identity examples include:**
  - WS-Security user/pass token
  - SSL client certificate
  - SAML assertion
  - HTTP basic-auth
  - IP Address
  - Proprietary SSO cookie/token

- **Resource examples:**
  - URL
  - SOAP method
Access Control (2)

Leading Standards and Third-party Integration Support

- **Access control policy:**
  - On-board: certs, XML file [can start simple]
  - Off-board: external access control servers

- **Standards-based integration:**
  - LDAP (for CRL, authentication, authorization)
  - RADIUS (authentication)
  - XKMS (for CRL, authentication)
  - SAML (consume, authentication, authorization, produce)
  - WS-Security, WS-Trust, WS-*, XACML
  - Outbound SOAP or HTTP call

- **Integration with access management solutions:**
  - Tivoli Access Manager
  - Tivoli Federated Identity Manager
  - RSA ClearTrust
  - Microsoft Active Directory
  - Sun Identity Server
  - Netegrity SiteMinder
  - CA eTrust
  - …others including custom integration with any customer environment
Access Control (3)

AAA Framework Diagram - Authenticate, Authorize, Audit

DataPower AAA Framework

- Extract Identity
  - SAML
  - WS-Security
  - SSL client cert
  - HTTP Basic-Auth

- Extract Resource
  - Web Service URI
  - SOAP op name
  - Transfer amount

- Map Credentials
  - SAML assertion
  - Non-repudiation
  - Monitoring

- Map Resource

- Authenticate

- Authorize

- Audit & Accounting

External Access Control Server or On-Board Policy

SOAP/XML Message

SOAP/XML Message
MultiStep & XML Routing

Flexible Drag & Drop Message Processing and Policy Creation

- **Basic routing capability** similar to [XML Filtering](https://www.ibm.com)
- **Arbitrary steps of message processing:**
  - Encrypt, Decrypt, Sign, Verify
  - Access control, Filter, Validate
  - Route (e.g., route-set https://soapfoobar.com:321), T-Route, Rewrite, (e.g. header-rewrite X-foo (.*) now)
  - Call out or Fetch artifacts such as XSLT, XSD, XML, WSDL, etc
  - Custom error handling – create policies to respond to processing errors
  - Callable rules
  - Transform (XML or legacy data)
  - Logging – log individual transactions (including message) for analysis and archiving
  - Service Level Management – shape and monitor traffic and/or send alerts based on transactional data and context
  - XPath extract (e.g. extract INPUT three //games/url var://local/urls)

- **Full variables and state:**
  - Scope: context / session / multistep-scope
  - Accessible both in config and from within XPath
Packet Level Security vs. Application Level Security

SSL is not enough
- XML-level threats and XML-aware security
- securing stored or spooled messages
- multi-party transactions, multi-hop networks
Web Services Management

Service Level Management

- Configure and install in minutes
- Hierarchical Service Level at WSDL, service, port, operational level
- Flexible actions when reaching a threshold: notify/alert, shape, throttle
- Threshold for both overall requests and failures
- Graphical display
Web Services Management (2)

Service Level Management

- **Configure Policies:**
  - Based on any parameter: WSDL; Service Endpoint; Operation; Credential
  - Based on Rate (TPS) or Count by Time (Outlook like Calendar)
  - Based on Request; Response; Fault; XPath
  - Support for enforcement across a pool of devices
  - Action: Notify (Alert); Shape (Slow Down); Throttle (Reject)
  - Notify other applications such as billing, audit, etc.

- **SLM is a verb in the policy pipeline**
- **Support for WSDM, Web services management standards, …**
- **Allow subscription to SLM for alerts, logging, etc.**
IBM Tivoli Composite Application Manager

Simplify Web Services Management and SOA Deployment

- Composite view of both Web services and IT infrastructure
- ITCAM for SOA [Event Correlation]

Deployment Example
Event Correlation

ITCAM for SOA Dashboard
Content-based Routing Features

- Dynamically route based on context (e.g. originating URL, protocol headers and attributes, etc.) and message content (both legacy and XML):
  - XPath-based routing against any part of the message content or context
  - XPath statements can point to dynamically set URLs and/or message queues (MQ, JMS)
  - Routing may be one way (a response from the service may not be necessary)

- XI50 can be configured to accept a routing table where routing parameters are supplied using XML:
  - A table results in extremely fast turnaround of routing changes, including transport protocol conversions

- XI50 can dynamically retrieve routing information from other systems:
  - Databases, web servers, file servers, etc.
Protocol Bridging

- First-class support for message and transport protocol bridging
- Protocol mediation with simple configuration:
  - HTTP ↔ MQ ↔ WebSphere JMS ↔ FTP ↔ Tibco EMS
- Request-response and sync-async matching
- Able to configure to preserve fully guaranteed, once-and-only-once delivery
Award-Winning WebGUI: Ease of Use
Configuration & Administration

Fits Into Existing Environments

- Depth of functionality to scale to full operational complexity
- Web-based GUI:
  - 100% of config exposed in both GUI & CLI
- ITCAM SE for DataPower Multi-box Management
- IDE integration:
  - Eclipse/Rational Application Developer
  - Altova XML Spy
- CLI familiar to network operators
- XPath / XML config files
- SNMP
- SOAP management interface:
  - Easy integration into home-grown mgmt systems or top products
  - Programmatic access to all status and config
- Integration For Management strategy:
  - Industry leading integration support across IBM and 3rd party application, security, identity management and networking infrastructure
Hardware Reliability

- **Dual swappable power supplies:**
  - Separate power cords, designed for high availability
- **Careful thermal design:**
  - Multiple fans & high air flow capacity
- **No hard disks or rotating media for higher reliability:**
- **Integrated failover or Active-Active self-balancing option:**
  - VRRP-like failover ensures systems defaults to redundant appliance without service interruption
- **Works seamlessly with existing load balancers, firewalls, routers and other network infrastructure**
- **No spooled application messages on device:**
  - Prevents stored message loss in the unlikely event of device failure
- **Internal self-monitoring & self-healing features**
- **Extensive utilization monitoring & alerts** (see [Configuration & Logging](#))
Security Selling Domain Topics: Physical Device Security

- With Server Appliance products, which are based general purpose computing platforms, physical device security is always a major “Achilles Heel”
  - All bets are off when I can walk up to the device and boot a CDROM or USB drive
  - Boot CDROM, peruse filesystem, install trojans, blah, blah, blah, Yippee!
- DataPower is a fully secure platform, including physical security
  - No CDROM
  - No USB Ports
  - No way to boot external media
  - All firmware is encrypted and digitally signed with the DataPower root certificate
  - There is no way to make a DataPower device run anything other than legal DataPower firmware from IBM
    - No way to run compromised, altered, or 3rd party firmware
- Critical when “locking the device in a room” isn’t possible
- Critical when you don’t trust those who do have physical access to the device
- There isn’t a single DataPower competitor that has anything close our level of physical device security – they are all based on commodity HW
Security Selling Domain Topics: Resilience to Network Attack

- Primary customer concern is the ability (or preferably inaudible) of the device to be compromised through a network-based attack.

- Network-based attacks come in multiple forms:
  - Attempts to compromise security services themselves through exploits.
  - Attempt to gain “login access” and eventually “root access” to the device.
  - Denial of Service Attacks.

- Because DataPower is not a general purpose computing platform running a general purpose operating system, it is not vulnerable to traditional network-based attacks:
  - All network services created by IBM and hardened against network-based attacks.
  - No “command shells” or “user accounts.”
  - Network services do not run in “Processes”, so there is nothing to exploit/hijack.
  - Denial-of-Service attacks thwarted at multiple layers (network, service, etc.).
  - Device threat protection prevent malformed (intentionally or unintentionally) attack data from getting through to your backend host services.
Summary – IBM SOA Appliances

- Hardened, specialized product for helping integrate, secure & accelerate SOA
- Many functions integrated into a single device
- Broad integration with both non-IBM and IBM software
- Higher levels of security assurance certifications require hardware
- Higher performance with hardware acceleration
- Simplified deployment and ongoing management

http://www.ibm.com/software/integration/datapower/

SOA Appliances: Creating customer value through extreme SOA performance and security

- Simplifies SOA with specialized devices
- Accelerates SOA with faster XML throughput
- Helps secure SOA XML implementations
Thank You