Using WebSphere DataPower SOA appliances to extend the value of System z assets

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both. For a complete list of IBM trademarks please visit www.ibm.com/legal/copytrade.shtml

CICS	IBM Logo	S/390
DB2	IMS	Tivoli
E-business logo	iSeries	VM/ESA
ESCON	MVS	VSE/ESA
eServer	OS/390	WebSphere
FICON	pSeries	z/OS
IBM	Rational	zSeries
	RS/6000	System z

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. Microsoft trademark guidelines

Intel is a registeredtrademarksof Intel Corporation in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Agenda

- WebSphere DataPower product line overview

- WebSphere DataPower XI50 as an ESB

- What's new in the latest release?

SOA: Unlock business value.
→ New software and services.

WebSphere DataPower SOA Appliances

An SOA Appliance…

Creating customer value through extreme SOA connectivity, performance and security

- **Simplifies** SOA and accelerates time to value
- **Helps secure** SOA XML implementations
- **Governs and enforces** SOA/Web services policies

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.

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*

- **Enables run-time SOA governance and policy enforcement**
  - *Impact: dynamically control service availability, security, performance, and endpoint selection*

- **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*

- **Proven Green / IT Efficiency Value**
  - *Example: Appliance performs XML and Web services security processing as much as 72x faster than server-based systems*
  - *Impact: Same tasks accomplished with reduced system footprint and power consumption*

WebSphere DataPower SOA Appliance Product Line

LLM Appliance XM70 (4Q08)

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

B2B Appliance XB60 (4Q08)

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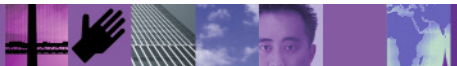- Simplified management and configuration

Integration Appliance XI50

- Hardware ESB
- "Any-to-Any" Conversion at wire-speed
- Bridges multiple protocols
- Integrated message-level security
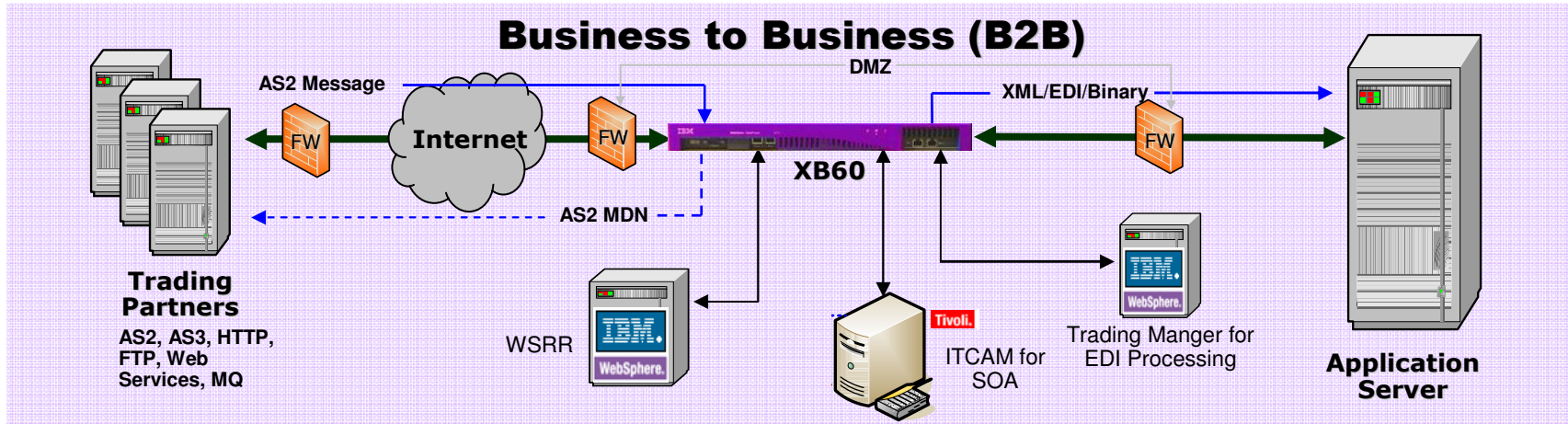
XML Security Gateway XS40

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

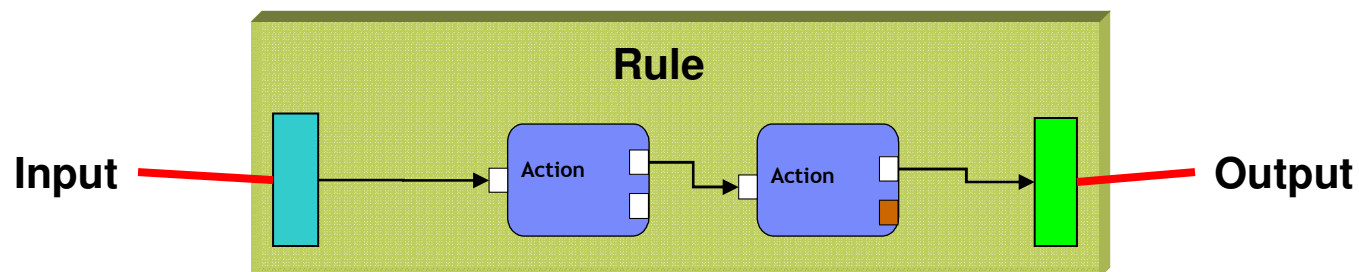# IBM SOA Appliance Deployment Basic Examples

Integration & Governance

→
HTTP XML REQ

HTTP XML RESPONSE
←

REPLY Q

→ **LEGACY REQ**

LEGACY RESP
←

XI50

Web Services Client

WSRR

ITCAM for SOA

Tivoli.

Security

Internet　　**IP Firewall**

XS40

Application Server

Tivoli Access Manager

Federated Identity Manager

Tivoli.

Acceleration

Client

Client or Server

Internet

XML HTML WML

XA35

XML XSL

Application Server Web Server
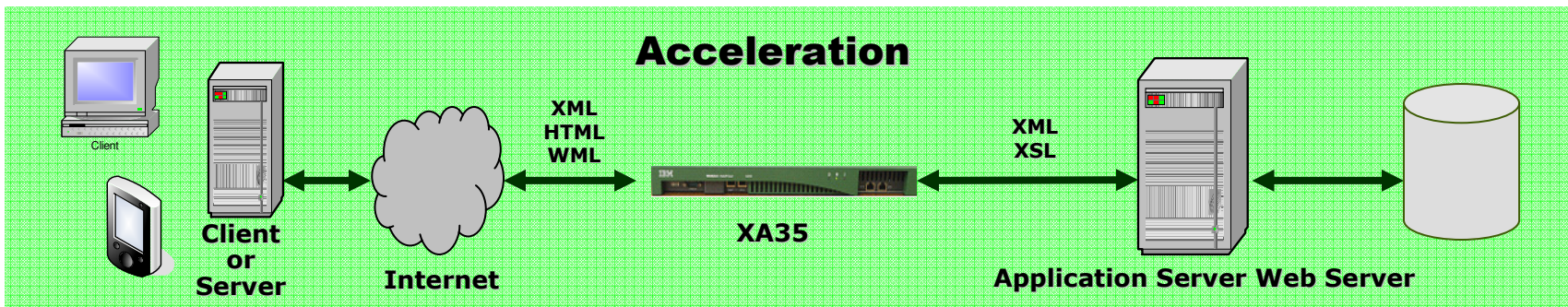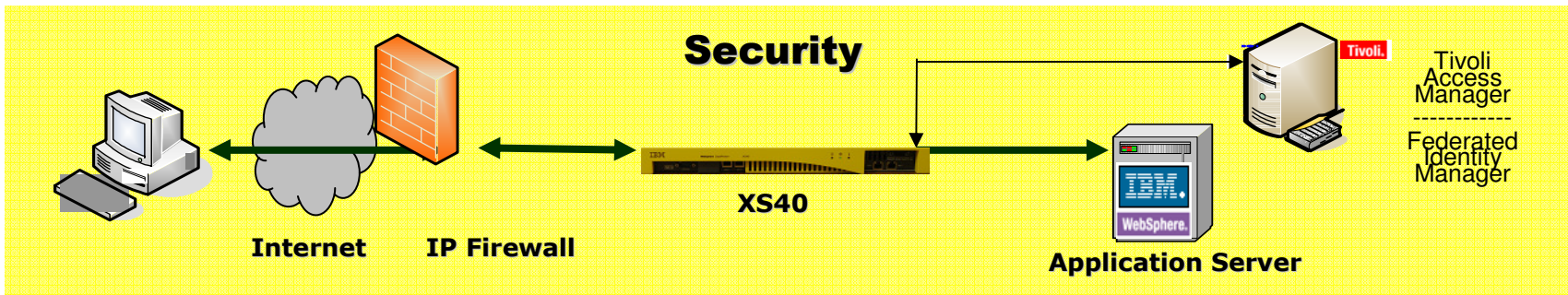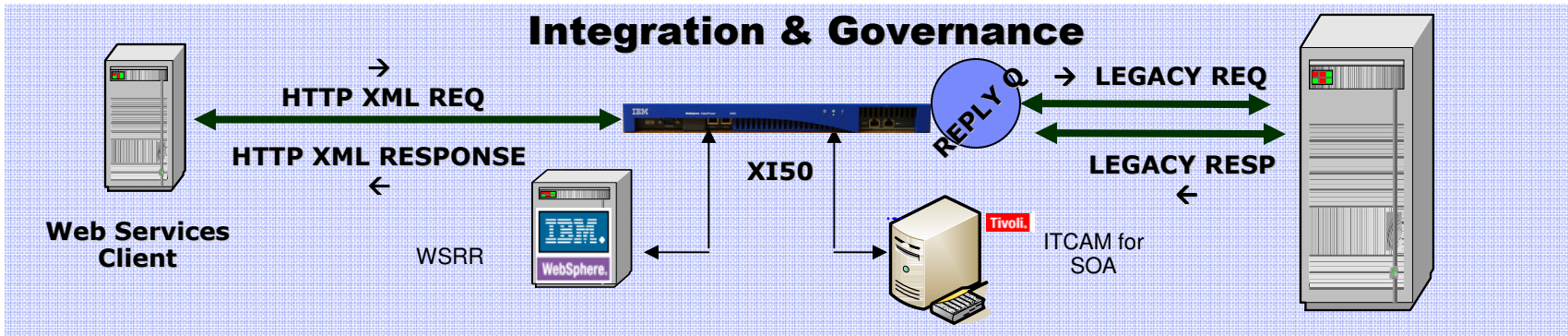
B2B and Low Latency Deployment Scenarios

Business to Business (B2B)

DMZ

AS2 Message

XML/EDI/Binary

FW   Internet   FW   XB60   FW

AS2 MDN

Trading Partners

AS2, AS3, HTTP, FTP, Web Services, MQ

WSRR

ITCAM for SOA

Trading Manger for EDI Processing

Application Server

Low Latency Messaging (LLM)

Receiver

RMM

Receiver

Transmitter

RUM

(unicast)

XM70

RUM

Receiver

Transmitter

RMM

(multicast)

MQ/TIBCO

MQ/TIBCO
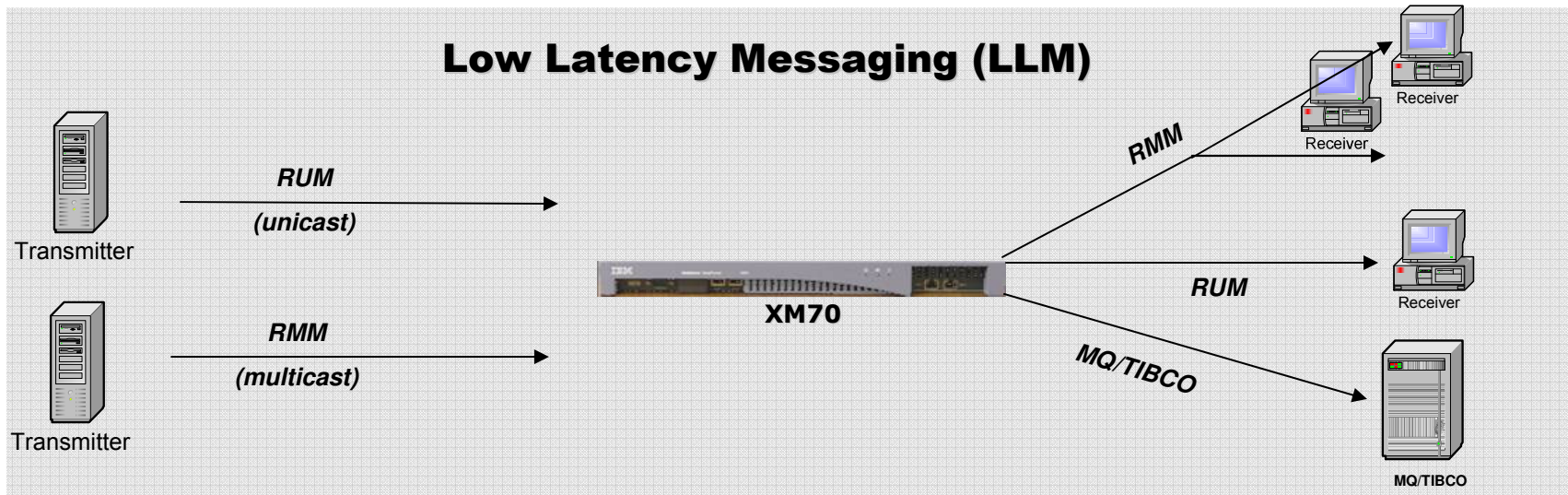
DataPower XI50 as an ESB - Concepts

- DataPower = "container" for rules

- Rule = deployable unit of mediation, definition of mediation
  - Input = means of getting message into message flow
  - Output = means of getting message out of message flow

- Action = atomic unit of message processing

Rule

Input ➝ → Action → Action → ➝ Output

Integration Appliance XI50

Middleware Appliance Purpose-Built for Application Integration

- DataGlue "Any-to-Any" Transformation Engine
- Content-based Message Routing:
- 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, metadata or network variables
- Data Validation:
  - Approve incoming/outgoing XML and SOAP at wire speed
- 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)

Simple Appliance Configuration for *Complex* Functionality

Fits into your existing environment

- **Address broad organizational needs** *(Architects, Developers, Network Operations, Security)*

- **Complete Configuration from GUI or CLI interface**

- **IDE integration / Eclipse plug-in**

- **XPath / XML config files**

- **SNMP**

- **SOAP management interface**

Access Control
AAA Framework Diagram - Authenticate, Authorize, Audit

DataPower AAA Framework

SOAP/ XML Message

Extract Resource

Web Service URI
SOAP op name
Transfer amount

Map Resource

SAML assertion
Non-repudiation
Monitoring

Extract Identity

SAML
WS-Security
SSL client cert
HTTP Basic-Auth

Authenticate

Map Credentials

Authorize

Audit & Accounting

SOAP/ XML Message

External Access Control Server or On-Board Policy
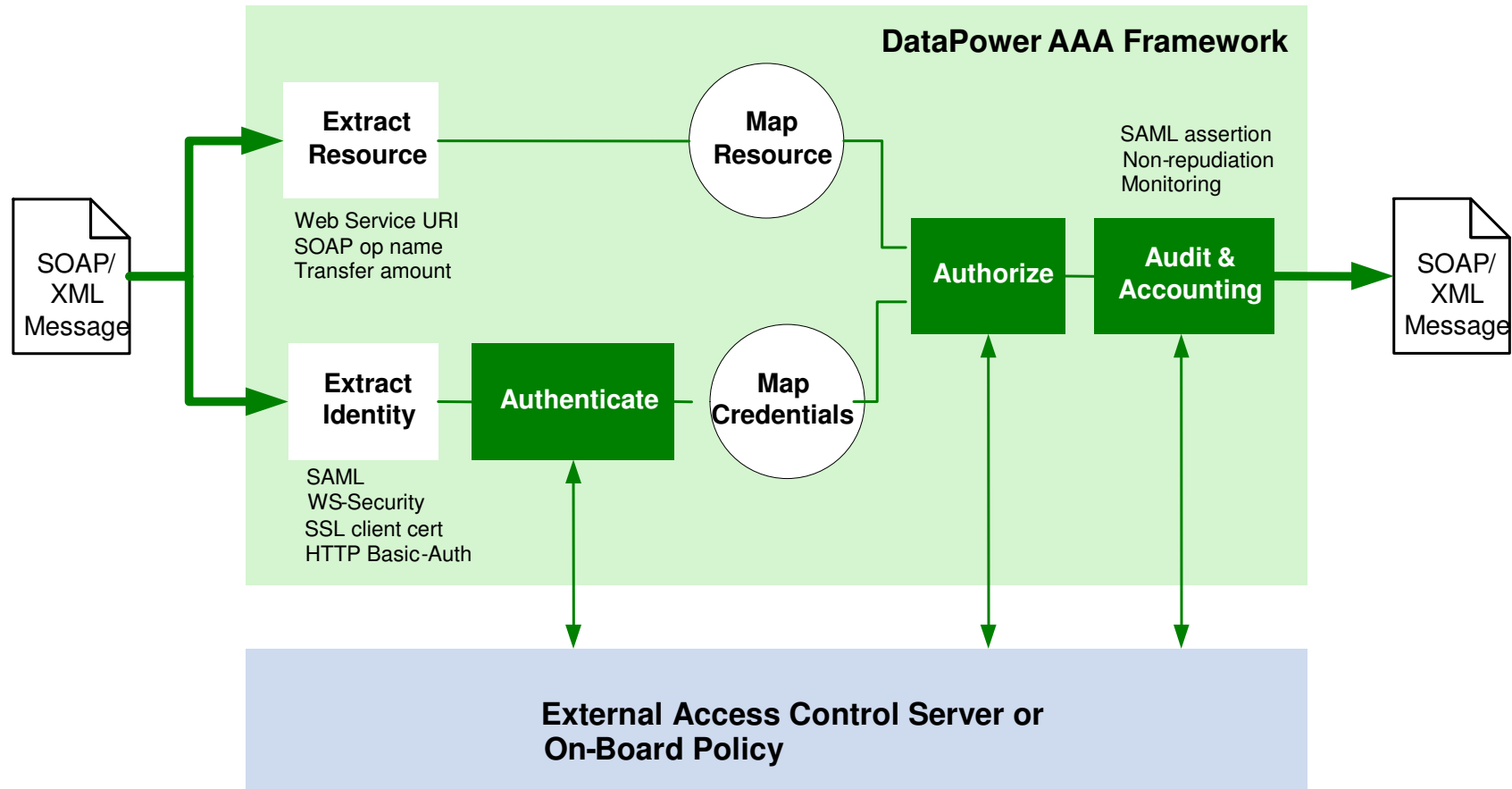
*Enforce Who can access Which service & When*

Access Control (2)
XACML, an open standard for fine-grained authorization policy

- XACML (eXtensible Access Control ML) open standard
  - Expresses complex, fine-grained access control policy rules in XML
  - Enables distributed policy enforcement throughout the network
  - Allows policies to be moved between different vendor systems
  - Defines PEP (enforcement), PDP (decision), PAP (admin) and PIP (information)
- XS40 and XI50 leverage their core XML engine for XACML processing (XACML doc similar to XSLT, XSD, WSDL)
  - High performance, robust caching and familiar administration
  - Not a XACML server or authoring environment
- Flexible and extensible
  - Base bias, deny-biased, permit-biased, custom obligations
  - Integrated into AAA Framework
- For complete enterprise XACML solution, add IBM Tivoli products

App. Request   **XACML Request**

XACML Query/Response   **XACML Policy**

PEP   **PDP**   **PAP**
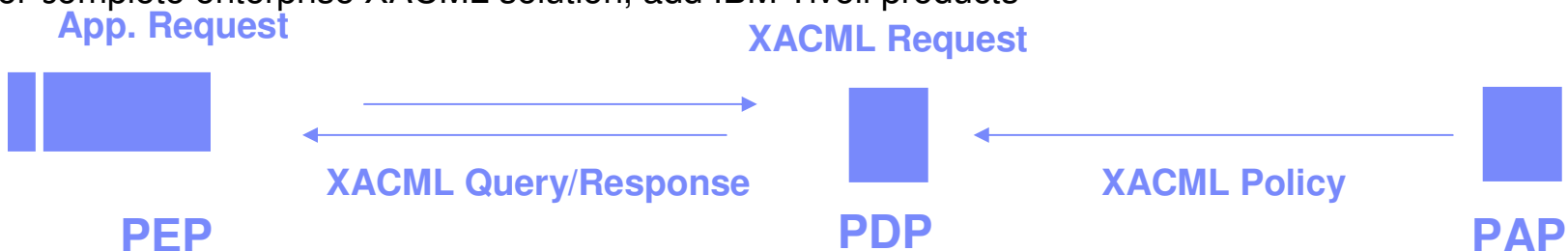
MultiStep & XML Routing
Flexible Drag & Drop Message Processing and Policy Creation

- **Basic routing capability similar to XML Filtering**

- **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 (incl. 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

Web Services Management
Service Level Management

- **Easy to use WSDL-driven graphical interface**

- **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**

- **Events / Notifications via WSDM, WS-Management, SOAP API and integration with ITCAM for SOA**

- **Allow subscription to SLM for alerts, logging, etc.**

Web Services Management (2)
Web Services Management Framework

- **Powerful framework enables easy integration:**

- **Centralized Management:**

  – Integrates with UDDI Registry, Dynamic Discovery (push configuration of a new service)

  – Enforce/Pull policies for execution on the XS40

  – Unified Dashboard (e.g. IBM Tivoli Composite Application Manager)

  – WSRR (WebSphere Service Registry & Repository) Integration

- **WSDM (Interop with IBM, HP, Tibco and Hitachi):**

  – WS-Addressing, WS-BaseNotification, and WS-ResourceProperties

  – Manager obtaining operation status and metrics from XS40 for Web service

  – Manager subscribing to notification from XS40

 – Manager informing the XS40 to bring web service down then up
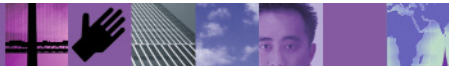
Web Services Management (3)
## Service Virtualization

- **Web services security best practice:**
  - Create abstraction barrier between internal and external Web services
  - Especially important for auto-generated web services
  - Helps with varying standards support between partners, versioning, availability, and scalability

- **WSDL-centric design:**
  - WSDL Versioning: Automatically retrieve updated internal WSDL and update external one

- **Multi-layer:**
  - Optionally, internal/external transport-layer proxy (e.g. MQ in XI50)
  - Dynamic routing
  - SOAP header stripping / rewriting
  - Payload transcription & wirespeed schema transformation

- **Very XML processing intensive**
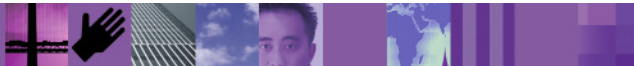
Web Services Management (4)
Registry/Repository Support & SOA Governance

- **Use of a central repository can facilitate Discovery and Reuse of Web services:**

  - WSRR and UDDI supported today

- **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 for SOA:**

  - Central management console

  - Polls device at set intervals

  - Traffic inspection, statistical analysis
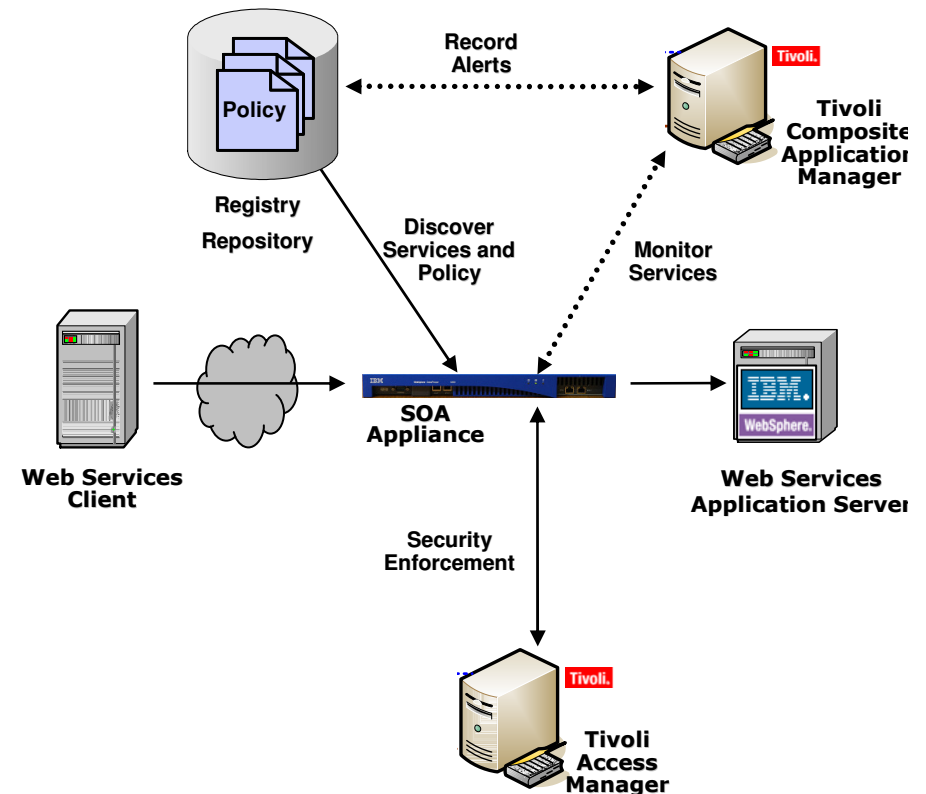
DataGlue's "any-to-any" Transformation

- **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**
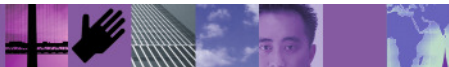
Content-based Routing Features

- **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.

Routing Policy

IBM SOA Appliance

Unclassified Requests

Service Providers
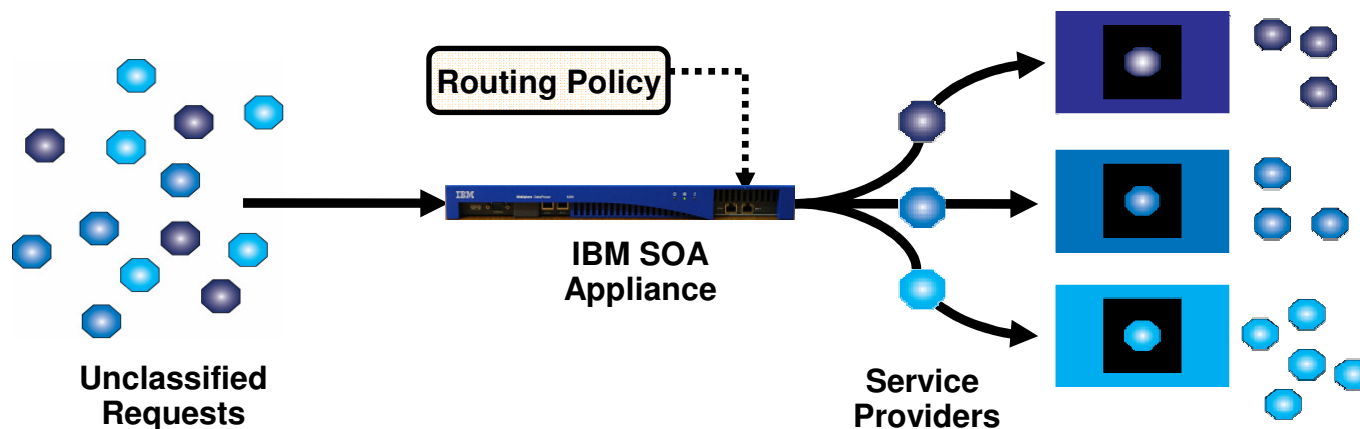
Protocol Bridging

- **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**
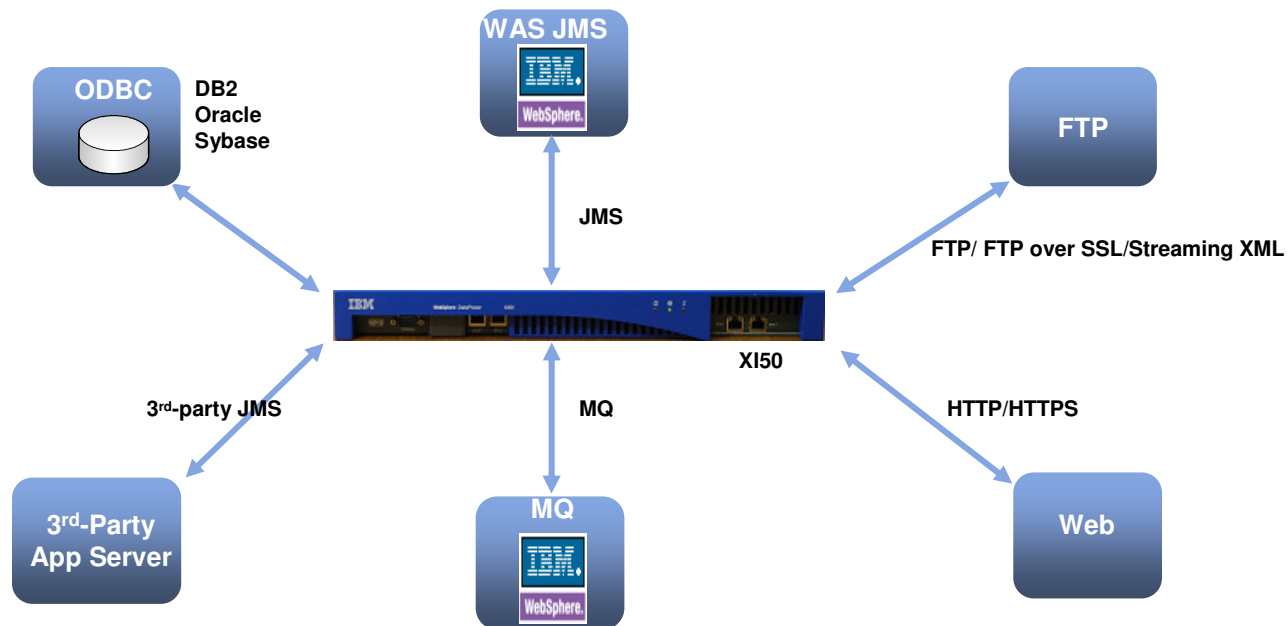
DataPower and System z Integration

- Web Services enablement and security for CICS and IMS applications

- DataPower XI50 acts as a services gateway to host-based applications

  - Web Services and XML security

  - Web Services management and service level agreements

  - Tight integration with WebSphere MQ on Z for connectivity and reliability

  - Any-to-any transformation (e.g. SOAP/XML to Cobol Copy Book) for simplified legacy integration

  - Protocol mediation and bridging – variety of inbound/outbound protocols – HTTP, HTTPS, MQ, WAS JMS, Tibco EMS, FTP, FTP/SSL, NFS, Database

  - Easy Configuration & Management:

    - WebGUI, CLI, IDE and Eclipse configuration to address broad organizational needs (Architects, Developers, Network Operations, Security)

DataPower for CICS and IMS Web Services

- **Web Services Security and Management for CICS and IMS web services**

SOAP/HTTP

Client

**System z**

IMS SOAP Gateway

CICS Web Services

- Content-based Message Routing

- Protocol Bridging (HTTP, MQ, JMS, FTP, etc.):Request-response and sync-async matching

- XML/SOAP Firewall: Filter on <u>any</u> 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.

- 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)
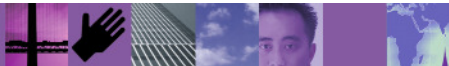
DataPower for DB2 on System z

- Simply, secure and accelerate Web Services processing
- Helps establish DB2 on z as the data hub for the enterprise
- Compute cycle intensive XML and security-related processing (especially re Crypto)
- Additional processing capabilities: XML firewalling and threat protection, web services management , service level management, protocol bridging
- Appliance model: improved consumability
- High performance Web Services processing and mapping to SQL/CALL
- DataPower communicates with DB2 via DRDA
- DB2 and DataPower tooling support

Web Services Consumers

DataPower DB2 WebServices Appliance

SOAP/REST

DRDA

DB2 on z
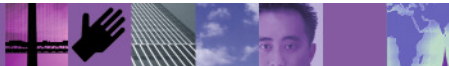
What's New in WebSphere DataPower SOA Appliances v3.7.1 –

- **Centralized policy and governance between WSRR and DataPower**
  - WSRR administrator submits WS-Policy and WSDL
  - DataPower subscribes to and enforces Policy on WSDL endpoints
- **Policy-driven security and flexibility improvements**
  - Policy-driven SSL client cert validation
  - AAA cache invalidation improvements for performance and policy enforcement
  - LDAP bind-search-rebind semantics useful for large LDAP repositories (for example)
- **WebSphere family enhancements to satisfy a greater class of applications (financial services, etc.)**
  - MQ Ordered messaging improvements
  - MQ browse, better sync point support, more automated ReplyQ behavior, better backout queue support
  - WTX interop
- **Configuration file handling for better production elevations**
  - Profiler to identify non-standard practices
  - Environment-specific configuration mediation components (IP addresses, variables)
- **Interoperability with other products for even better heterogeneous environment support**
  - Database stored procedure return value support
  - WS-Security Policy interop testing and validation with Microsoft .net and BEA WL 10
  - ActiveDirectory search improvements for role-based management
- **Tibco support improvements**
  - Active/passive server config
  - Improved LB/failover behavior
- **Connectivity enhancements**
  - Better url-open timeout control, per-transaction timeout, non-XML input size reporting
- **Other Usability, Serviceability improvements for better operations**
  - MOTD and banner support, CLI Wizard, SNMP ease-of-use etc.
  - Domain deletion safety, Ethernet interface disable control
  - Better workflow with in-situ file viewer / edit, Internal Load Balancer programmatic control

MQ Backout Queue, comprehensive support

Added the ability to retrieve message backout settings from an MQ server.

New in 3.7.1

Retrieve Backout Settings

- **on** - Use backout settings from the MQ server.

- **off** - Do not use backout settings from the MQ server. Use backout settings in the MQ Queue Manager object.

Configure MQ Front Side Handler

Main

MQ Front Side Handler

[Apply] [Cancel]

Name	_____	*
Admin State	● enabled ○ disabled	
Comments	_____	
Queue Manager	(none) ▼ [+] [...]	*
Get Queue	_____	*
Put Queue	_____	
CCSI	0	
Get Message Options	4097	
Exclude Message Headers	☐ CICS Bridge Header (MQCIH)	
	☐ Dead Letter Header (MQDLH)	
	☐ IMS Information Header (MQIIH)	
	☐ Rules and Formatting Header (MQRFH)	
	☐ Rules and Formatting Header (MQRFH2)	

connection... 1

Polling Interval	30	seconds
Header to extract Content-Type	None ▼	
Retrieve Backout Settings	○ on ● off	

What's New in WebSphere DataPower 3.7.2?

- **Enhanced Interoperability** with WTX, TAM and TFIM

- **Improved Serviceability** for configuration, deployment, operability and administration

- **Additional Connectivity** for file transfer and direct DB

  – Support for DB2 v9.1 on z/OS, Oracle 11g

- **More Robust Security** for System z and CC EAL4
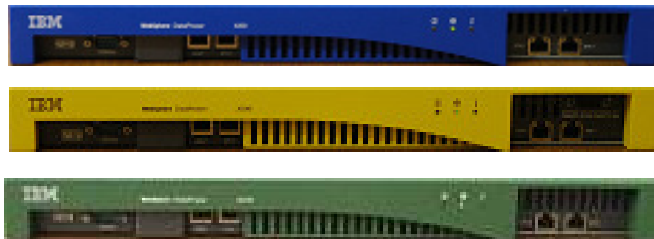
SOA Appliances: Creating customer value through extreme SOA performance and security

- **Integrates** SOA with specialized devices
- **Accelerates** SOA with faster XML throughput
- **Helps secure** SOA XML implementations
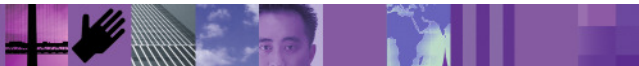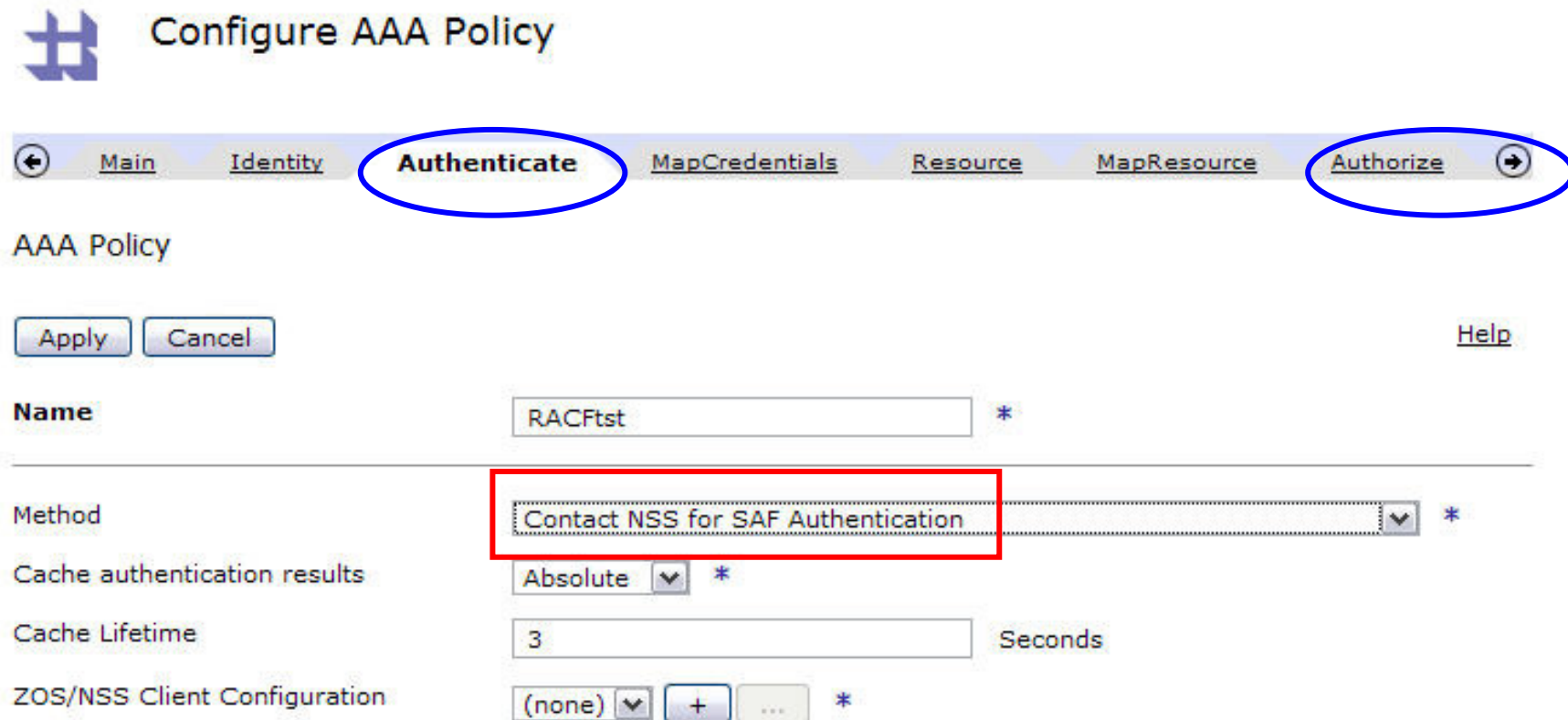
RACF Support

- RACF (Resource Access Control Facility) is a security system that provides access control and auditing functionality for the z/OS and z/VM operation systems.

- DataPower version 3.7.2 includes adds support for RACF, the IBM implementation of the Security Authorization Facility (SAF). RACF provides authentication and authorization through z/OS® Network Security Services (NSS).

  – RACF authentication is available using:

  - AAA policy
  - Extension functions
  - RBM

  – RACF authorization is available using:

  - AAA policy
  - Extension functions

  – Firmware 3.7.2 is compatible with:

  - z/OS Communications Server, V1R10

RACF – How to create a AAA policy

- RACF is configured within the AAA Policy under the Authenticate or Authorize tabs when the user selects *Contact NSS for SAF Authentication (or Authorization)*

RACF – How to configure the z/OS NSS Client

- The z/OS NSS client enables integration with RACF on the z/OS Communications Server. The z/OS NSS Client object specifies the authentication information required to allow the DataPower appliance to function as an NSS client.

Configure z/OS NSS Client

Main

z/OS NSS Client

[Apply] [Cancel]   Help

Name	myNSSclient *
Admin State	○ enabled ● disabled
Comments	Profile for my RACF id
Remote Address	9.21.69.77 *
Remote Port	993 *
SSL Proxy	(none) ▼ [+] [...] *
Client ID	ZMCLIENT *
System Name	PROD *
User Name	JANEDOE *
Password	••••••••••
	•••••••••• *

RACF – Manage User Access via RBM

- The DataPower appliance manages access through role-based management (RBM).

  - RBM provides a flexible and integrated means to control whether an authenticated user has the necessary privileges to access resources through access policies.

- DataPower version 3.7.2, role-based management consists of the following capabilities:

  - Authenticating users

  - Evaluating the access profile

  - Enforcing access to resource

- RBM provides authentication to RACF through Security Authorization Facility (SAF).

  - In the Web GUI, select **saf** for User Authentication Method to use z/OS NSS Server for SAF authentication

MIB Group, Inc.
SOA Security & Integration

Challenge

- Difficult to modify home-grown custom software application
- Adopt SOA to enable an online Web service to greatly increase revenues, while reducing costs & increasing the security of the service

Solution

- Deployed WebSphere DataPower Integration Appliance XI50 for SOA security and to transform & route messages
- Acts as a gateway by forwarding messages to System z mainframe to be checked against database
- Integrates ACORD XML services with existing WebSphere MQ
- Integrates SchemaTron validate to generate XSLT to load the generated XSLT onto the XI50 for runtime execution & filtering

Benefits

- More than 10 times faster than internally developed custom software
- Fraud-protection processes are faster, more secure & less error prone
- Web service allows MIB to offer more services to customers while reducing overhead cost
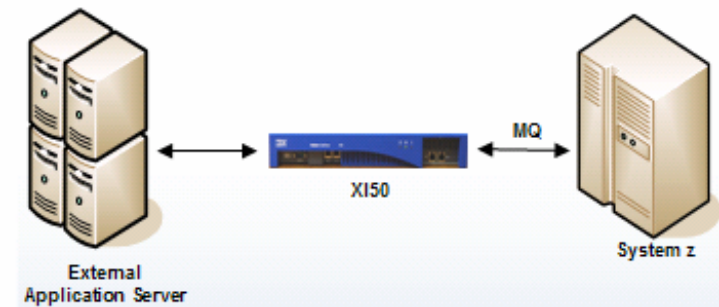
- **WebSphere DataPower Integration Appliance XI50**
- **WebSphere MQ**
- **System z**

Summary – IBM Specialized Hardware for Smart SOA Connectivity

- 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

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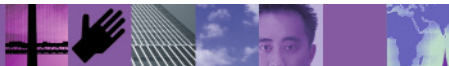
Thank You

Additional Information:
Example - Why do you need anything in front of a CICSWS?
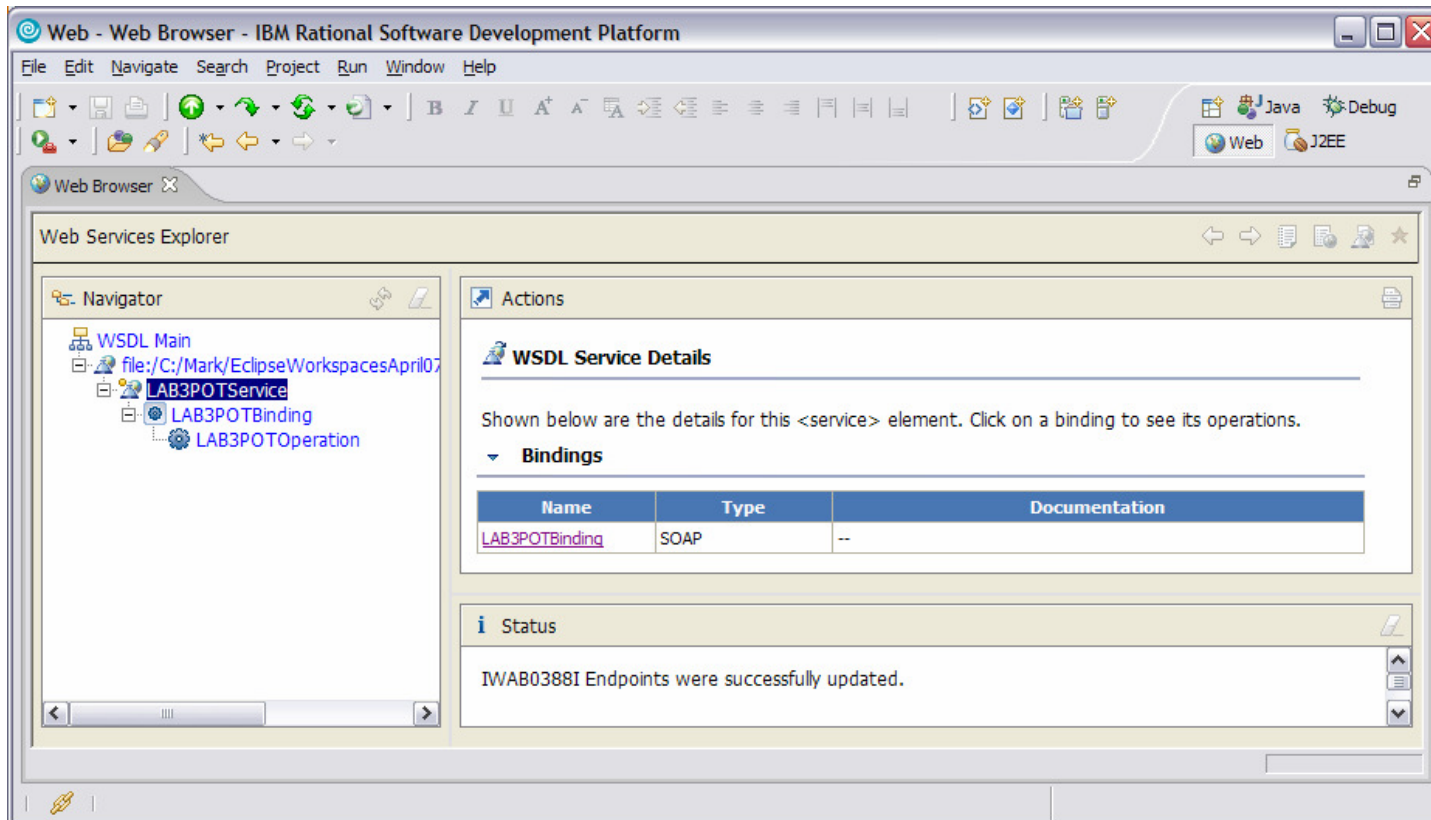
name

An example round trip: RDZ → Datapower → CICSWS

SLM Action: Check to see if more requests allowed through in this time period

Transform Action: Change "DFHCOMMAREA" to "getCustomer"

```
<?xml version="1.0" encoding="UTF-8" ?>
<SOAP-ENV:Envelope>
   <SOAP-ENV:Body>
      <q0:DFHCOMMAREA>
         <CustNo>7</CustNo>
      </q0:DFHCOMMAREA>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<SOAP-ENV:Envelope>
   <SOAP-ENV:Body>
      <q0:getCustomer>
         <CustNo>7</CustNo>
      </q0:getCustomer>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Transform Action: Change Content-Type: text/xml to Content-Type: text/xml; **charset=UTF-8.** If you don't the CICSWS will reject it.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope>
   <SOAP-ENV:Body>
      <cbl:DFHCOMMAREA>
         <CustNo>7</CustNo>
         <LastName>Barosa</LastName>
         <FirstName>Daniel</FirstName>
         <Address1>123 Calle Oro</Address1>
         <City>BuenosAirres</City>
         <State>AR</State>
         <Country>ARGENTINA</Country>
         <RetCode>0</RetCode>
      </cbl:DFHCOMMAREA>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Step 1: Import the WSDL from the CICS-2-WSDL process

Step 2: Setting up RDz for a second binding

3: Configure the Datapower MPGW

4. Press "GO" in RDZ and see the results in the Datapower probe

Clients send the web service request here. They think this the address of the mainframe – but it is not. It is Datapower's proxy address

This where Datapower forwards the call after executing the policy. The is the actual mainframe service endpoint.

5. Look at the processing policy for log 220769

The outside world calls it "getCustomer"

The CICS Web Service calls it "DFHCOMMAREA"

BEFORE transformation happens

Notice the step-by-step probe window!

AFTER transformation happens

5. Look at the system log and see all that happened

6. Another simple, little practical example – the content type

Question: *The outside world doesn't always play nice with CICSWS requirement for content type "text/xml; charset=UTF-8". RDZ and WAS usually place nice, but what about .NET, SOAPUI, oXygen, cURL, WebLogic Workshop, and many others?*

Answer: *RDZ worked. oXygen worked. SOAPUI failed. Curl failed unless you tweak it. I don't have .NET or weblogic workshop. So only 50% worked with the CICSWS and I didn't get to test the two others. That is why you need DP in front of your CICSWS. Many WS clients are badly behaved. CICSWS can't account for all their various bad behaviors. Despite the best effots of WS* interoperability working groups the problem gets worse as standards become more sophisticated (think WS-ReliableMessaging and WS-Policy). Datapower massages and normalizes these problems on behalf of CICSWS so they are no longer problems.*

BEFORE transformation happens

AFTER transformation happens

Additional Information:
DataPower Enhancements

name

Interoperability Enhancements

WebSphere Transformation Extender (WTX)

- **Comprehensive DataGlue Engine improvements**

  - Performance optimization

  - Support for multiple **WTX Map Modes**

  - New **DPA Map Type** for map files that were compiled in WTX using DataPower mode.

- **Compatibility with WTX Version 8.2**

  - Improved conformance and expanded capability in WTX Design Studio "DataPower Mode"

WebSphere software

Tivoli Access Manager and Federated Identity Manager

- **TAM Integration**

  – Added support for version 6.1 of IBM Tivoli® Access Manager (TAM). Use of TAM requires a license on the DataPower appliance.

- **TFIM Integration**

  – Added support for version 6.2 of IBM Tivoli Federated Identity Manager (TFIM)

Tivoli software

Serviceability Enhancements

Enhanced Operability and Serviceability

- **Robust and flexible instrumentation for operational analysis**

- **Parameterized system resource thresholds and fine granularity of system audit messages for improved operational management**

- **Auto hardware crypto detection for enhanced deployment**
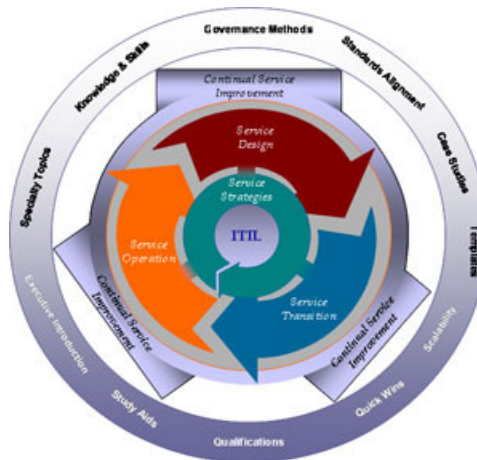
New WebGUI Look and Feel
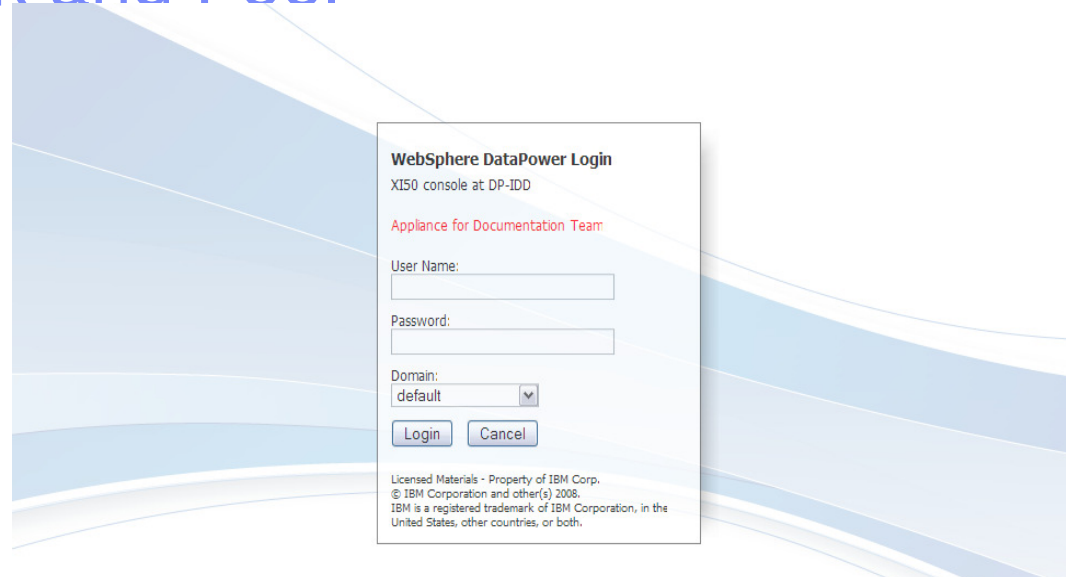
Connectivity Enhancements

Support for SFTP

- **Secure Shell (SSH) File Transfer Protocol (FTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream.**

  – Typically used with version two of the SSH protocol to provide secure file transfer.

  – It is often referred to as Secure File Transfer Protocol or SFTP.

- **SFTP is not FTPS**

  – FTPS refers to standard FTP protocol over SSL connection

    - This is already supported in DataPower

SFTP – Supported Clients & Protocols

- **Supported Clients**
  - CuteFTP Professional 8.3
  - OpenSSH 5.1
  - OpenSSH 3.p1 (Red Hat Linux 7.3)
  - OpenSSH 4.6p1 (Ubuntu Linux)
  - PuTTY PSFTP, version 0.60
  - SmartFTP, version 3.0
  - WinSCP, version 4.1.6

- **Supported Protocols**
  - SSH-2 protocol defined by IETF RFC 4251
  - SFTP version 3 defined by the draft-ietf-secsh-filexfer-02.txt Internet-Draft

SFTP – authentication/authorization checking

- **In this example, DataPower acts as a security policy enforcement point for protecting access to backend FTP data**

SFTP

Client/host
authentication

AAA

FTP server
Authentication/
authorization

FTP

Backend
FTP server
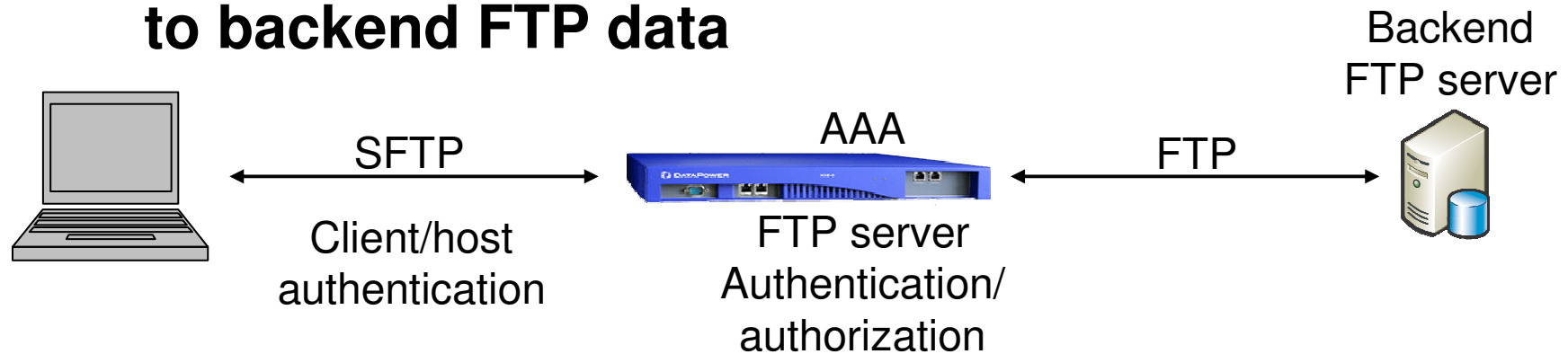
SFTP Server Front Side Handler configuration

- **Configuration of an SFTP Server Front Side Handler**

Main

SFTP Server Front Side Handler

[Apply] [Cancel]

Name	[_____] *
Admin State	⊙ enabled ○ disabled
Comments	[_____]
Local IP Address	[0.0.0.0] [Select Alias] *
Port Number	[22] *
Access Control List	(none) [▼] [+] [...]
Host Private Keys	(empty)
	[_____▼] [Add] [+] [...]
User Authentication	☑ Public Key
	☑ Password
	*
Allow Backend Listings	⊙ on ○ off
AAA Policy	(none) [▼] [+] [...]
Filesystem Type	Transparent [▼]
Default Directory	[/] *
Idle Timeout	[0] seconds

Database Connectivity Enhancements

- **Improved performance through comprehensive optimization**

- **Improved flexibility on connection managements**

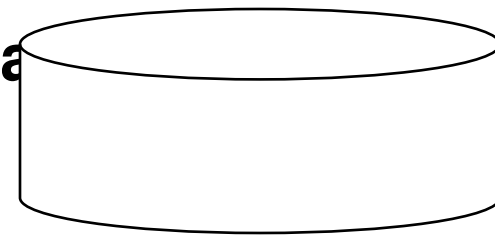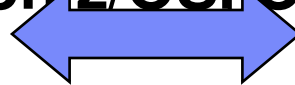- **Support for DB2 v9.1 on z/OS, Ora**

Additional Information: DataPower 3.7.2 Enhancements

name

Hardware Performance + Highly Customizable Configuration

- More future-proof solution required for today's emerging SOAs:
  - Evolving specifications, varied corporate policies, changing security requirements
  - Efficient Processing needed for XML Web services integration
  - High Customization required for broad-based SOA

- DataPower Agility ("DA") Architecture Enables Flexibility & Performance:
  - Advanced Patented XML Processing Engine for wirespeed performance
  - Customizable XML configuration files for highly flexible configuration
  - Easily adapts to changes in standards, service requirements and customer needs

- Benefits:
  - No need to wait for software or hardware code change, QA, and patch upgrade
  - Quicker time to market and reduced maintenance cost

Integration across the IBM Software Portfolio

- **Mature integration within WebSphere software portfolio**
  - *WebSphere MQ with WebSphere DataPower: 4+ years, numerous customers*
  - *Industry-leading SOA Runtime Governance with WSRR + DataPower*
 - *Many more examples: WTX for data maps, WS-Security for WMB*
  - *Auto-configure XML firewall by importing WebSphere service descriptors*

- **Complete SOA Security and Management solution with Tivoli products**

- **Robust enterprise integration through native DB2 and IMSConnect**
  - *Deliver data as Web services into new or existing SOA solutions with DataPower/Data Studio integration*

- **IBM Autonomic Integrati**

WebSphere. software

Rational. software

RAD, Eclipse

WebSphere MQ,
HTTP,
JMS,
Web Services

WSRR,
WTX,
WS-Security
WS-Policy

IMSConnect

TAM, TFIM,
ITCAM4SOA,
WS-Trust,
SAML,
XACML

LDAP,
SNMP,
Syslog,
AMP,
NetView

DB2 software

SQL, Xquery,
Data Studio

Tivoli. software
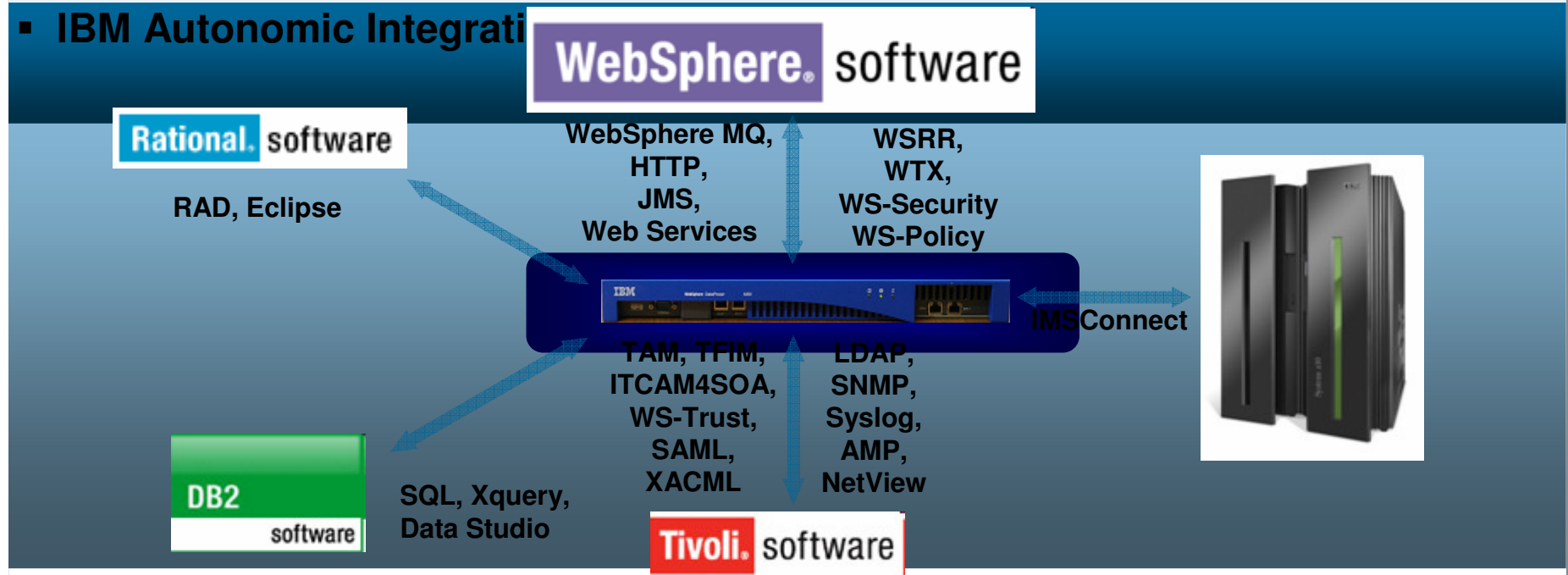
Integration with 3rd Party Vendors

- **Standards-based integration with third party vendors**

- **Tighter integration with some key competitors**

- **No platform dependencies – hardware or software**

- **Exceptional interoperability through industry profiles and te**
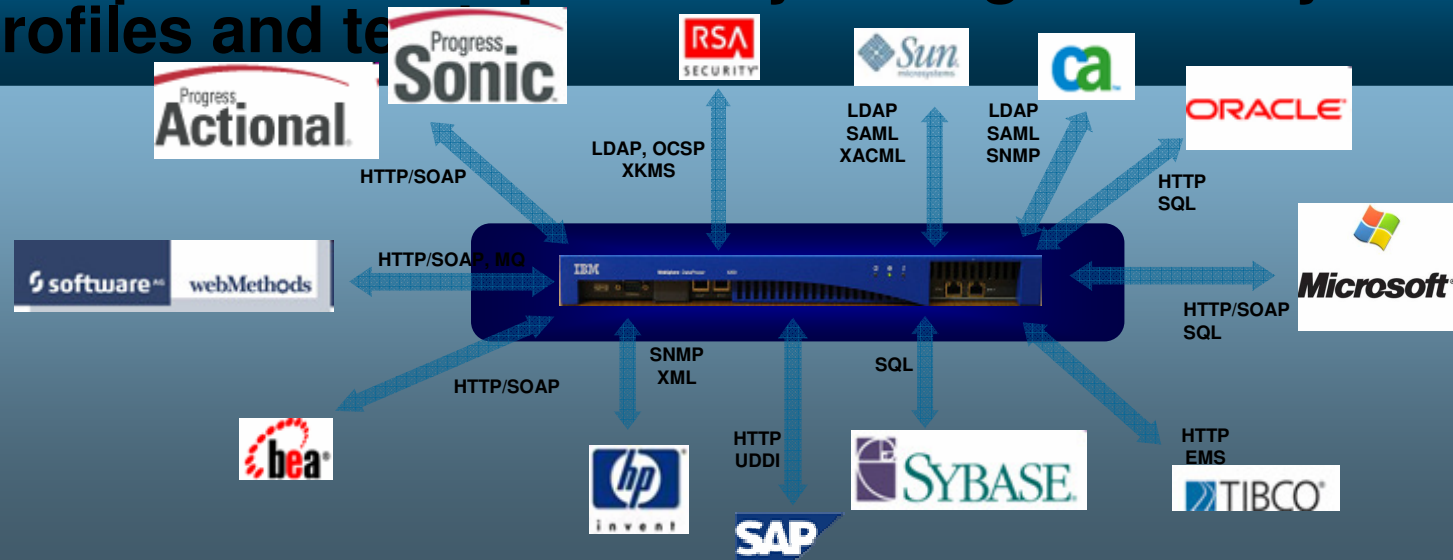
WebSphere DataPower Appliances Benefits

- Flexible Connectivity: **an XML appliance shields the applications from security requirements, protocol changes and service versioning - no application modifications needed**

- Reduce Complexity: **Replace software servers functionality with an XML appliance, reduce infrastructure footprint, and off-load heavy processes to dedicated XML appliances**

- Lower TCO: **Dedicated XML appliances have shown to reduce operational costs by as much as 50%**

- Improved Agility by Reduced Time to Market: **dramatically decrease the testing time and amount of development required to upgrade your environment, most policies are configuration driven as opposed to development driven**

- Reduce Risk: **the XML appliance provides the connectivity layer without requiring application modification, and delivers improved security and audit support**

- Configuration Driven: **The XML appliance is configuration driven to do policy definitions, it does not involve development to support your infrastructure**

International Automotive Manufacturer
Web Services Security Gateway & Lightweight ESB for SOA

Business Challenge

- Implementing Web services based SOA
- Ability to access services that will provide a list of known issues for each vehicle

Solution

- Implemented WebSphere DataPower Integration Appliance XI50 as an ESB

- Implemented WebSphere DataPower XML Security Gateway XS40 as a Web services proxy for verification, digital signatures, and authentication between Web server client and reverse proxy

- Integration of WebSphere DataPower & WSRR for service management

Benefits

- Deployed more than 100 new services since 2007
- Log files & SNMP alerts to HP OpenView
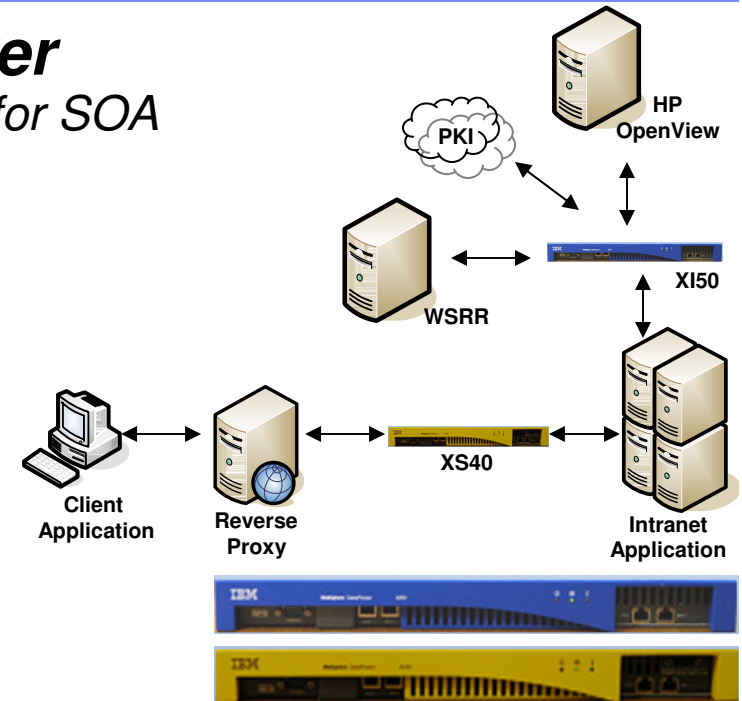
Software/Hardware

WebSphere DataPower Integration Appliance XI50

WebSphere DataPower XML Security Gateway XS40

WebSphere Service Registry & Repository

System z

Major US Investment Firm
## Web Services Security and ESB Infrastructure

Challenge

- 1) New web services security for internal and external application integrations and 2) replace existing ESB/RR Bus
- Previous ESB (called RR Bus) became unmanageable - 48 servers at end of 2007
- Increased load expected through 2008 as Home page traffic moved onto the RR Bus

Solution

- Web Services Security – 2 DataPower XS40 XML Security Gateway Appliances provide standards-based web services security for internet and intranet applications
- RR Bus – 4 DataPower XI50 Integration appliances replaced 48 existing servers to provide high-performance ESB for transactions with System z via SOAP/HTTP

Benefits

- Offered new service to business partners: Secure Web Services
- Simplification of the home grown routing solution – easier to support and maintain 4 XI50 appliances vs. 48 servers
- Lowered TCO by reducing ESB hardware infrastructure by 75%
- Forecasted ROI within 6 months
- High-performing routing of transactions to mainframe
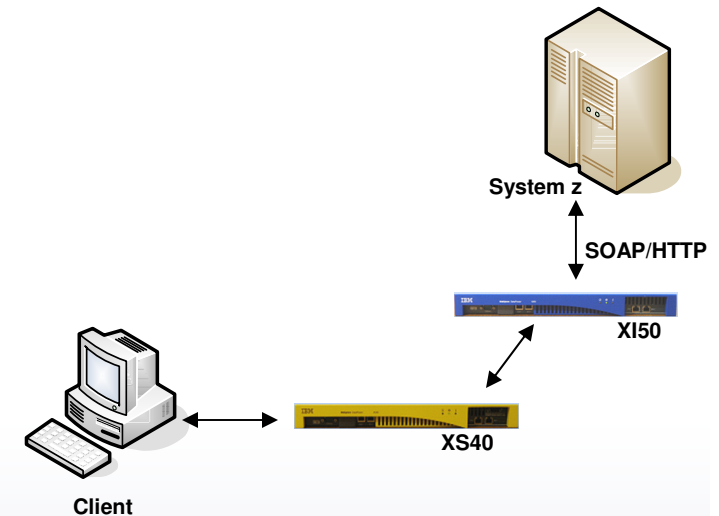
System z

SOAP/HTTP

XI50

XS40

Client

- **WebSphere DataPower Integration Appliance XI50**
- **WebSphere DataPower XML Security Gateway XS40**
- **WebSphere MQ**
- **System z**

What's New in WebSphere DataPower Integration Appliance XI50 *v3.6.1*

- **Expanded integration and connectivity**
  - Enhanced MQ support
  - Full support for WS-ReliableMessaging (WS-RX)
  - Additional support for VLAN and NFSv4
  - Enhanced support for WSRR and UDDI v3 registries
  - Full support for SOAP 1.2, WS-Security 1.1 updates
  - Integration with DB2 V9 pureXML

- **Enhanced governance capabilities**
  - Dynamic Web Services policy framework (WS-Policy and WS-Security Policy)
  - WS-I Basic Profile and Basic Security Profile support

- **Breakthrough enhancements for ease of use**
  - Streamlined Multi-step Transaction Processing
  - Expanded Quality of Service (QoS) support

Main

MQ Front Side Handler

[Apply] [Cancel]

Name	mq1 *
Admin State	⊙ enabled ○ disabled
Comments	
Queue Manager	test (MQ Queue Manager) ∨ [+][...] *
Get Queue	get *
Put Queue	put
CCSI	0
Get Message Options	0
Exclude Message Headers	☐ CICS Bridge Header (MQCIH) ☐ Dead Letter Header (MQDLH) ☐ IMS Information Header (MQIIH) ☐ Rules and Formatting Header (MQRFH) ☐ Rules and Formatting Header (MQRFH2) ☐ Work Information Header (MQWIH)
The number of concurrent MQ connections	1
Polling Interval	30 seconds
Header to extract Content-Type	MQRFH ∨
XPath expression to extract Content-Type from MQ header	[XPath Tool] *

WebSphere DataPower Enhancements
WS-Policy framework

- Flexible WS-Policy framework

  - Enables quick consumption of new and updated standard and custom WS-Policies for central enforcement and management via DataPower appliances

  - Supports WS-PolicyAttachment

    - Via embedded WS-Policy references

    - External attachment

    - WSRR

    - UDDI

  - Provides standard policy templates out of the box

    - WS-Security Policy

    - WS-ReliableMessaging Policy

WebSphere DataPower Enhancements
Multi-step Processing Enhancements

- Streamlined Multi-step Transaction Processing

  – Makes common processing patterns more consumable and easier to configure

– New and updated processing actions to support

  - looping
  - conditional branching
  - parallel processing
  - multi-way fan-out and aggregation
  - asynchronous processing of any action
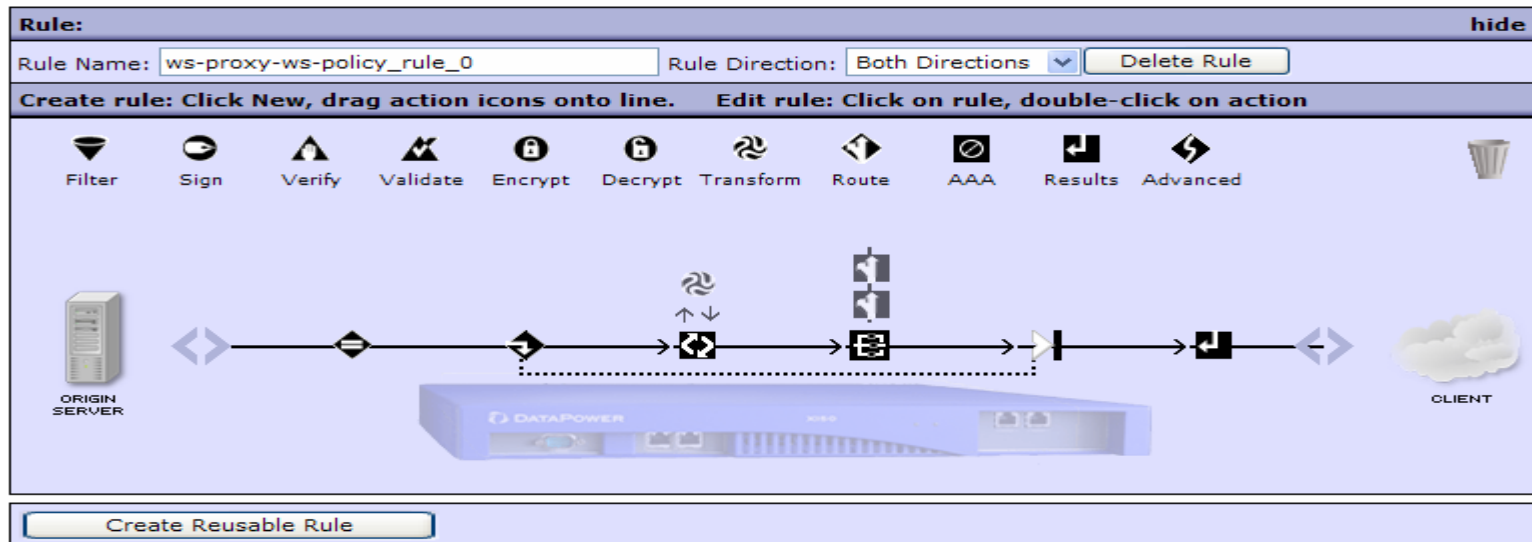
WebSphere DataPower Enhancements

Enhanced Connectivity

- Enhanced MQ connectivity

  – MQ connectivity performance optimizations

  – Simplified DP->MQ->CICS/IMS connectivity

  – Simplified parsing and generation of MQ headers

    • MQMD, MQRFH,MQRFH2, MQIIH, MQCIH, etc

    • Simplified use of MQ API

      – MQOD, MQOR, etc

- New support for NFSv4

  – Includes Kerberos support

- New support for VLANs

  – Allows easier deployments into existing network environments

Main

MQ Front Side Handler

[Apply] [Cancel]

Name	mq1	*
Admin State	⊙ enabled ○ disabled	
Comments		
Queue Manager	test (MQ Queue Manager) [+] [...]	*
Get Queue	get	*
Put Queue	put	
CCSI	0	
Get Message Options	0	
Exclude Message Headers	☐ CICS Bridge Header (MQCIH) ☐ Dead Letter Header (MQDLH) ☐ IMS Information Header (MQIIH) ☐ Rules and Formatting Header (MQRFH) ☐ Rules and Formatting Header (MQRFH2) ☐ Work Information Header (MQWIH)	
The number of concurrent MQ connections	1	
Polling Interval	30	seconds
Header to extract Content-Type	MQRFH	
XPath expression to extract Content-Type from MQ header	[XPath Tool]	*