IBM SOA

DataPower SOA Appliances

Simplify, Help Secure & Accelerate SOA

Jo Torsmyr

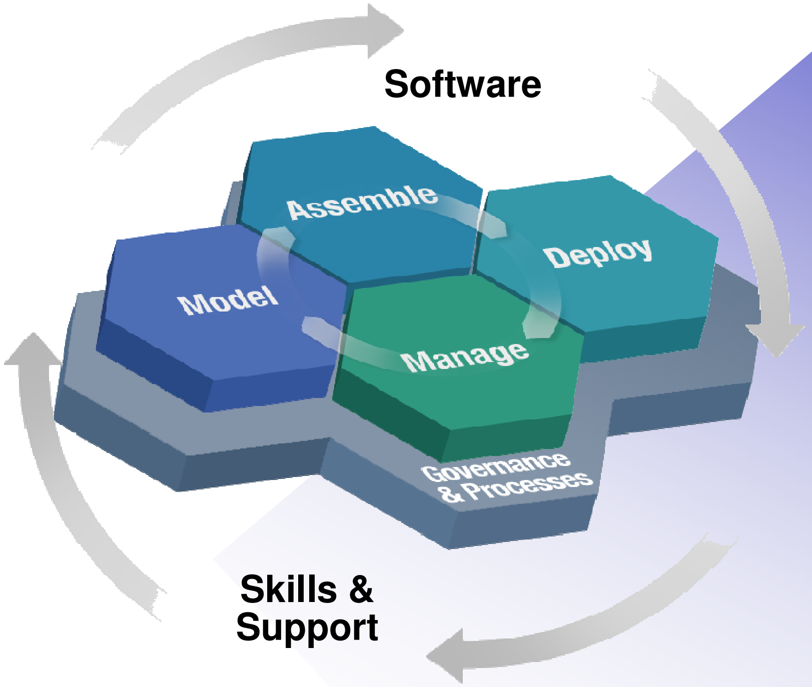
WebSphere IT Specialist

torsmyr@no.ibm.com

Agenda

- DataPower introduction
  - History & Background
  - Green, Yellow, Blue…
  - Hardware appliance – why?
  - Deployment scenarios
- Use Scenarios
  - XML Acceleration
  - Secure Gateway
  - Hardware ESB / SOA Appliance
  - Mainframe integration
  - Web Services Management
- New appliances…
- Education

IBM’s acquisition of DataPower



An SOA Appliance…

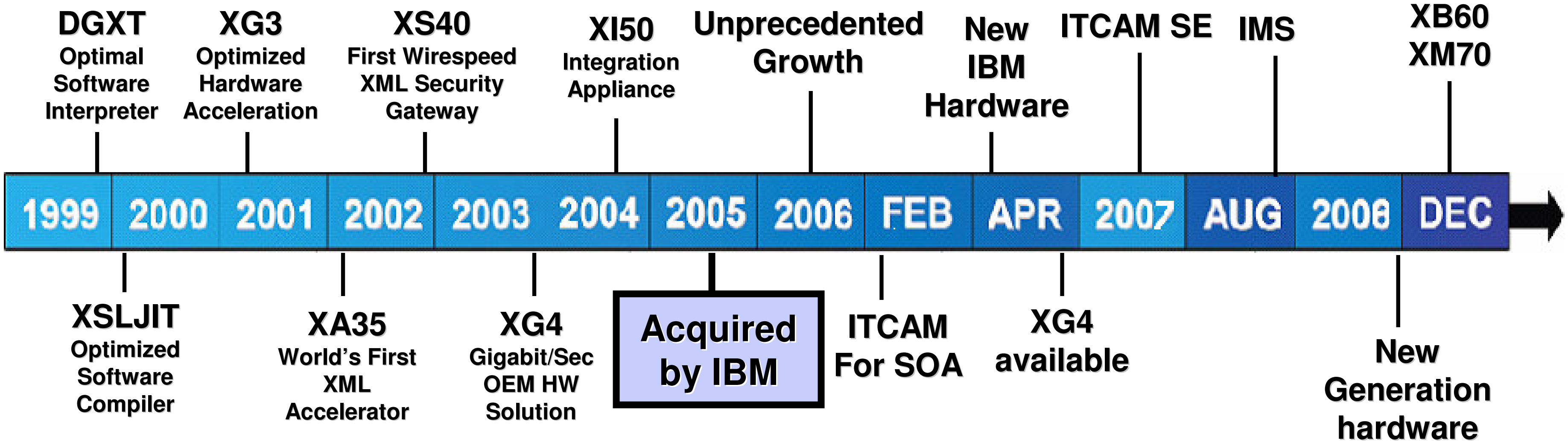
Creating customer value through extreme SOA performance and security

- **Simplifies** SOA with specialized devices
- **Accelerates** SOA with faster XML throughput
- **Helps secure** SOA XML 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.

DataPower Pre-IBM Overview

- Extensive Experience in XML Processing Optimization
- Seven Years in a Six Year Old Field
- Advantages: First to Market, Great Team, Deep Standards Involvement, Invented and Owns Core XML Technology, Comprehensive product portfolio



DGXT Optimal Software Interpreter

XG3 Optimized Hardware Acceleration

XS40 First Wirespeed XML Security Gateway

XI50 Integration Appliance

Unprecedented Growth

New IBM Hardware

ITCAM SE

IMS

XB60 XM70

1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | FEB | APR | 2007 | AUG | 2008 | DEC

XSLJIT Optimized Software Compiler

XA35 World's First XML Accelerator

XG4 Gigabit/Sec OEM HW Solution

Acquired by IBM

ITCAM For SOA

XG4 available

New Generation hardware

Post-Acquisition Innovation Continues

- 150% Staff increase / Core DataPower Leadership team Intact / Global reach and expansion
- New improved hardware platform –IBM hardware combined with DataPower technology innovations
- New capabilities – WS-*, 3rd party JMS, NFS, XG4, WSDL compiler, XACML, more…
- Continued IBM Technology Integration – ITCAM for SOA, WebSphere JMS, IMS etc.

Why an Appliance?

- **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

IBM SOA Appliance Product Line

Specialized network devices simplify, help secure & accelerate SOA

XML Accelerator XA35

- Accelerates XML processing and transformation
- Increases throughput and reduces latency
- Lowers development costs

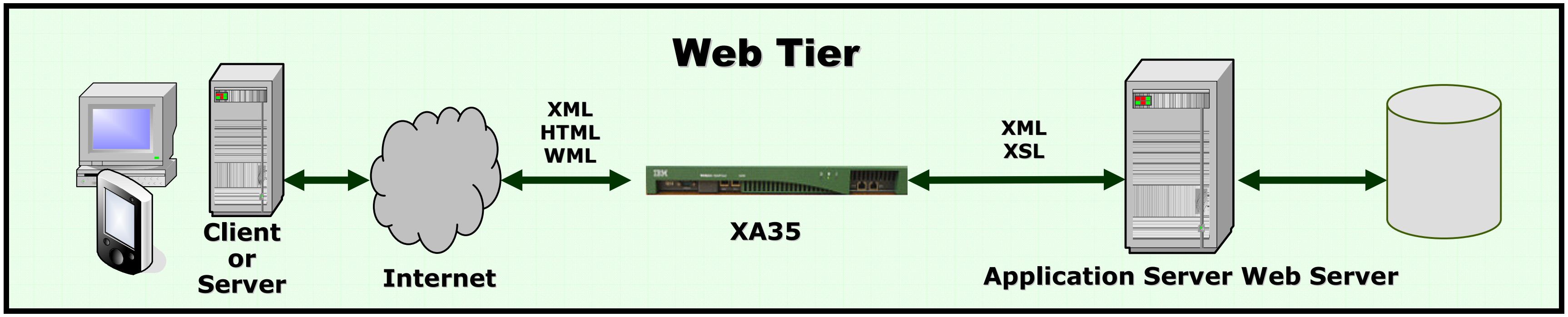
XML Security Gateway XS40

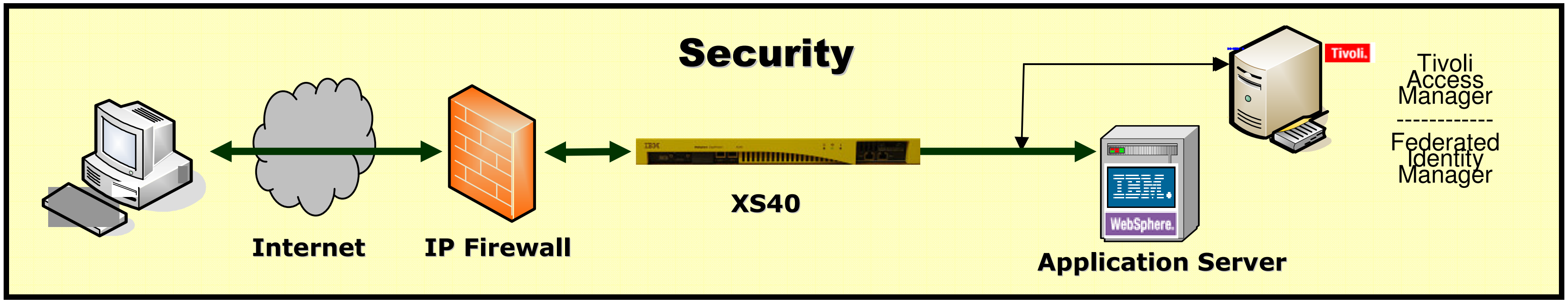
- Help secure SOA with XML threat protection and access control
- Combines Web services security, routing and management functions
- Drop-in, centralized policy enforcement
- Easily integrates with exiting infrastructure and processes

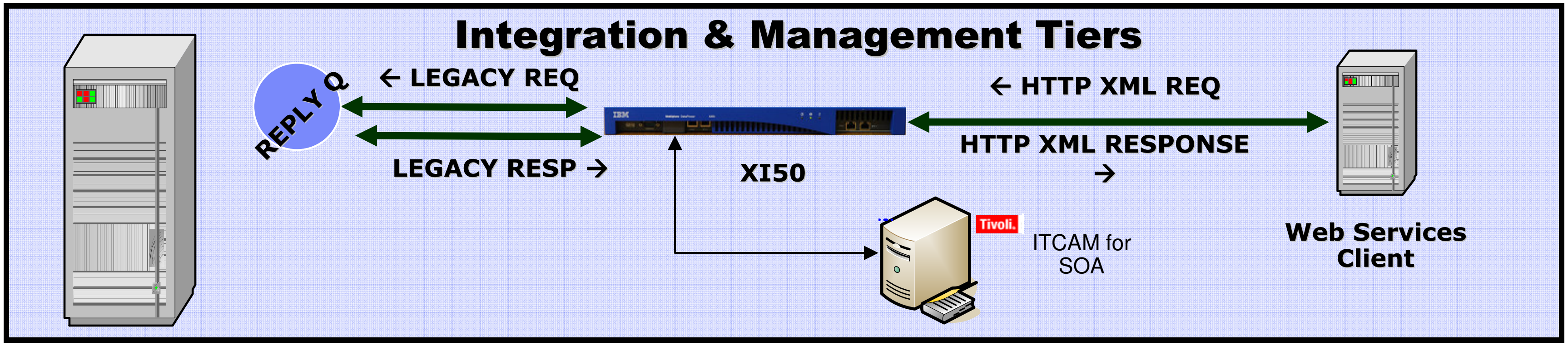
Integration Appliance XI50

- Transforms messages (Binary to XML, Binary to Binary, XML to Binary)
- Bridges multiple protocols (e.g. MQ, HTTP, JMS)
- Routes messages based on content and policy
- Integrates message-level security and policy functions

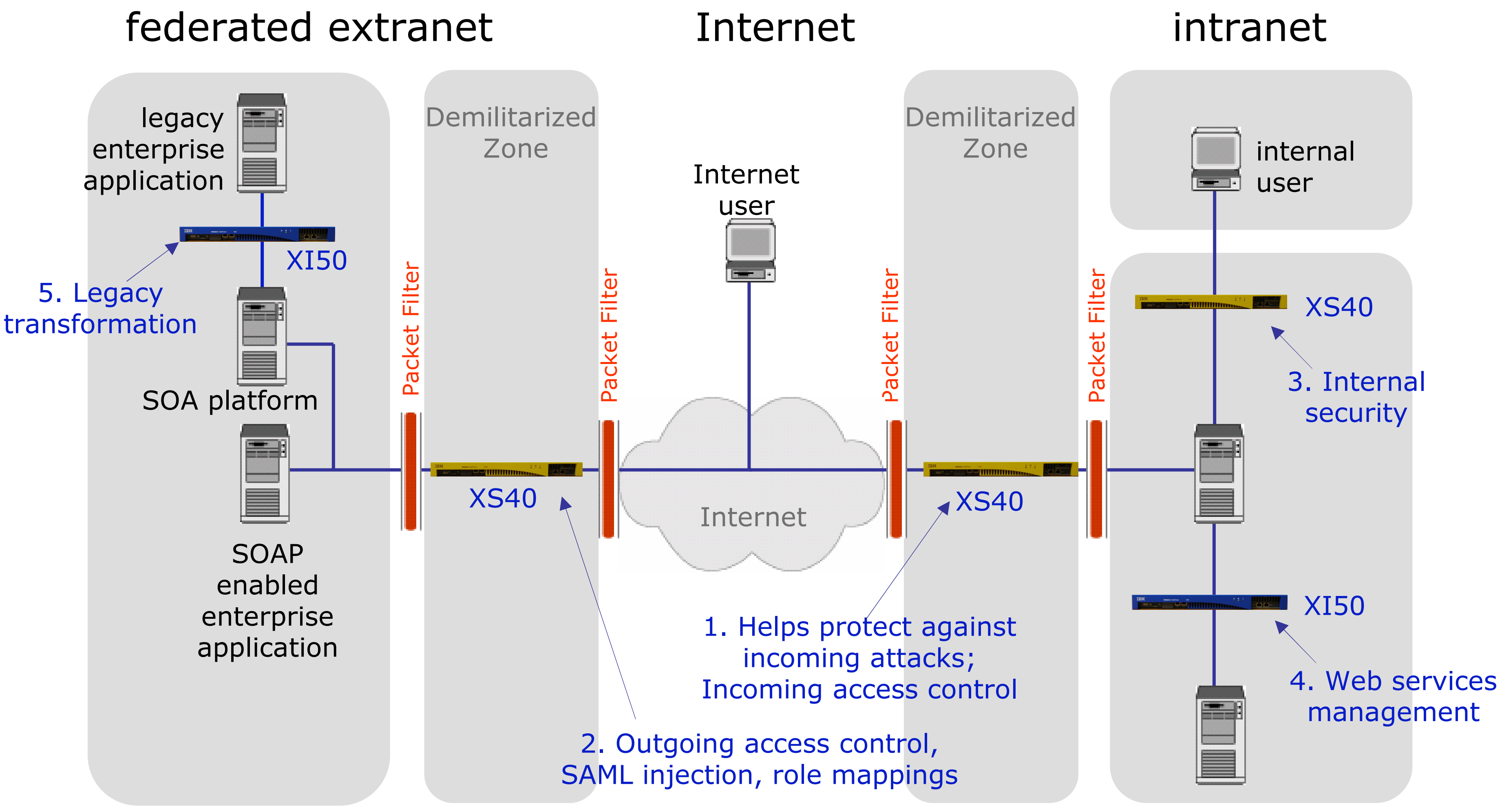
IBM SOA Appliance Deployment Summary







Deployment Scenarios



Use Scenario: XML Acceleration

- **Why?**
  - **Offload XML processing from servers, e.g. Portals, payment solutions etc.**
- **What:**
  - **DataPower XA35 – Accelerator**
    - Wirespeed XML processing
    - SSL termination and acceleration

XML Accelerator XA35

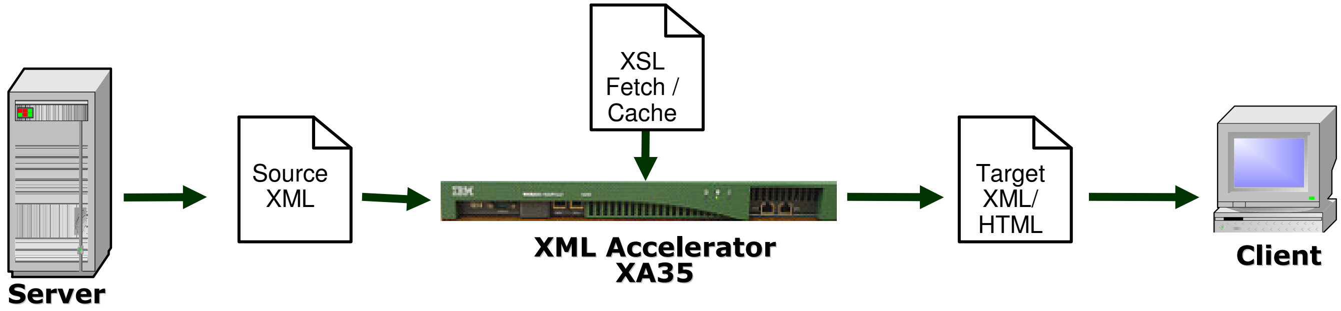
Centralized XSLT Management
Offload XML Processing

- **Wirespeed XML/XSLT/XPath Processing:**
  - Accelerates XML processing, increasing throughput and decreasing latency for XML-based applications by offloading transformation and other resource-intensive functions
- **Schema Validation:**
  - Performs XML Schema validation to ensure incoming/outgoing XML documents are legitmate and properly structured
- **XML Compression, XML Caching:**
  - Reduces impact of increased XML traffic
- **XML Pipeline Processing:**
  - Enables dynamic content generation, data and forms processing
- **SSL Termination/Acceleration:**
  - Accelerates SSL with industry-leading hardware further lessening server workload
- **Easy Configuration & Administration:**
  - Support CLI and WebGUI as well as fully integrated with industry standard IDEs such as Altova XML Spy and Eclipse allowing developers to design, debug and deploy against one single XML and XSLT processor, saving valuable cycles in the progression from pilot to production

High-speed XML Processing

XSLT Transformation, XPath Processing

- **DataPower's purpose-built message processing engine delivers "wirespeed" performance for both XML to XML and XML to HTML transformations with increased throughput and decreased latency**
- **Combines the XML processing power of multiple servers in a single network devices, off-loading heavy lifting from general purpose servers**



*Performance varies depending on usage and customer scenarios, for example 100-200 Mbps

SSL Termination & Acceleration

- **Two-way SSL:**
  - Server and client authentication capture
- **Unlimited identities:**
  - Enabled for scalability
- **SSL acceleration:**
  - Offloads processor intensive crypto to device
- **Flexible support for LDAP over SSL, SOAP over SSL, etc.**

Hardware Reliability

- **Dual swappable power supplies**
  - Separate power cords, designed for high availability
- **Careful thermal design**
  - Multiple fans & high air flow capacity
- **No rotating media for higher reliability**
- **Integrated failover:**
  - VRRP-like (Virtual Router Redundancy Protocol) failover ensures systems defaults to redundant appliance without service interruption
- **Works seamlessly with existing load balancers, firewalls, routers and other network infrastructure**
- **New generation hardware released this Fall:**
  - Faster XML processing
  - Hard disk or flash memory option

Use Scenario: Secure Gateway

- **Why?**
  - **Secure XML / Web Services, secure communication with business partners**
- **What:**
  - **DataPower XS40 – Security Gateway**
    - XML/SOAP Firewall
    - Web Services Security
    - Web Application Firewall

XML Security Gateway XS40

Easy to Use Appliance Purpose-Built for SOA Security

- **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, secure attachments processing (SOAP with Attachments)
- **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

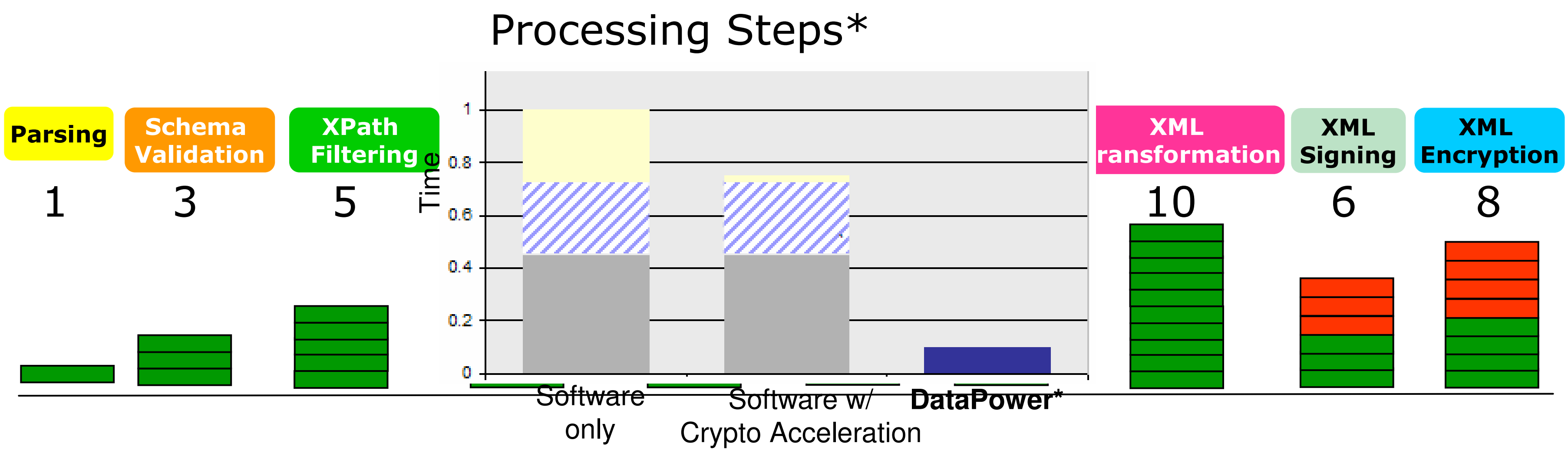
Hardware Device for Improved Security

- **Sealed network-resident device:**
  - Optimized hardware, **firmware**, embedded OS
  - 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
  - Hardware storage of encryption keys, locked audit log
  - Option: **HSM** (Hardware Security Module)
  - No CD/DVD drives/USB ports, no way to boot external media
  - Tamper-proof case

- **Third party certification:**
  - **FIPS** (Federal Information Processing Standards) 140-2 level 3 HSM (Hardware Security Module) (option)
  - Under evaluation by **Common Criteria EAL4** (Evaluation Assurance Level)

Performance Cost of XML Policy Processing

Performance is key to security & mediation


Processing Steps*

- **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.**

XML/SOAP Firewall

- **Integrated multi-layer filters:**
  - IP-layer parameters (e.g., client IP address)
  - SSL params (e.g., client certificate)
  - Any part of HTTP header
  - Any part of SOAP header
  - Any part of XML payload
  - First-level filter select based on service, URL, etc.
- **Easy “point and click” XPath Filtering**
- **Enable/Disable each SOAP method using WSDL wizard**
- **Can be applied at any point in message processing**

XML Threats

Security Risks Growing

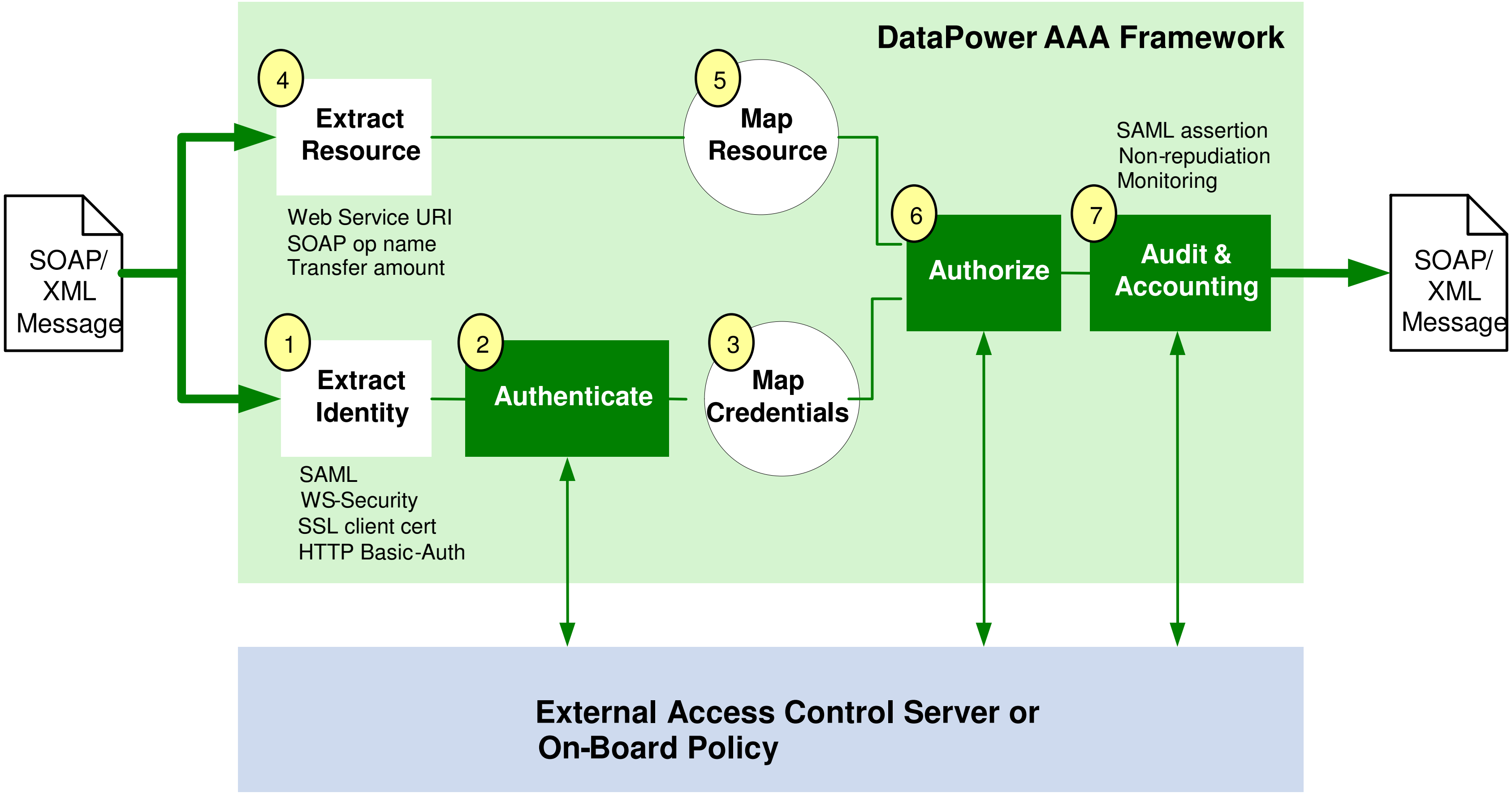
- XML Entity Expansion and Recursion Attacks
- XML Document Size Attacks
- XML Document Width Attacks
- XML Document Depth Attacks
- XML Wellformedness-based Parser Attacks
- Jumbo Payloads
- Recursive Elements
- MegaTags – aka Jumbo Tag Names
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary 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
- …others

Web Application Firewall

- URL-encoded HTTP application protection in addition to XML Web Services firewall security
- Protection for static or dynamic HTML-based applications
- Supports browser-based clients and HTTP/HTTPS backend servers
- Cross-site scripting and SQL Injection protection
- Cookie watermarking (sign and/or encrypt)
- HTTP Header stripping, injection and rewriting

Access Control (3)

AAA Framework Diagram - Authenticate, Authorize, Audit



Access Control - details

Encrypt

AAA Framework Diagram - Authenticate, Authorize, Audit

1. Extract Identity from incoming request
2. Authenticate the output from step 1
3. Map Credentials: how to map the credentials if required (if the authorization service requires a different format than that provided in the request)
4. Extract Resource from incoming request (i.e, what the user is trying to access)
5. Map Resource: how to map the resource if required (if the authorization service requires a different format than that extracted from the request)
6. Authorize, based on the outputs from steps 3 and 5
7. Audit and post-processing: define logging settings and whether the device should generate and insert a security token into the request (trusted by the downstream server). It is also possible to define count monitors so a special alert may be generated at a specified number of failed access attempts.

Use Scenario: SOA Appliance

- **Why?**
  - **Integration, routing, non-XML**
- **What:**
  - **DataPower XI50 – SOA Appliance**
    - Content-based routing
    - Protocol bridging
    - Any-to-any message content mapping

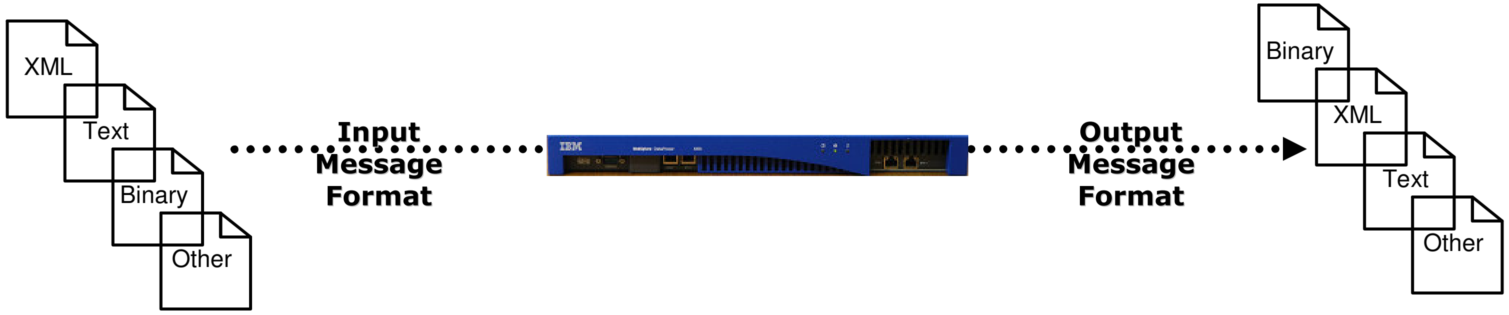
Integration Appliance XI50

Middleware Appliance Purpose-Built for Application Integration

- **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
- **WebSphere MQ integration**
- **IMS integration**
- **DB2 v9 native support**
- **Option: ODBC database integration**
- **Option: TAM (Tivoli Access Manager)**
- **Option: Tibco**

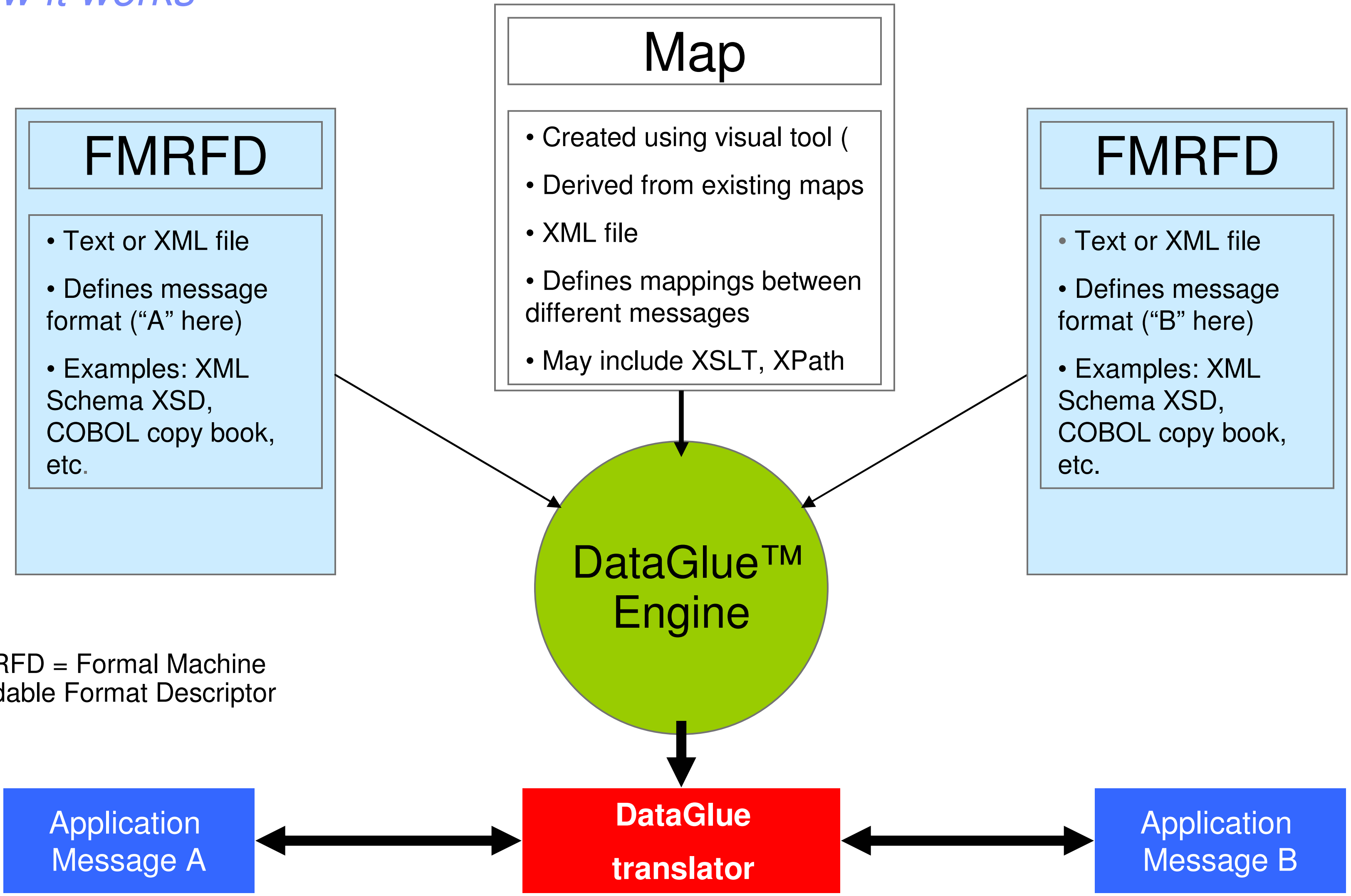
DataGlue’s “any-to-any” Transformation

- **Transform Disparate Data Formats (XML, Binary, Text, etc.)**
- **Broker data between previously siloed systems**
- **Simplifies Reuse of and Connectivity to existing systems**
- **Promotes loose coupling**
- **Transformation of data on the wire enables integration without coding**
- **Note: Updated to run WTX (WebSphere Transformation eXtender transformations**



DataGlue Format Descriptors:

How it works



Map

- Created using visual tool (
- Derived from existing maps
- XML file
- Defines mappings between different messages
- May include XSLT, XPath

FMRFD

- Text or XML file
- Defines message format ("A" here)
- Examples: XML Schema XSD, COBOL copy book, etc.

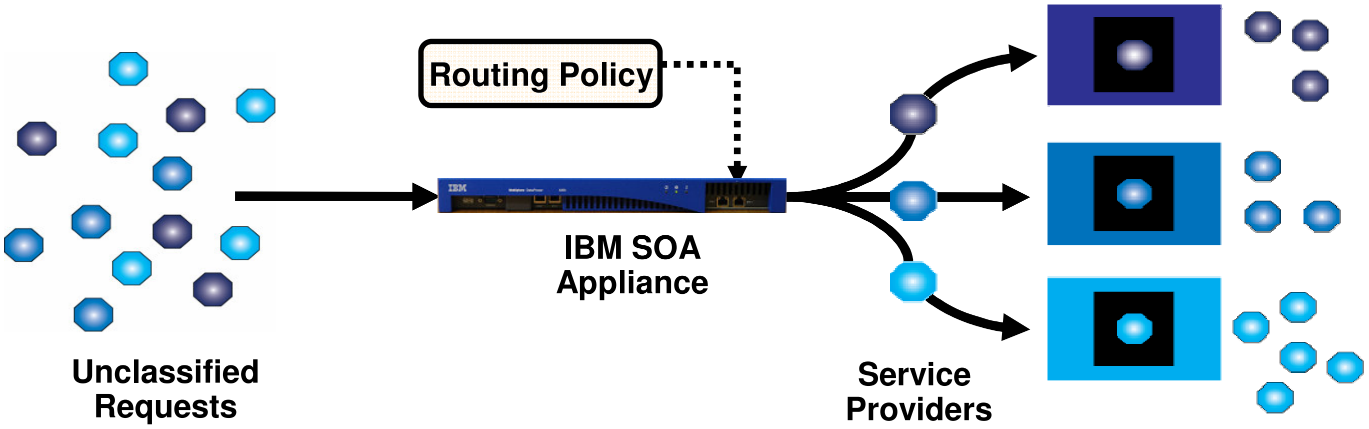
FMRFD

- Text or XML file
- Defines message format ("B" here)
- Examples: XML Schema XSD, COBOL copy book, etc.

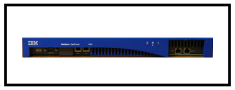
FMRFD = Formal Machine Readable Format Descriptor

Content-based Routing Features

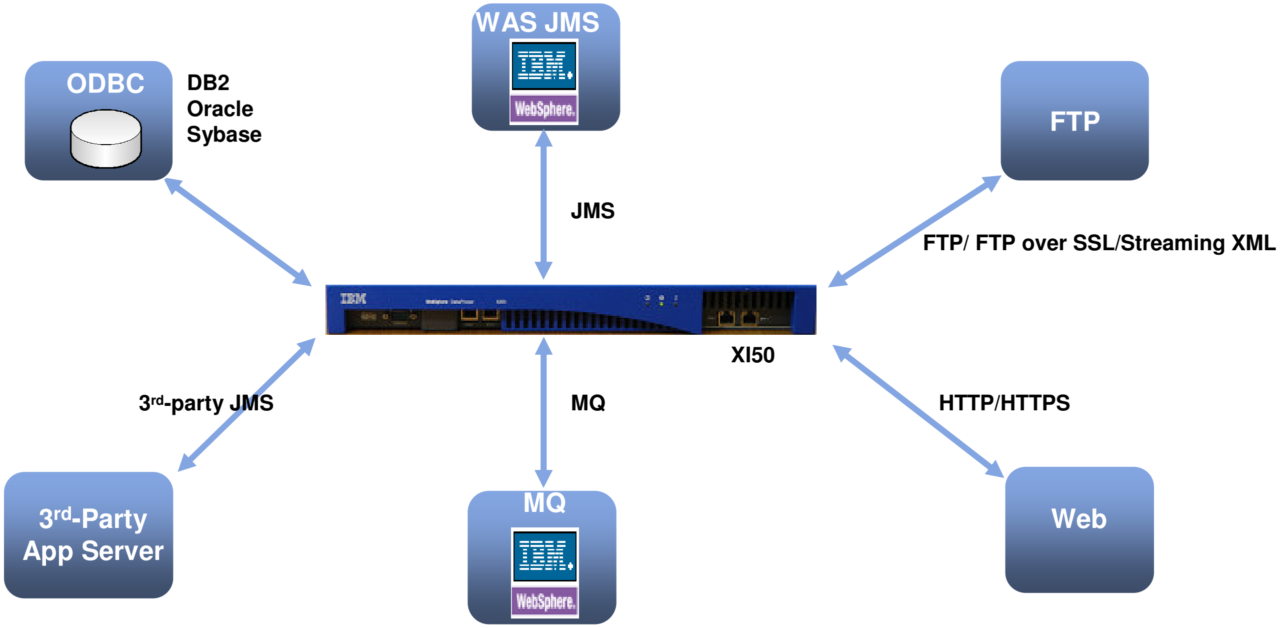
- **Dynamically route based on context (e.g. originating URL, protocol headers and attributes, etc.) and message content (both legacy and XML):**
  - XPath-based routing against any part of the message content or context
- **XI50 can be configured to accept a routing table where routing parameters are 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



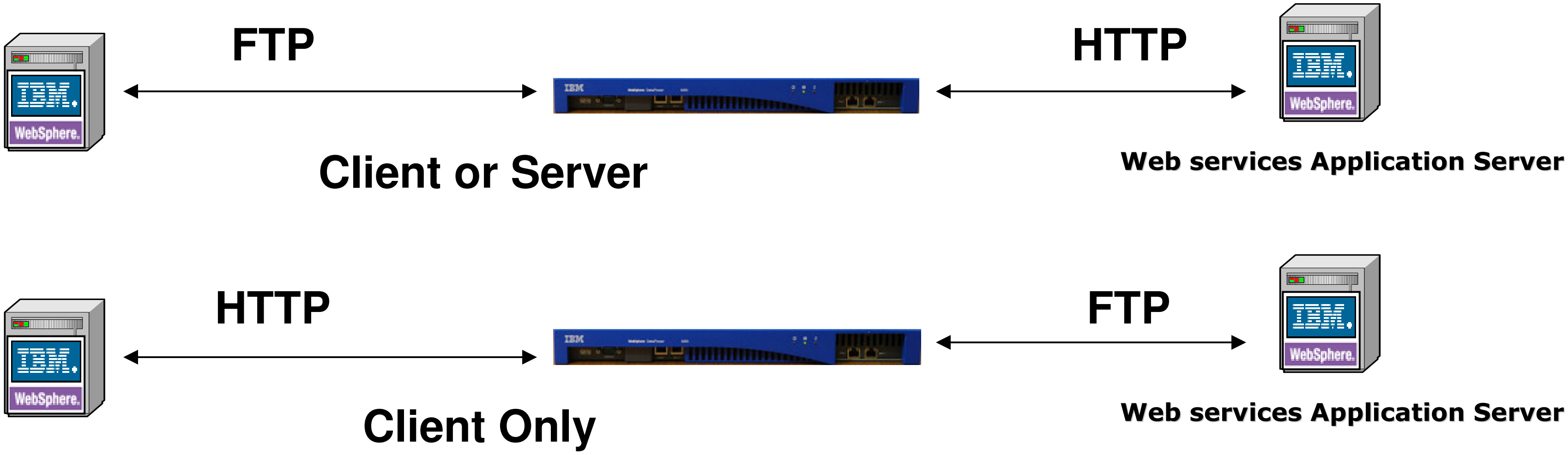
- **First-class support for message and transport protocol bridging**
- **Protocol mediation with simple configuration:**
  - HTTP←→ MQ ←→ WebSphere JMS ←→ FTP ←→ Tibco EMS
- **Request-response and sync-async matching**
- **Able to configure to preserve fully guaranteed, once-and-only-once delivery**



Protocol Bridging (2)

Enhanced File-Based Input

- **Improved transparent file sharing (NFS and FTP) from both front and back side of the DataPower XS40 and/or XI50**
- **File-Based Input:**
  - **retrieve a file (NFS Poller or FTP client)**
  - **accept a file transfer (FTP Server)**
  - **file contains message (SOAP, XML, Binary, Text formats)**
- **FTP URL support allows FTP connections to back end (App Server)**



FTP

HTTP

Client or Server

Web services Application Server

HTTP

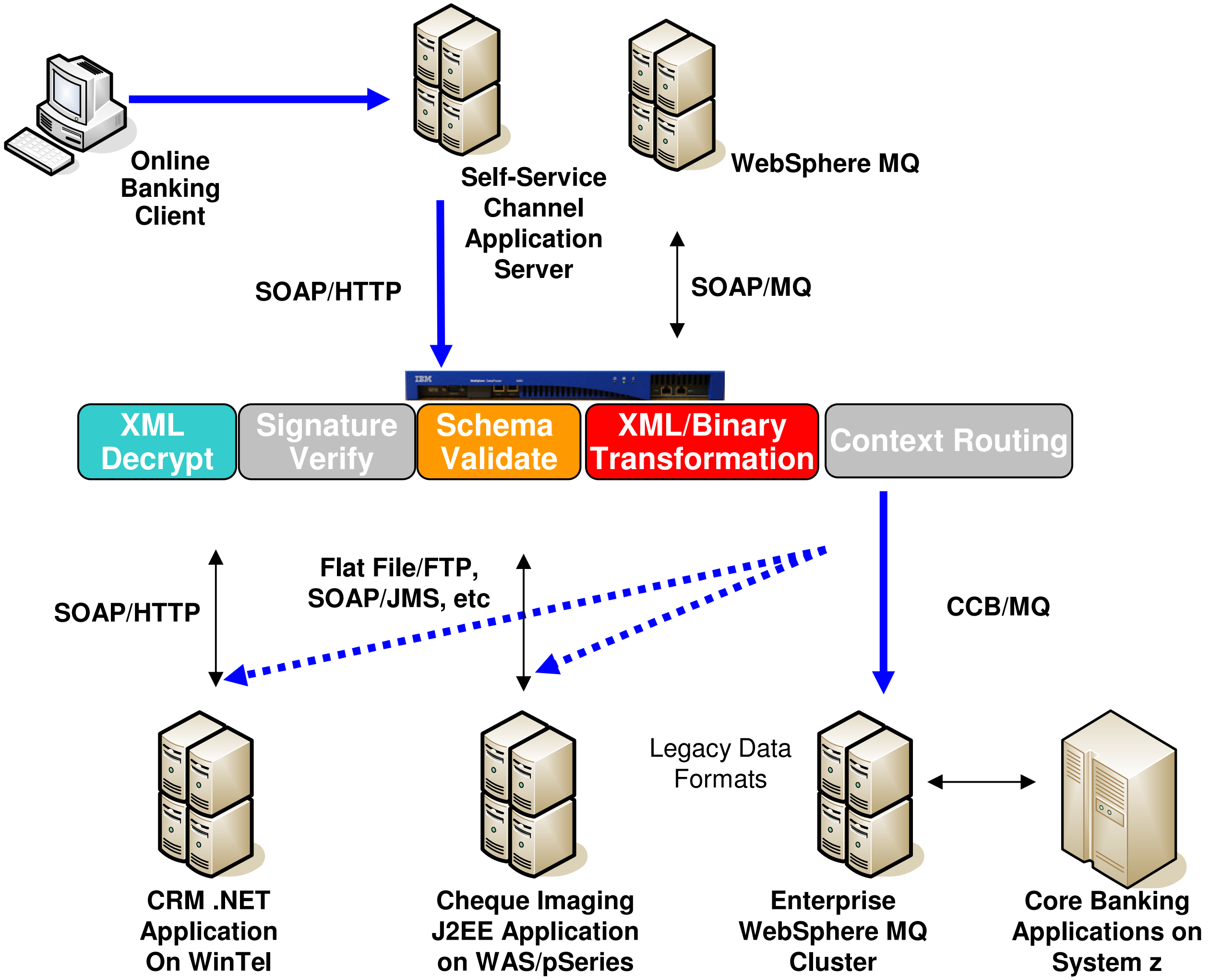
FTP

Client Only

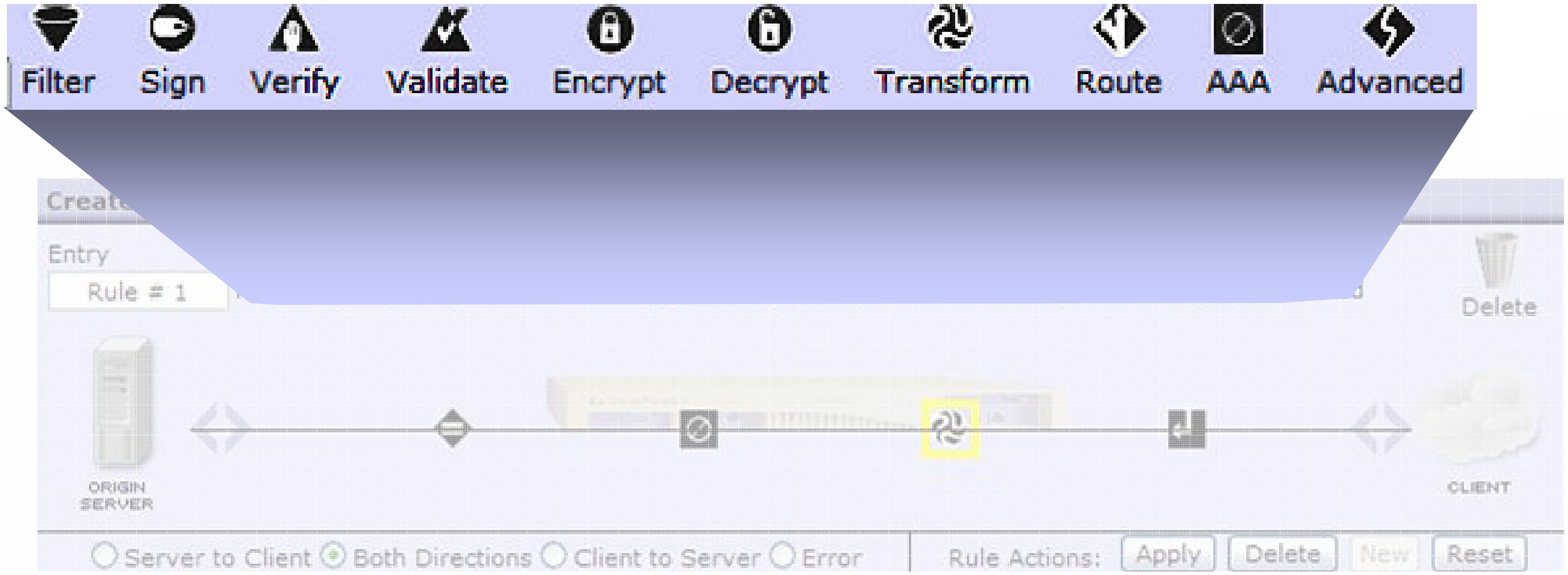
Web services Application Server

Deployment Scenario: Hardware Enterprise Service Bus

- Client Makes Service request
- Application Server sends data to the Gateway to update legacy systems
- Decrypts, Verifies and Validates the message
- Tranforms message to non-XML or XML format
- Routes request to one or more backend systems via MQ


Online Banking Client
Self-Service Channel Application Server
WebSphere MQ
SOAP/HTTP
SOAP/MQ
XML Decrypt
Signature Verify
Schema Validate
XML/Binary Transformation
Context Routing
SOAP/HTTP
Flat File/FTP, SOAP/JMS, etc
CCB/MQ
Legacy Data Formats
CRM .NET Application On WinTel
Cheque Imaging J2EE Application on WAS/pSeries
Enterprise WebSphere MQ Cluster
Core Banking Applications on System z

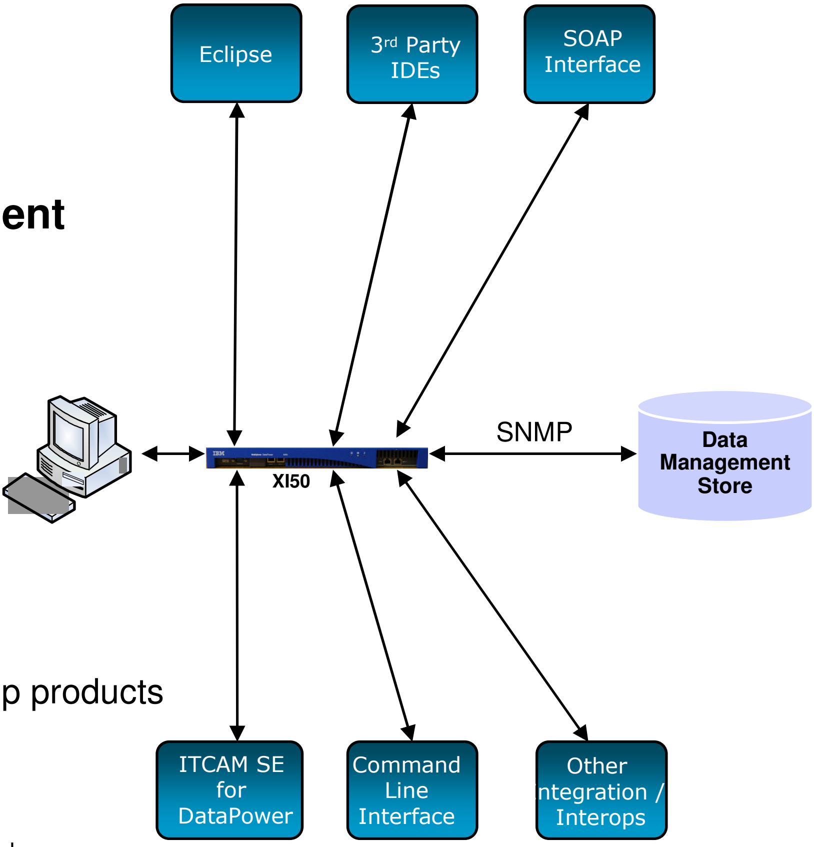
Award-Winning WebGUI: Ease of Use



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
- **<u>Integration For Management</u> strategy:**
  - Industry leading integration support across IBM and 3rd party application, security, identity management and networking infrastructure



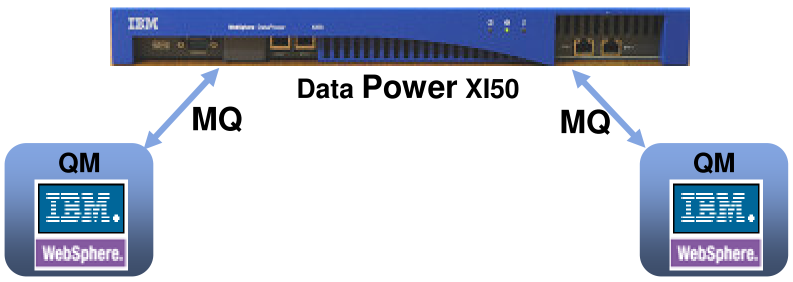
Use Scenario: Mainframe integration

- **Why?**
  - **Access and enable functions and applications on mainframe**
- **What:**
  - **DataPower XI50 – SOA Appliance**
    - CICS integration
    - IMS integration

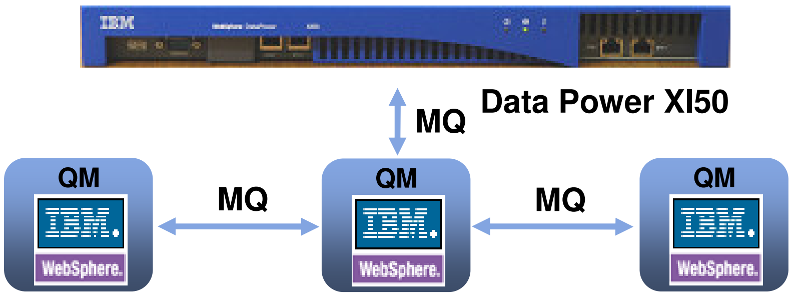
WebSphere MQ Integration

- DataPower can participate as a component in a fully transactional MQ environment; adding DataPower to an MQ environment does not diminish transactionality
- DataPower's MQ Client implementation has been customized in conjunction with IBM's MQ Lab to add improvements beyond the use of the typical client libraries

Configuration 1

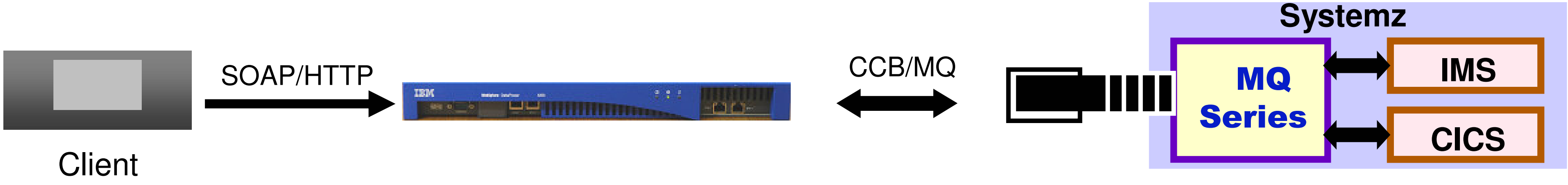


Configuration 2



Legacy Integration with DataPower and Systemz

- **Web Services enablement and security for CICS and IMS applications**

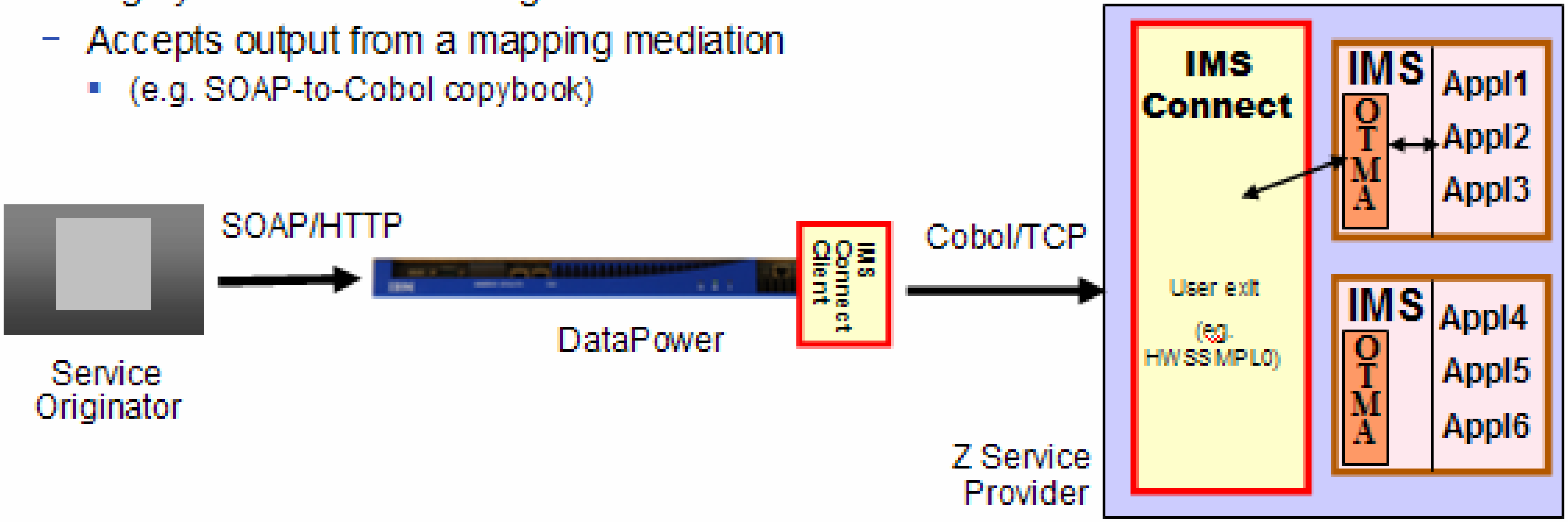


- **WebSphere MQ on Systemz is the first and best answer**
  - Proven reliability and performance
  - Very widely deployed

- **Integrated system administration, configuration and monitoring**
  - Tivoli Enterprise Portal is the management framework
  - ITCAM SE for DataPower TEP-based product for multi-box management

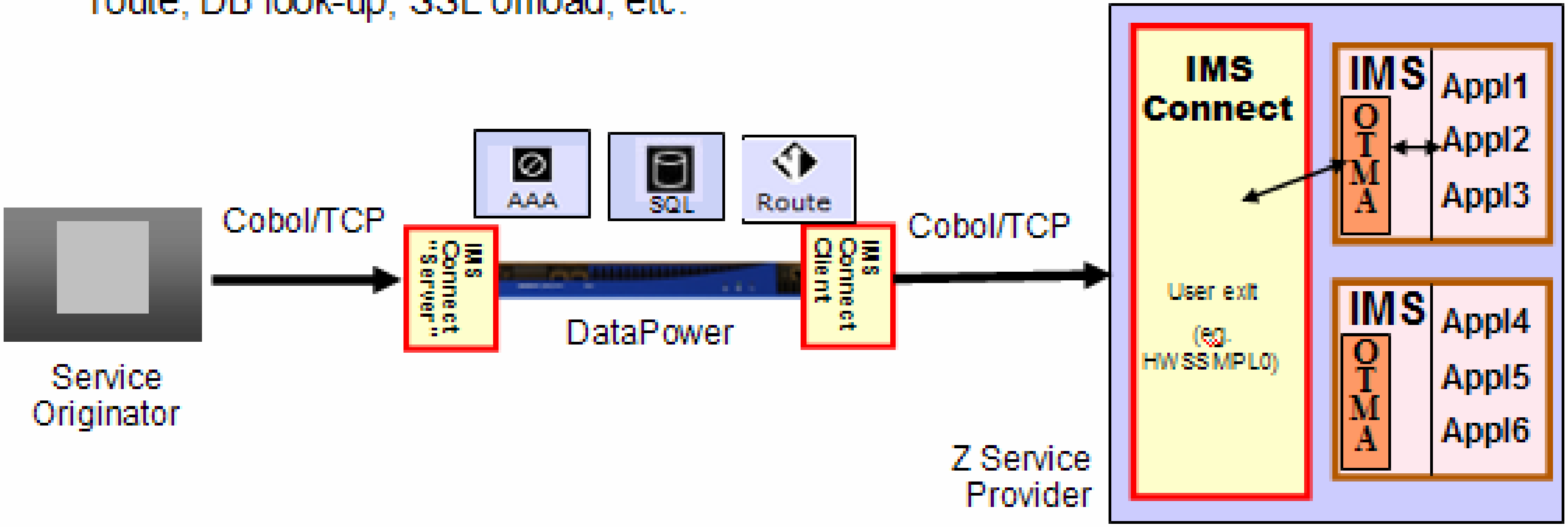
IMS

- Remove MQ requirement of WS-enablement of IMS
  - IMS has few alternatives (IMS SOAP Gateway is an entry-level solution)
- Implement an “IMS Connect Client” on DataPower that natively connects to IMS Connect using its custom request/response protocol w/ well-defined header structure
  - Highly consumable for the common case
  - Highly extensible and integrates well with DataPower model
  - Accepts output from a mapping mediation
    - (e.g. SOAP-to-Cobol copybook)



IMS

- Bring DataPower value add to standard IMS connect usage patterns
- Provide an "IMS Connect Client" on DataPower that natively connects to IMS Connect
- Provide an "IMS Connect Server" on DataPower that accepts IMS Connect client connections and provides an intermediation framework that leverages DataPower
  - Can do things like authentication checks, authorization, logging, SLM, transformation, route, DB look-up, SSL offload, etc.



Use Scenario: Web Services Management

- **Why?**
  - **Management & Monitoring of Web Services**
- **What:**
  - **DataPower XI50**
    - Service Level Management & Monitoring
    - Reuse
    - Policies

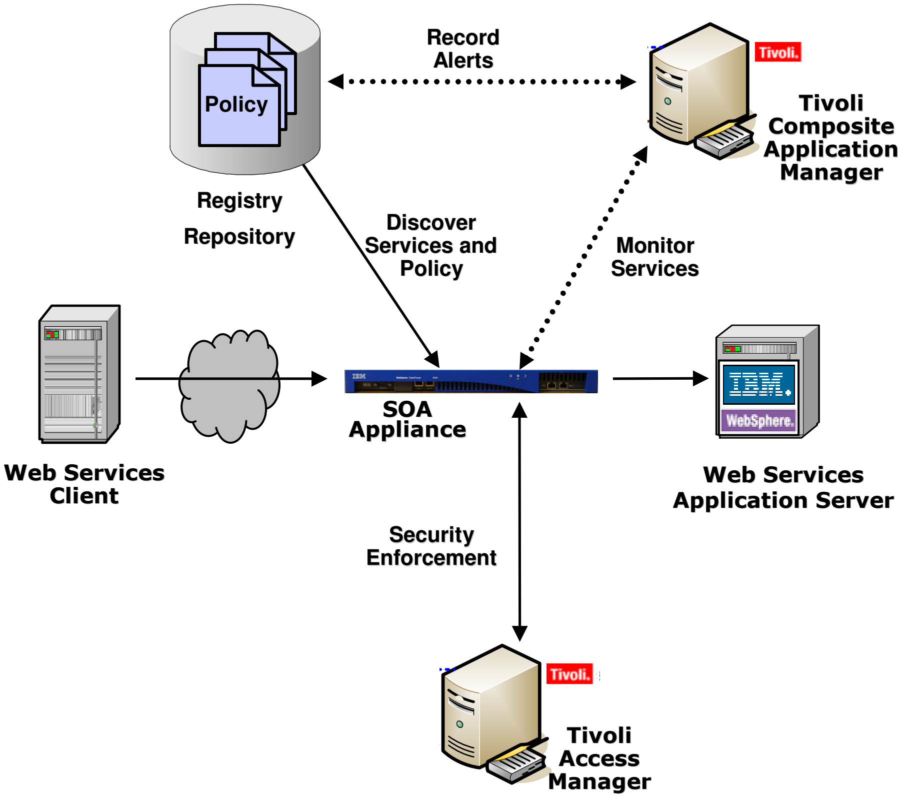
Web Services Management

- **SLM - 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.
- **Support for WSDM, Web Services Distributed Management**
  - **Manage and monitor Web Services**
- **Allow subscription to SLM for alerts, logging, etc.**

Web Services Management

Registry/Repository Support & SOA Governance

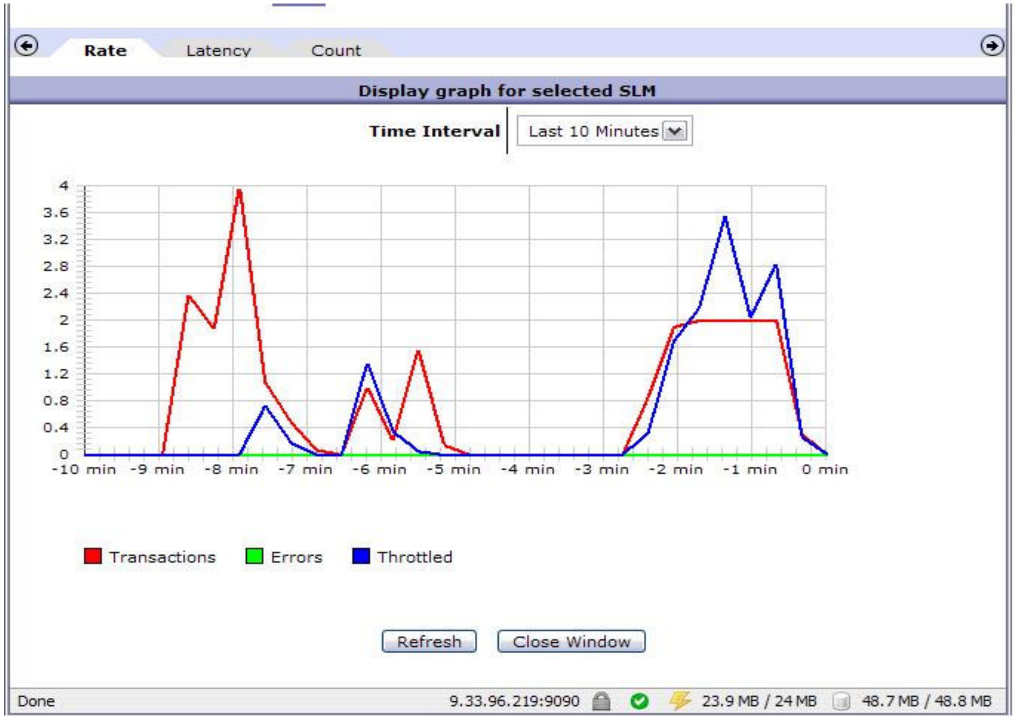
- **Use of a central repository can facilitate Discovery and Reuse of Web services:**
  - WSRR and UDDI supported
- **Artifacts can be stored, updated via repository**
- **Push/Retrieve configuration of new services to DataPower for enforcement**
- **Policy and Security enforcement for SOA Governance on DataPower**
- **ITCAM (IBM Tivoli Composite Application Manager) for SOA:**
  - Central management console
  - Polls device at set intervals
  - Traffic inspection, statistical analysis



Web Services Management

Service Level Management

- **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**

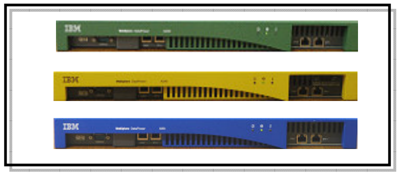


Display graph for selected SLM

Time Interval: Last 10 Minutes

Done 9.33.96.219:9090 23.9 MB / 24 MB 48.7 MB / 48.8 MB

Integration Across IBM

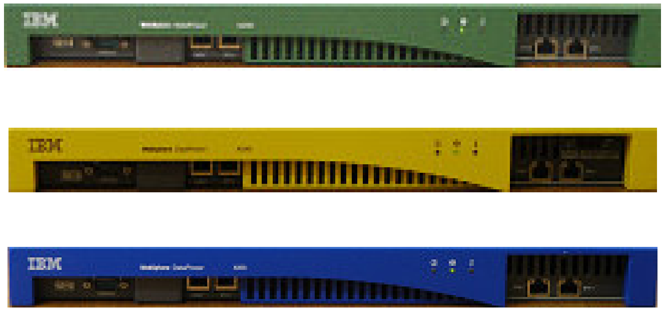


- **XI50 includes support for**
  - WebSphere MQ
  - WebSphere JMS
  - IMS – IMS Connect Client & IMS Connect Server on DataPower
- **DB2 v9 native support**
- **Tivoli Ready**
  - Fine-grained access control with Tivoli Access Manager (TAM) - Certified
  - Tivoli Federated Identity Manager (FIM) Certified (SAML, WS-Trust) - Certified
  - Monitoring of XML traffic flows with NetView
  - End-to-end SOA Management with IT CAM for SOA
- **RAD/Eclipse integration**
  - Rich console allows creation and monitoring of policies from within IDE
- **WTX – WebSphere Transformation eXtender**
  - For complex transformations, industry standard formats etc.
- **WSRR – WebSphere Service Registry and Repository**
  - Service resolution and policy enforcement
- **Futures**
  - Integrated SOA tooling across the portfolio
  - Continued investment in 3rd party (competitive middleware) integration & interop

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

IBM SOA

DataPower new appliances…

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

B2B Appliance XB60

- B2B Messaging (AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Unparalleled performance
- Simplified management and configuration

2005 Network Computing WELL-CONNECTED AWARDS WINNER

XML Accelerator XA35

- Offload XML processing
- No more hand-optimizing XML
- Lowers development costs

RATED EXCELLENT InfoWorld

XML Security Gateway XS40

- Enhanced Security Capabilities
- Centralized Policy Enforcement
- Fine-grained authorization
- Rich authentication

Integration Appliance XI50

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

Business to Business (B2B) Appliance XB60

Purpose-built B2B hardware for simplified deployment, exceptional performance and hardened security

- Extend integration beyond the enterprise with B2B
- Hardened Security for DMZ deployments
- Easily manage and connect to trading partners using industry standards
- Simplified deployment and ongoing management

Trading Partner Management for B2B Governance; B2B protocol policy enforcement, access control, message filtering, and data security

Application Integration with standalone B2B Gateway capabilities supporting B2B patterns for AS2, AS3 and Web Services

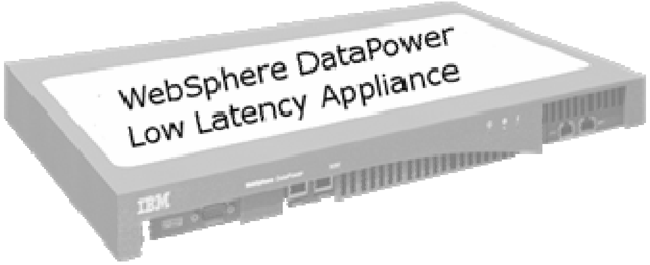
Full featured User Interface for B2B configuration and transaction viewing; correlate documents and acknowledgments displaying all associated events

Simplified deployment, configuration and management providing a quicker time to value by establishing rapid connectivity to trading partners

Low Latency Appliance XM70

Purpose-built hardware for low-latency, network-based messaging and data feed processing

- Drop-in messaging solution which plugs into existing network infrastructure
- Enhanced QoS and performance with purpose-built hardware
- Simplified, configuration-driven approach to low-latency, publish/subscribe messaging and content-based routing
- High availability out of the box (two or more appliances)

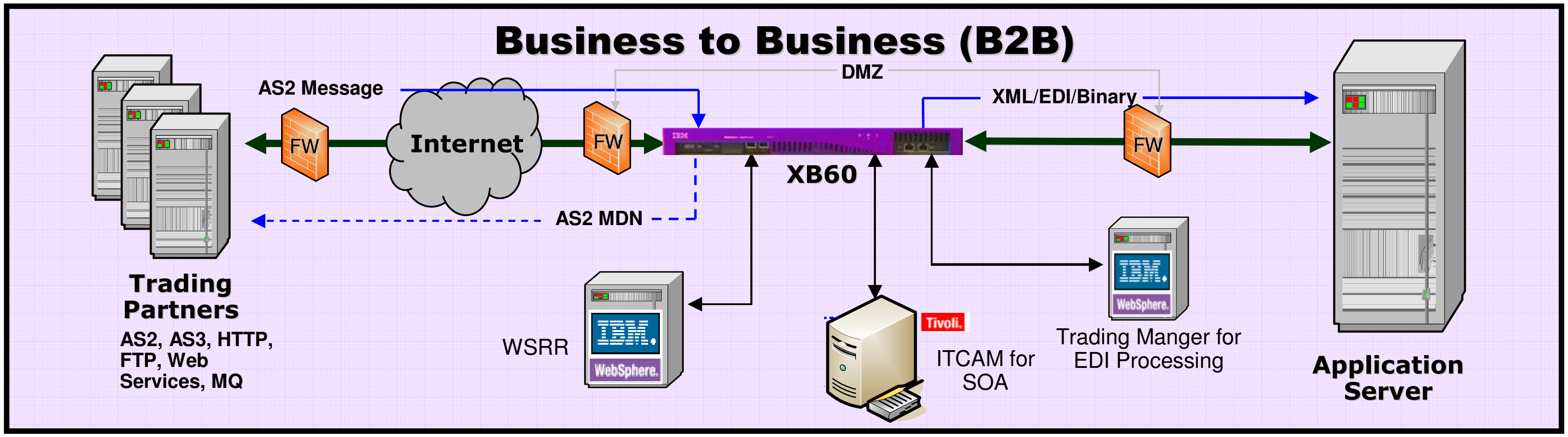


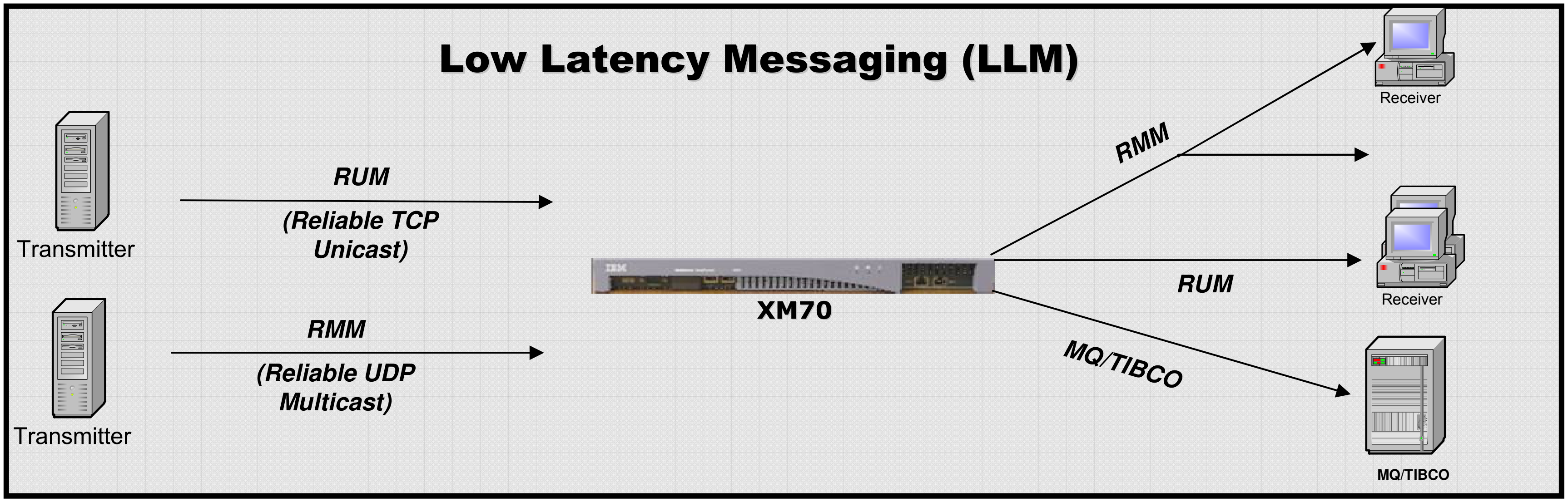
Low-latency unicast and multicast messaging, scaling to 1M messages / sec with microsecond latency

Destination, property and content-based routing, including native XML and FIX parsers

Optimized to bridge between leading standard messaging protocols such as MQ, Tibco, WebSphere JMS and HTTP(S)

Simplified deployment, configuration and management providing a quicker time to value by rapidly configuring messaging destinations, connectivity and routing


Business to Business (B2B)
AS2 Message
DMZ
XML/EDI/Binary
FW
Internet
FW
FW
XB60
AS2 MDN
Trading Partners
AS2, AS3, HTTP, FTP, Web Services, MQ
WSRR
Tivoli.
ITCAM for SOA
Trading Manger for EDI Processing
Application Server


Low Latency Messaging (LLM)
Transmitter
RUM
(Reliable TCP Unicast)
Transmitter
RMM
(Reliable UDP Multicast)
XM70
RMM
Receiver
RUM
Receiver
MQ/TIBCO
MQ/TIBCO

IBM SOA

Education

Education

- **Courses**
  - SW550NO – Accelerating XML Applications Using DataPower Devices
  - SW551NO – Securing Web Services Applications using IBM WebSphere DataPower SOA Appliances
  - WB552NO – Accelerate and secure XML and Web Services with IBM DataPower SOA Appliances
- **Certification**
  - Tutor or self-study approach
- **PoT – Proof of Technology**
  - Norway, last run in June 2008
  - Free of charge
  - General or possibly customer tailored

IBM SOA

SWG Norway contact information

Jo Torsmyr - torsmyr@no.ibm.com