Building a smarter planet together

2010 CSI Interchange, IBM India | August 11th - 13th

Common WebSphere DataPower Architectural Patterns and ESB/Security Gateway Choices

Devaprasad Nadgir
Certified Sr. Architect, WebSphere Software
devaprasad@in.ibm.com

Bill Hines
WW Technical Sales Leader, WDP
bill.hines@us.ibm.com

Agenda

- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

Introduction

- Who am I ?
- What will we cover in this session?
- Assumed knowledge/pre-reqs
- When & how can you ask questions?
- If you have further questions, whom should you contact ?

Agenda

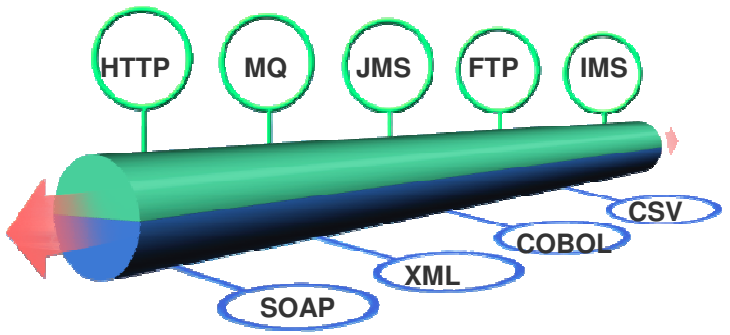
- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

Enterprise Service Bus Choices

- An ESB does:
  - ROUTING messages between services
  - CONVERTING transport protocols between requestor and service
  - TRANSFORMING message formats between requestor and service
  - HANDLING business events from disparate sources

- An ESB is typically the ‘heart’ of a service oriented architecture to prevent tight coupling of applications to one another

- IBM’s Three ESB Products
  - WebSphere DataPower SOA Appliance
  - WebSphere Message Broker
  - WebSphere Enterprise Service Bus

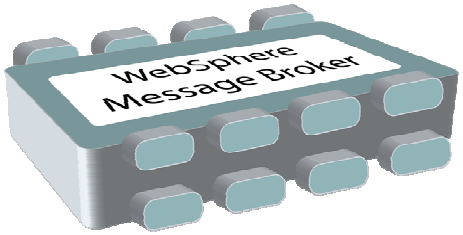


ESB offerings from IBM WebSphere

WebSphere delivers the most complete ESB solution

WebSphere ESB

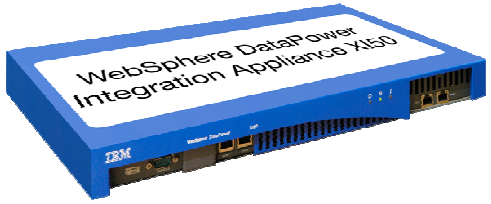
Built on WebSphere Application Server for an integrated SOA platform



WebSphere Message Broker

Universal connectivity and transformation in heterogeneous IT environments

ESB offerings from IBM WebSphere

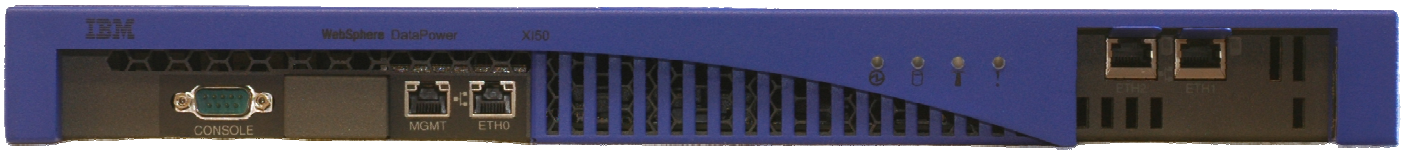


WebSphere DataPower Integration Appliance XI50

Purpose-built hardware ESB for simplified deployment and hardened security

Enterprise Service Bus Choices

- WebSphere DataPower SOA Appliance
  - Hardened ESB in rack-mount 1U appliance or blade form factor
  - Typically this is the XI50 model (blue box), but alternatively:
    - New form factor – XI50B Blade Appliance for BladeCenter
      ESB on a blade!
    - XB60 for AS1, AS2, AS3 B2B or file transfer scenarios
    - XM70 for low-latency messaging (unicast, multicast), TIBCO RV
  - Often used for other uses cases, but as an 'ESB' due to:
    - Numerous protocols supported for protocol mediation
      HTTP(s), (s)FTP(s), WAS JMS, WebSphere MQ, Tibco EMS,IMS
    - Extensive facilities for dynamic routing
    - Transformation capabilities for XML (XSLT) or non-XML payloads
      Non-XML transforms via graphic development in WTX or Analyst
    - Themes are DMZ-suitable, security, performance, ease of use



Enterprise Service Bus Choices

- WebSphere Message Broker
  - Native code software product for various platforms including z/OS
  - Integrates through standard protocols, WebSphere Adapters for enterprise applications, and specialized connectivity options
  - Optimized for high-volume processing and rapid time to value for complex mediation requirements with a robust set of pre-built mediation functions
  - Tight integration with WebSphere MQ
  - Optimized for high-volume processing and rapid time to value for complex mediation requirements with a robust set of pre-built mediation function
  - Development in C / C++, ESQL, Java, WTX

Enterprise Service Bus Choices

- WebSphere Enterprise Service Bus
  - Build on WebSphere Application Server Java EE Platform
  - Integration with WAS platforms such as Process Server
  - Optimized for standard XML and Web services formats, with basic support for other common formats
  - Extended support for WS-* Web services standards
  - Support Java Enterprise/SOA standards
  - J2EE, JMS, HTTP, SOAP, UDDI, XML, WSDL, BPEL, SCA. SDO
  - Development primarily in Java using tooling such as WebSphere Integration Developer

Enterprise Service Bus Choices

- So, which ESB for me?
  - Consider the following factors
    - Where does this functionality need to reside?
      DMZ, back-end secure/trusted zone, etc
    - In-house platforms, programming skills and existing assets
    - Security constraints/requirements
    - Connectivity needs to specialized environments
    - Best usage of existing hardware platforms

Enterprise Service Bus Choices

- Look to Message Broker for:
  - Back-end ESB needs, particularly native code speed and connectivity to environments such as SAP, Peoplesoft, Siebel with WMB Adapters
  - Transactional processing (i.e. XA, two-phase commit scenarios)
  - Persistent messaging needs
  - Diverse programming (C/C++, ESQL, Java)
  - Advanced/complex message/event flows
  - Sophisticated scheduling/timing requirements
  - Raw TCP, telemetry, device integration needs

Enterprise Service Bus Choices

- Look to WebSphere Enterprise Service Bus for:
  - Primarily pure Java/JEE environments
  - WAS platforms for LTPA/security integration
  - Persistent JMS messaging
  - XA transaction coordination/participation
  - Complex message flows
  - Pre-existing JEE programming/administrative experience
  - Extensive caching capabilities (Servlet/JSP/Web services)

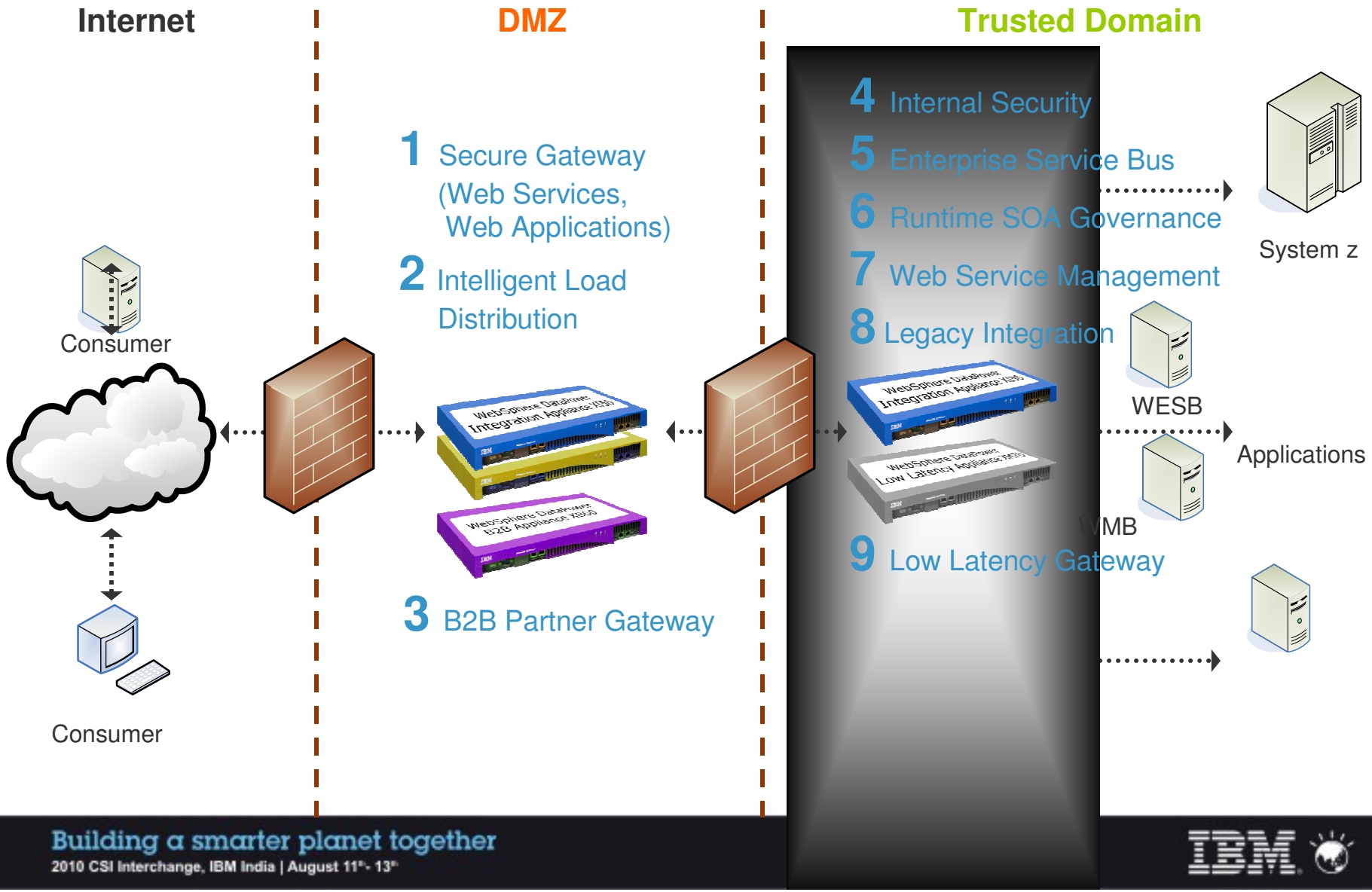
Enterprise Service Bus Choices

- Look to DataPower Appliances for:
  - DMZ ESB capability, including perimeter security
  - Quick and easy configuration, deployment, administration
  - High-speed offload of CPU/memory sucking tasks such as transformation, crypto operations, message validation, threat detection for XML, non-XML and standard Web applications
  - Service-level management to ensure back-end efficiency
  - Extensive integration with other IBM and 3rd party products
  - High security requirements (FIPS 140-2 L3, Common Criteria EAL, PCI, HSM, military/intelligence spec)
  - Special requirements for B2B or LLM (unicast/multicast)
  - Broadest and most up to date range of spec-level compliance for WS-*, SAML, XACML, and others
  - Broadest range of protocol/messaging support
  - Existing BladeCenter infrastructure

Enterprise Service Bus Patterns

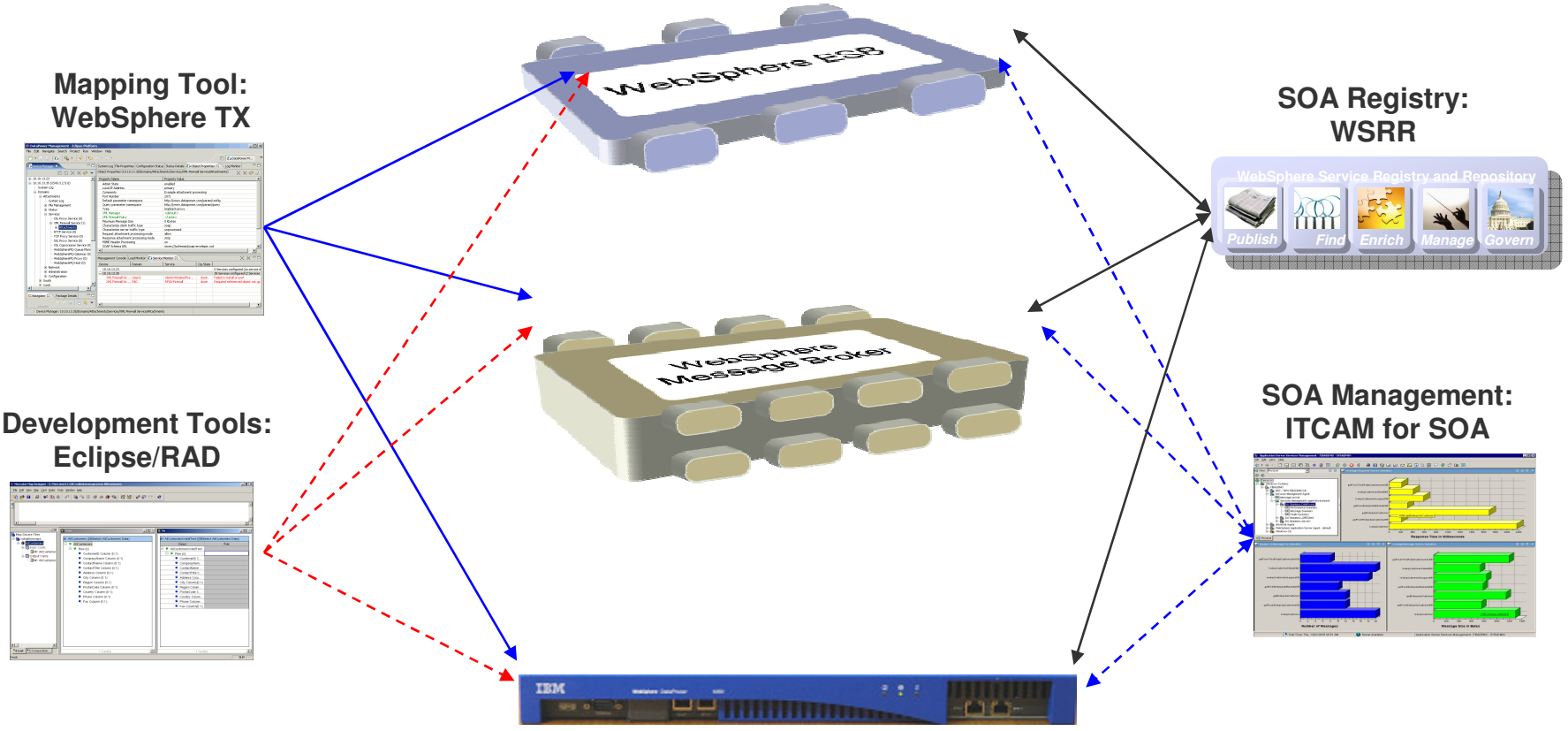
- A common solution: Combining technologies for a world class ESB
  - 'Gateway' pattern: DataPower in the DMZ to filter away threats, authentication/authorization failures, invalid messages, excessive traffic (including DoS), crypto offload (encrypt/decrypt/DSig/SSL), dynamically route and to transform to the "golden schema" in order to allow a back-end ESB or platform to operate at peak efficiency and focus on the business logic.
  - Hybrid ESB pattern: Often this consists of a DataPower XS40, XI50, or XB60 in the DMZ with a XI50, XM70, WMB or WESB back-end layer handling transactionality, persistence, audit control.
  - Federated ESB pattern: Used to associate two or more service buses in different organizational units

ESB Use Cases



Integrated SOA Tooling Across the ESB Runtimes

All 3 ESBs Integrate with Eclipse, WTX, ITCAM for SOA and WSRR



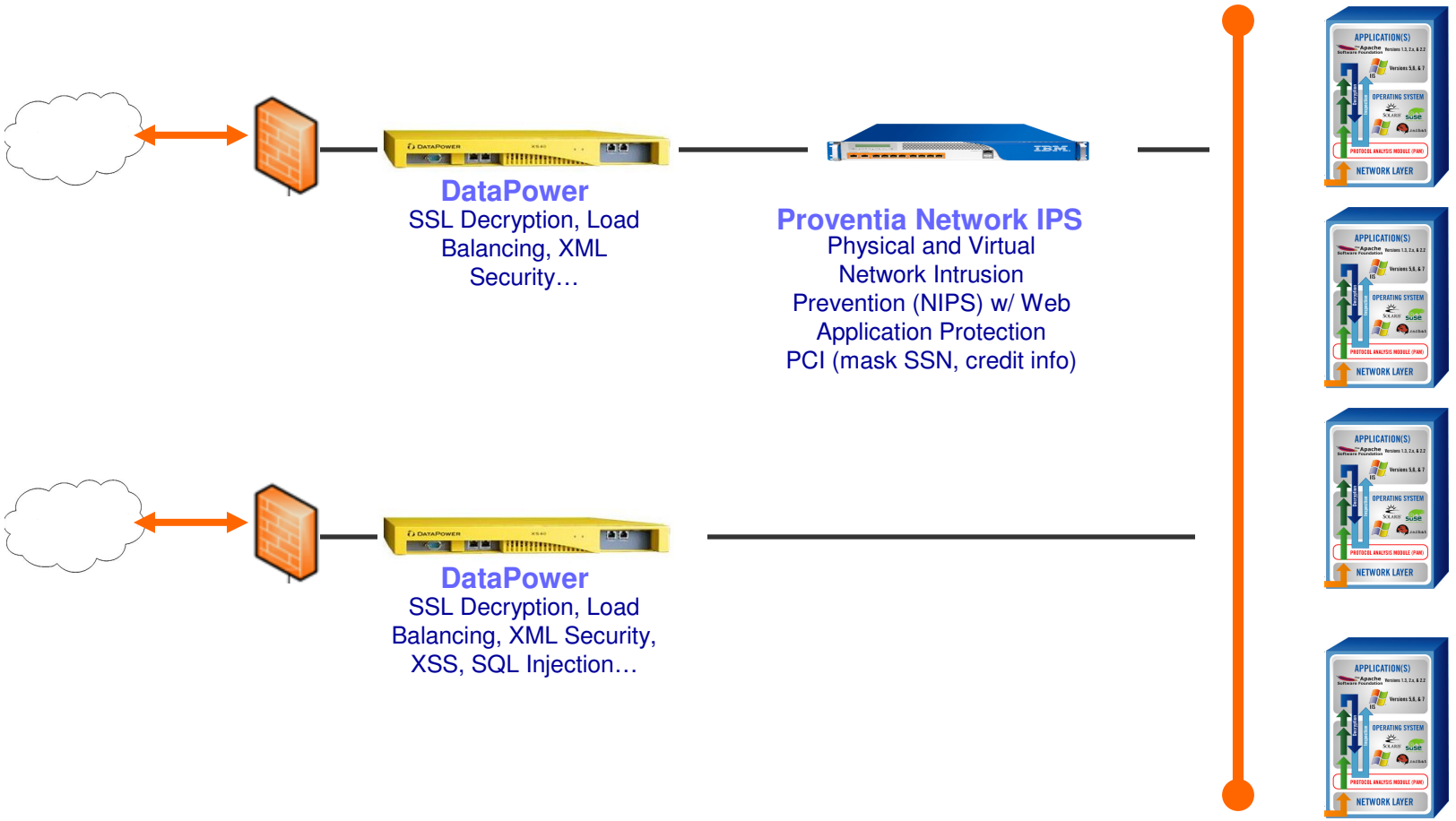
Agenda

- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

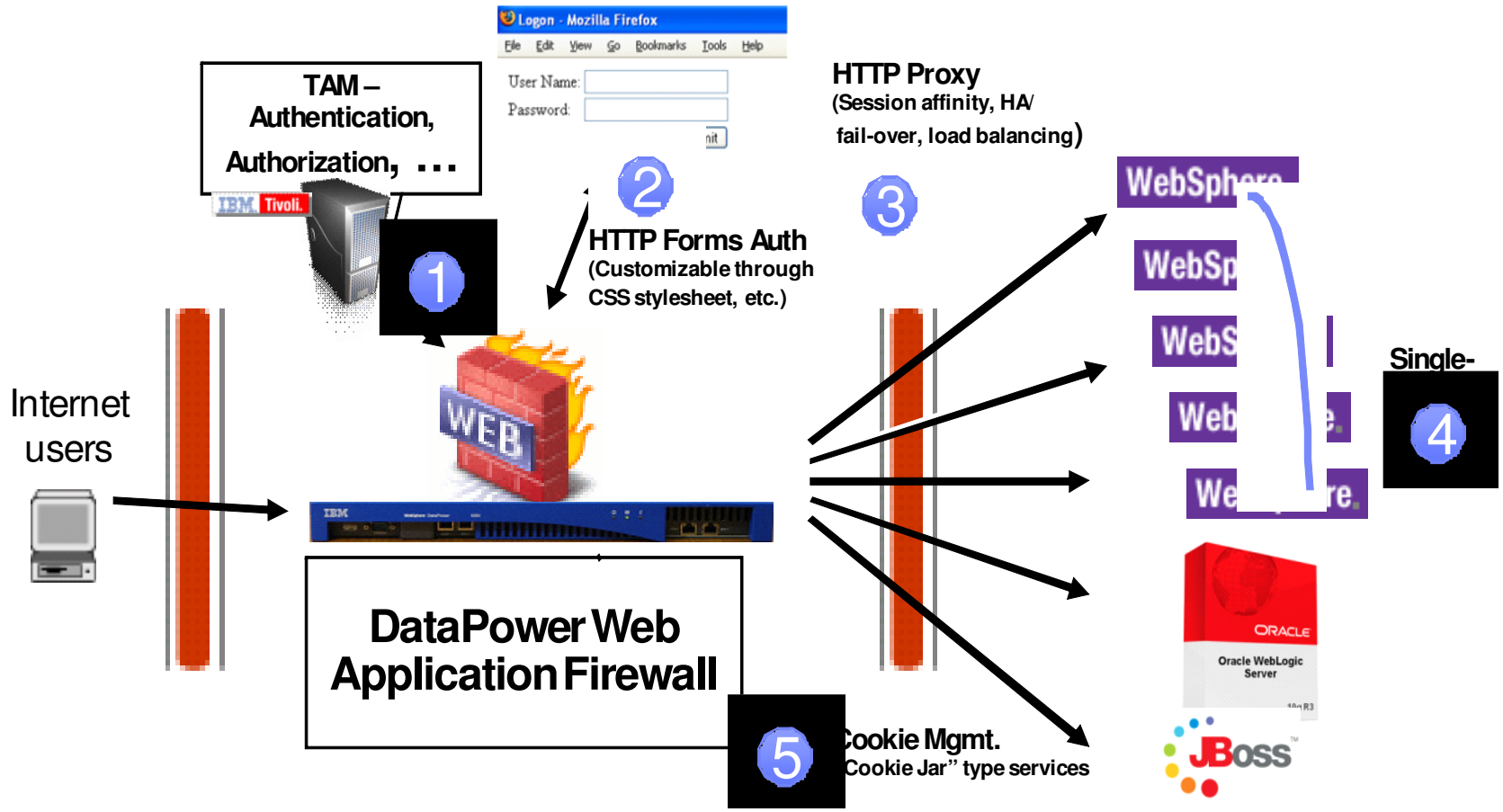
DataPower with Proventia for WAF

Capability		Proventia IPS	WebSphere DataPower
Web protocol and content inspection and blocking	▪ Buffer overflow exploits	X	X
	▪ PHP file-include	X	
	▪ Form/hidden field manipulation	X	
	▪ Forceful browsing	X	
	▪ Cross-site scripting (XSS)	X	X
	▪ Command injection	X	
	▪ SQL injection	X	X
	▪ Web site defacement	X	
	▪ Well-known platform vulnerabilities	X	
	▪ Zero-day exploits	X	
	▪ General name-value criteria boundary profiles for:		
	▸ Query string and form parameters		X
	▸ HTTP headers		X
	▸ Cookies		X
SSL termination, crypto acceleration	▪ SSL Acceleration and Termination (Link)		X
	▪ Cookie watermarking (sign and/or encrypt)		X
Application acceleration	▪ Dynamic routing and load balancing		X
	▪ Session handling policies		X
	▪ Rate limiting and traffic throttling/shaping		X
	▪ Customizable error handling		X

DataPower, Proventia Use Case



DataPower Web Application Firewall



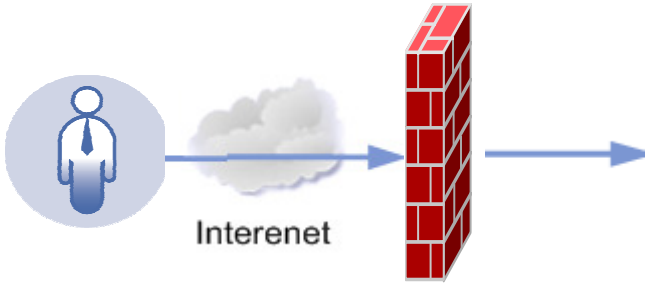
DataPower/WebSphere Application Server Plugin

- Often the issue of replacing the WAS plugin with DataPower arises
  - The ability to use DataPower as the sole DMZ proxy for all backend traffic and use the Application Optimization (AO) self-balancing feature to do away with front-end load balancers is attractive
- Many similar capabilities, particularly with the advances in Web app proxying in DataPower firmware 3.8.0, 3.8.1 and AO
  - AO allows DataPower to receive cell/cluster/app changes/updates on a periodic basis and dynamically adjust load balancer groups
  - Intelligent Load Balancing in 3.8.1 AO is now JEE application-aware
- Plugin still has some advantages
  - Better static/dynamic caching and Edge-Side Include (ESI) capabilities at this point
  - Better awareness of JEE/application deployment descriptors

Agenda

- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

Terminology



1. What are the policies of the Enterprise
2. Who is the user [Authentication]
3. Can the user access the resource [Authorization]
4. [Optional] What is the Identity for accessing backend service
5. Enforce all of the above

1. **What is the policy of the Enterprise**
   - **Policy Access Point [PAP]**
     - **Authoring policies and make them available to PDP**
2. **Who is the user [Authentication]**
   - **Validate a user against a trusted directory, or trusted mechanism**
3. **Can the user access the resource [Authorization]**
   - **Policy Decision Point [PDP]**
     - **Provide decision after evaluating policies/rules against subject and target**
4. **[Optional] What is the Identity for accessing backend service**
   - **Federation**
     - **From Client Certificate to LTPA Token**
     - **From UsernameToken to SAML**
5. **Enforce all of the above**
   - **Policy Enforcement Point [PEP]**

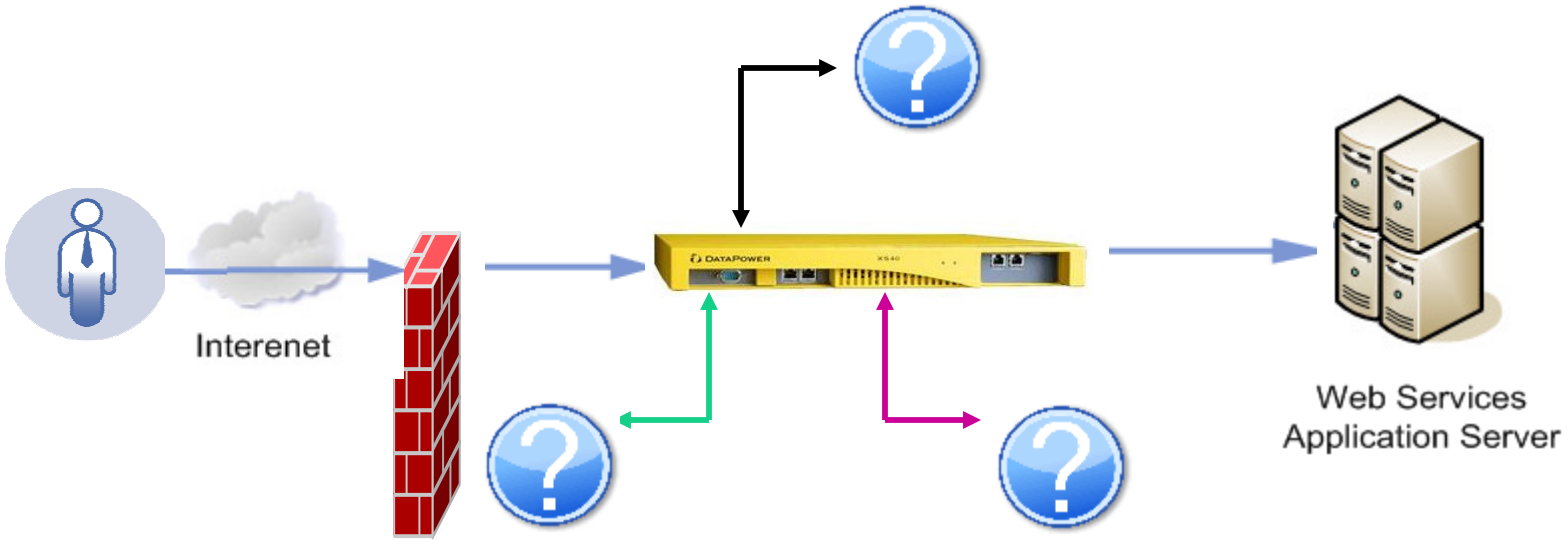
DataPower/Tivoli Work Together

- Tivoli Access Manager (TAM) & Tivoli Federated Identity Manager (FIM)
  - Widely-deployed access control solution
  - Full-featured federated identity management and Web Services Security solution
  - Act as PDP for making authentication and authorization decision
- Tivoli Security Policy Manager (TSPM)
  - Act as PAP, and provides full-featured policy authoring tool for WS-Security Policy, XACML
  - Act as PDP for making authorization decision
  - Distributes policy updates to Policy Distribution Targets (PDT) such as DataPower, WSRR
- DataPower XS40/XI50 XML Security Gateway
  - Most trusted, most widely deployed security hardware
  - Purpose-built, not based on general-purpose server or software
  - Performance & scalability for message processing
  - Act as PEP/PDP to enforce authentication, authorization, security policy requirement
  - Standards-based – SAML, XACML, WS-*
- Together protect XML Web services
  - Single IdM solution to control access for Web & Web services, XML and non-XML
  - Support for SAML, XACML, WS-Trust and other XML standards
  - Complete solution for XML security & business availability

Ready for IBM Tivoli. e-business software

Enterprise SOA

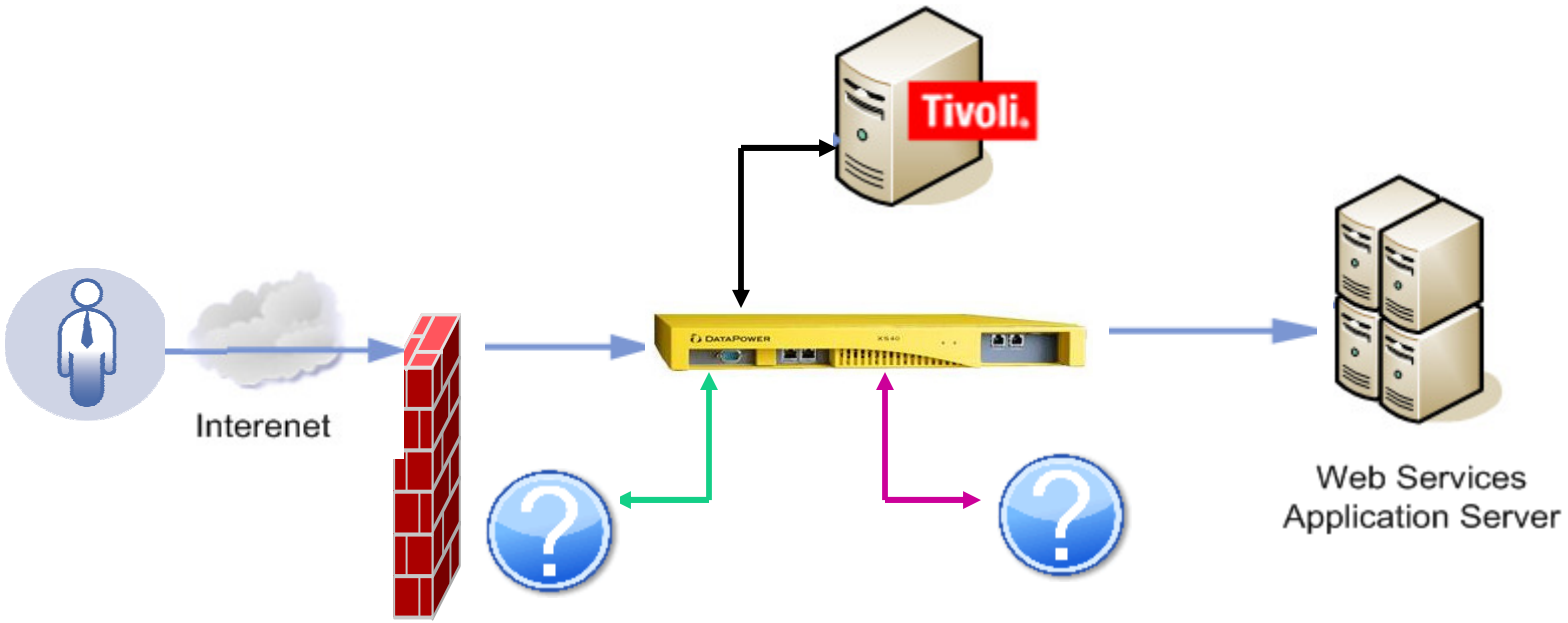
- **What are the policies to enforce [PAP, PDP]**
- For any given request
  - **Authentication ? [PDP, PEP]**
  - **Authorization ? [PDP, PEP]**
  - **Identity mapping ? [Federation]**



What are the policies to enforce [PAP]

Answer : Tivoli Security Policy Manager (TSPM)

Allow authoring of WS-Security Policy, XACML policy to be hosted by DataPower. DataPower will enforce policies.

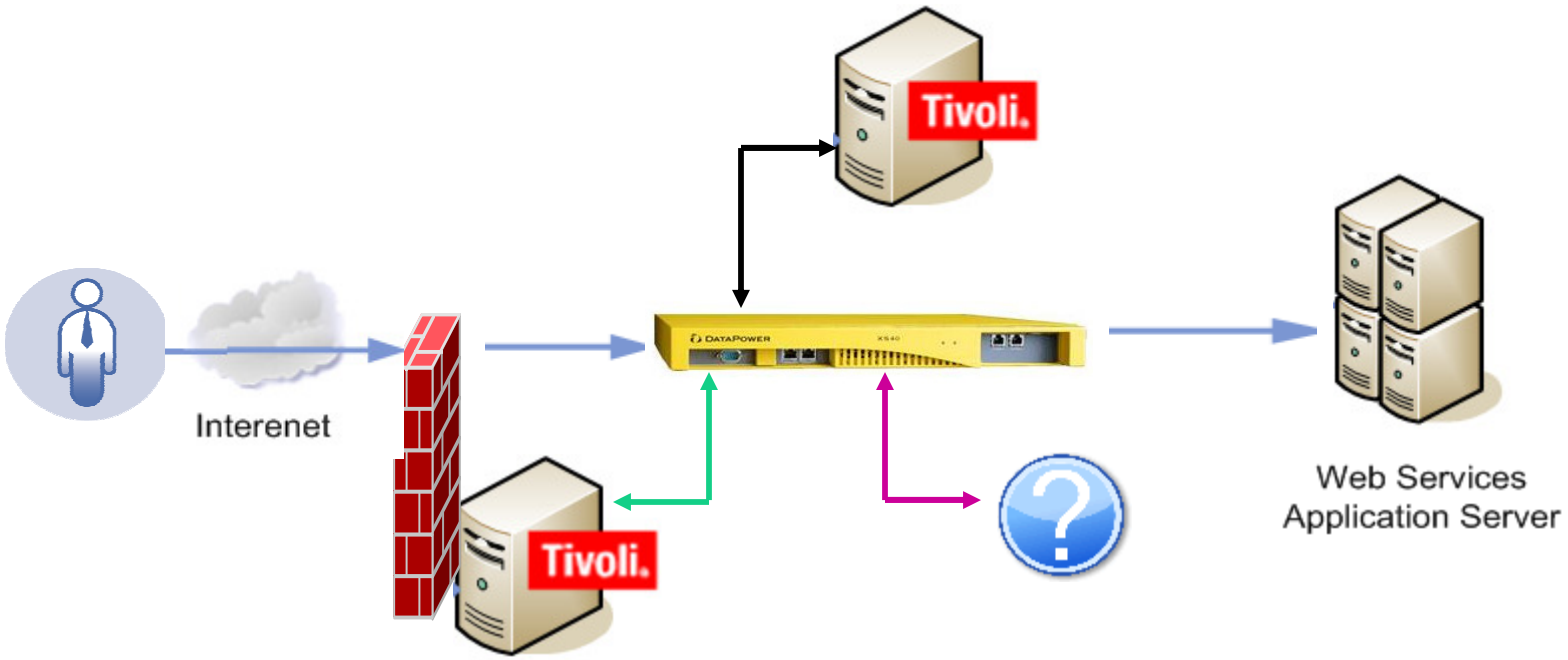


Authenticating and Authorizing a Request [PDP, PEP]

Answer : Tivoli Access Manager and/or DataPower

Provides a single point of decision making for making authentication and authorization. DataPower will enforce the decision.

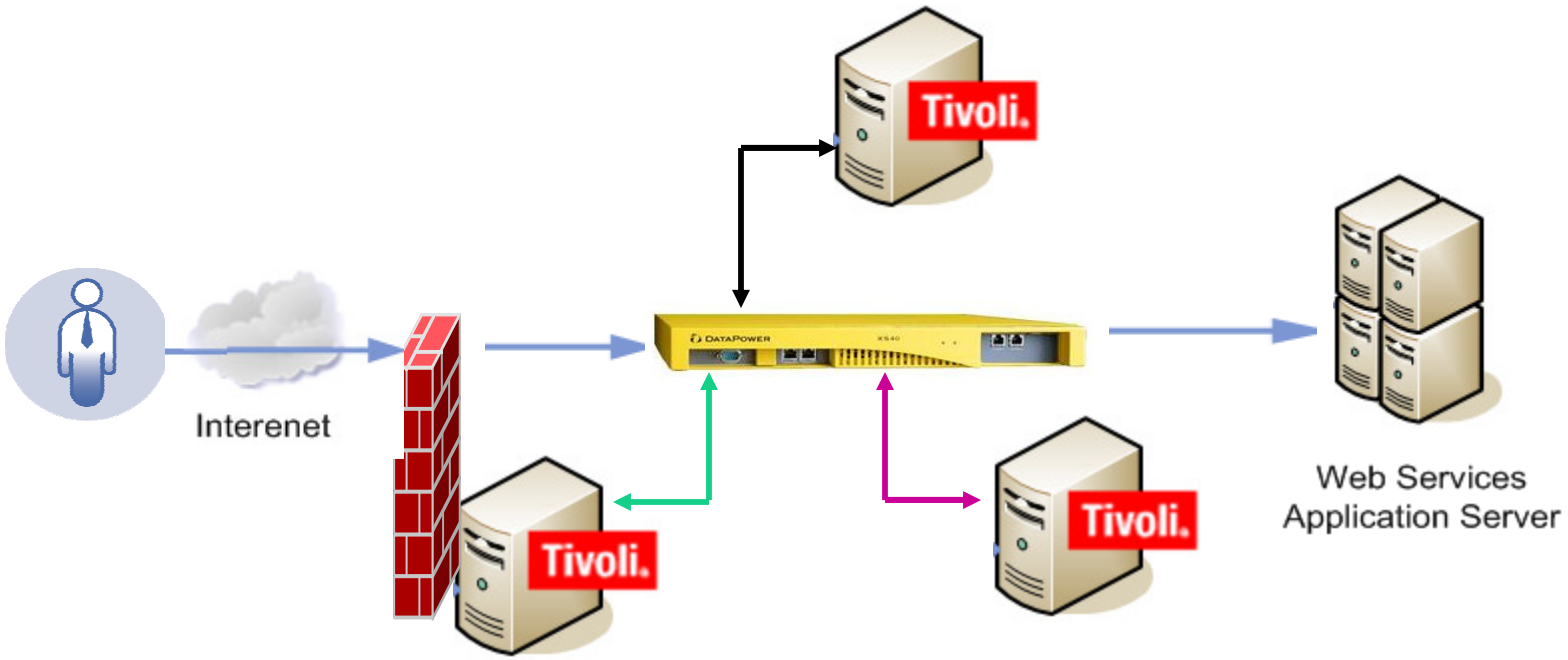
**** Optionally TSPM can act PDP for making Authorization decision**



Identity Mapping [Federation]

Answer : Tivoli Federated Identity Manager (FIM)

Provides an federated identity management, and it provides a single IdM enterprise solution



Enterprise Solution

- Tivoli Access Manager (TAM)
  - Widely-deployed access control solution
  - Act as PDP
- Tivoli Federated Identity Manager (FIM)
  - Full-featured federated identity management, single IdM enterprise solution
- Tivoli Security Policy Manager (TSPM)
  - Policy authoring solution and policy decision point
  - Act as PAP and PDP
- WebSphere DataPower
  - Act as PEP to enforce the policy, and acts as gatekeeper for the enterprise resources

Tivoli Access Manager WebSEAL

- Tivoli Access Manager (TAM) WebSEAL
  - Widely-deployed native-code HTTP reverse security proxy
  - Authentication, authorization, Web SSO, session management
  - Tight integration/caching with TAM Policy Manager (AA & Policy cache)
  - Uses TAM session credential, LTPA
  - Strong authentication mechanisms, step-up, step-down, reauthentication
  - Strong redirect, URL filtering & rewriting capabilities (i.e. Javascript URLs)

- DataPower
  - Reputation as “XML” appliance no longer so much true
  - Recent firmware enhancements have greatly improved Web app proxying ability
  - Some of these were done in conjunction with Tivoli
  - Useful when more complex requirements in play (i.e. multiple protocols)

- Often both are used side-by-side or in cascaded fashion
  - DataPower in front for SSL termination, threat protection, content filtering, validation, crypto, load balancing
  - WebSEAL for items listed above (caching, redirect, rewrites)
  - Both have integration with TAM, LTPA, and other security standards

Agenda

- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

Business-to-Business (B2B) Choices

- WebSphere Partner Gateway
  - Consolidated B2B Gateway based on the WebSphere platform, for a broad range of requirements
  - Extensive trading community management and additional protocol support
  - Supports Internet standards to connect partner systems, such as EDIINT AS1, AS2 and AS3; RNIF Version 1.1 and 2.0; cXML; CIDX Chem eStandards, Version 4.0; and ebMS, Version 2.0
  - Available in Express, Enterprise and Advanced editions

Business-to-Business (B2B) Choices

- WebSphere Transformation Extender Trading Manager
  - Universal Transformation for complex industry standards
  - Supports the latest versions of X12, EDIFACT, and HIPAA and includes a performance enhanced EDIFACT subsystem
  - Requires WebSphere Transformation Extender with Launcher and benefits from at least one of the X12, EDIFACT, TRADACOM or HIPAA Industry Packs.

Business-to-Business (B2B) Choices

- WebSphere DataPower XB60 B2B Appliance
  - Application Integration with standalone B2B Gateway capabilities supporting B2B patterns for EDIINT, AS1, AS2, AS3 and Web Services
  - Drummond AS2 Certified for interop with 20+ B2B vendors/platforms
  - Step up from XI50, can add application integration capability
  - Hardened appliance for DMZ-ready B2B interactions
    - Important as trading is often done with partners, whom you may not want to allow past the DMZ
    - Transaction viewer can be set up for partner access in DMZ

Business-to-Business (B2B) Choices

- Look to DataPower for:
  - Requirements for B2B function, governance, security in the DMZ
  - B2B within a simple ESB framework with embedded B2B protocols
  - No desire to extend the product with custom protocols or integration points
  - B2B separate from the WebSphere Application Server framework
  - Requirements around EDIINT, AS1, AS2, AS3
- Look to WPG for:
  - Requirements for many B2B and Integration Adapters that can be added on top of a WebSphere ESB or BPM applications
  - Wish to only purchase the B2B functions that are required
  - Need to extend with custom protocols or integration points
  - Requirements for EDIINT AS1, AS2 and AS3; RNIF Version 1.1 and 2.0; cXML; CIDX Chem eStandards, Version 4.0; and ebMS, Version 2.0
- Look to WTX/TM for:
  - Existing WTX infrastructure/skills
  - Requirements for X12, EDIFACT, and HIPAA formats

Business-to-Business (B2B) Choices

- Federated B2B Patterns
  - Typically these involve DataPower XB60 in the DMZ, in conjunction with WPG or WTXTP in the back-end zone
    - Deploy XB60 with MQFTE for B2B enabled Managed File Transfer
    - Deploy XB60 with WTX-TM for end-to-end EDI Processing
    - Deploy XB60 as B2B entry point for BPM and ESB solutions
    - Supplement WPG by offloading security and advanced Web services functions to XB60
    - WebSphere Partner Gateway supplemented by WTX Trading Partner

Agenda

- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

Low-Latency Messaging Choices

- MQ LLM
  - One of the newest members of the WebSphere MQ family
    - Along with MQ File Transfer Edition
  - Compliments existing MQ family technology
  - Software product to facilitate high-volume, low latency (sub-millisecond) messaging with flexible and reliable delivery, high availability, and persistence (lightweight message store)
  - Unicast, multicast, TCP, UDP

Low-Latency Messaging Choices

- DataPower XM70 Appliance
  - Hardened LLM in rack-mount 1U appliance form factor
  - Extreme volume 1M txn/sec, microsecond latency unicast/multicast messaging
  - Configuration-driven approach to LLM
  - Messaging protocol bridging (MQ, JMS, TIBCO RV & EMS)
  - Reliability
    - WebSphere MQ LLM Reliable and Consistent Message Streaming (RCMS)
    - Tibco Certified Message Delivery (CM)

Low-Latency Messaging Choices

- Look to the DataPower XM70 for:
  - Transport/protocol/messaging bridging
    - MQ/RV/EMS/JMS/LLM
  - DMZ requirements
  - High-performance add-ons to messaging requirements (crypto, xform, etc)
- Look to MQ LLM for:
  - Back-end LLM requirements, particularly in pure MQ environments

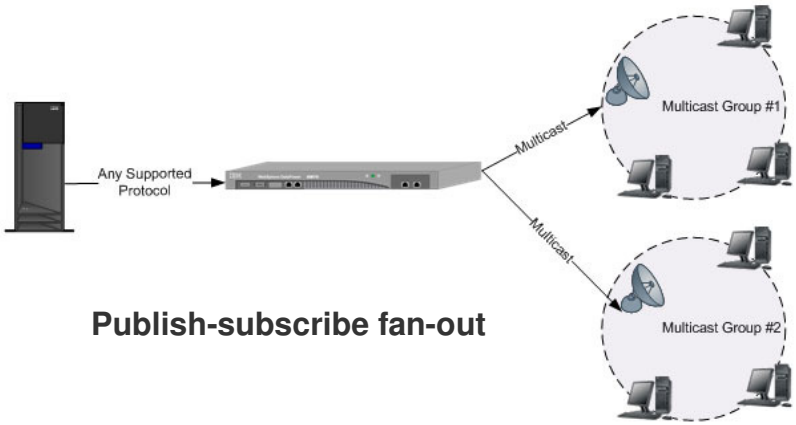
XM70 Low-Latency Messaging Patterns

from DataPower XM70 Use Cases and Patterns (REDP-4515-00 @ibm.com/redbooks)

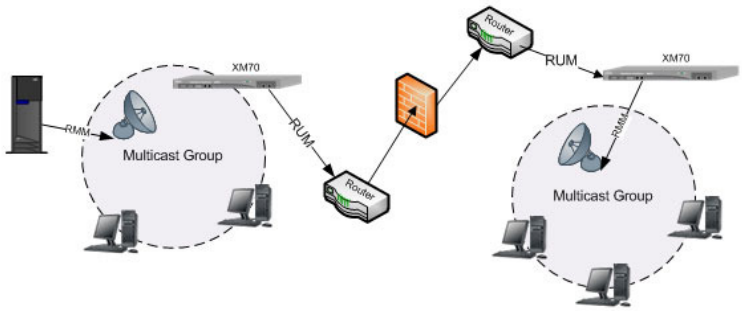
Point to point

Point to point fan-out

Publish-subscribe



Publish-subscribe fan-out



Publish-subscribe relay

Agenda

- Introduction
- Enterprise Service Bus Choices
- Web Proxy Choices
- Security Intermediary Choices
- B2B Platform Choices
- LLM Messaging Choices
- Wrap-up

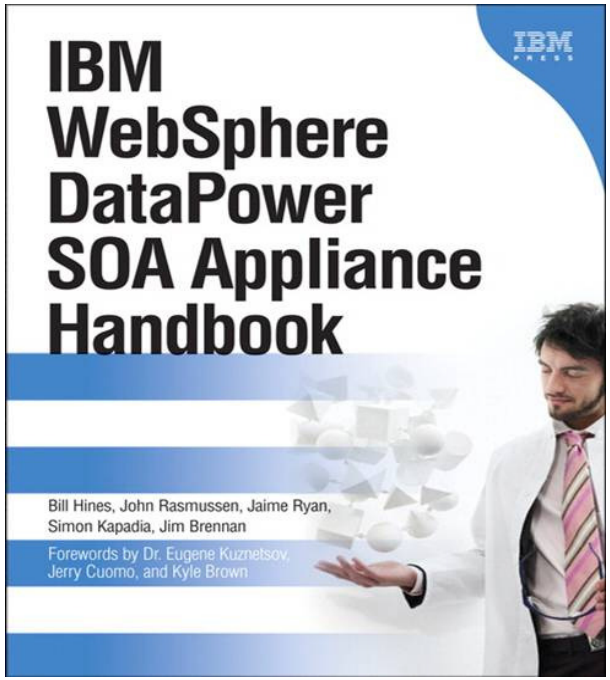
Wrap-up/Conclusion

- Often the “right choice” is some combination of products
  - Each performing their specialized roles – i.e. DMZ/perimeter security/transformation
  - For some functionality (particularly security) a layered approach is best
- Options will change as products evolve, new products emerge

WebSphere DataPower – IBM Appliances for Smarter Connectivity

- **Many years of appliance experience**
  - **Mature, growing products & capabilities**
  - **Army of experienced, knowledgeable support & field consultants**
- **A well established business model**
- Established Resources:
- **IBM DataPower Web Page (support, technotes, doc)**
- http://www-01.ibm.com/software/integration/datapower/
- **DeveloperWorks DataPower Discussion Area**
- http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1198
- **IBM Redbooks:**
- http://www.redbooks.ibm.com/cgi-bin/searchsite.cgi?query=datapower
- **External Publications →**
  - http://www.amazon.com/gp/product/0137148194?ie=UTF8&tag=dph-20&link_code=as3&camp=211189&creative=373489&creativeASIN=0137148194
- **Vast library of published articles:**
  - Http://www.ibm.com/developerworks

www.ibm.com/software/integration/datapower



THANK YOU

Copyright and Trademarks