IBM Software Group

Creating Customer Value Through Extreme SOA Performance And Security

Patcharee Nutthesri

WebSphere Specialist

patchare@th.ibm.com

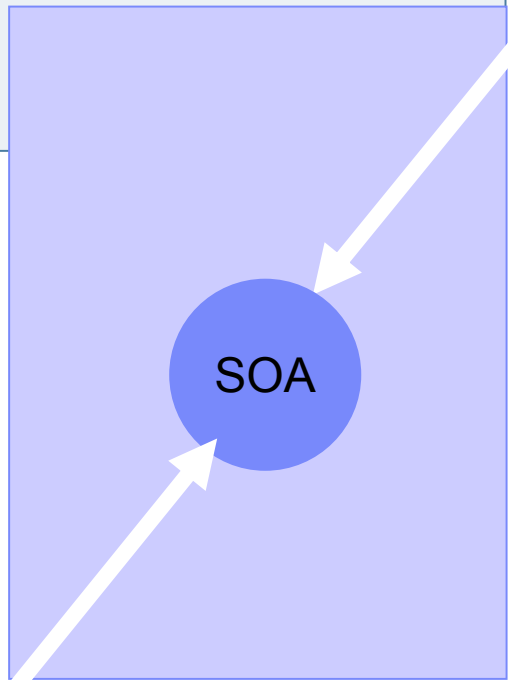
Overview

Challenges with XML & Web Services

Statement of Problem/Pain

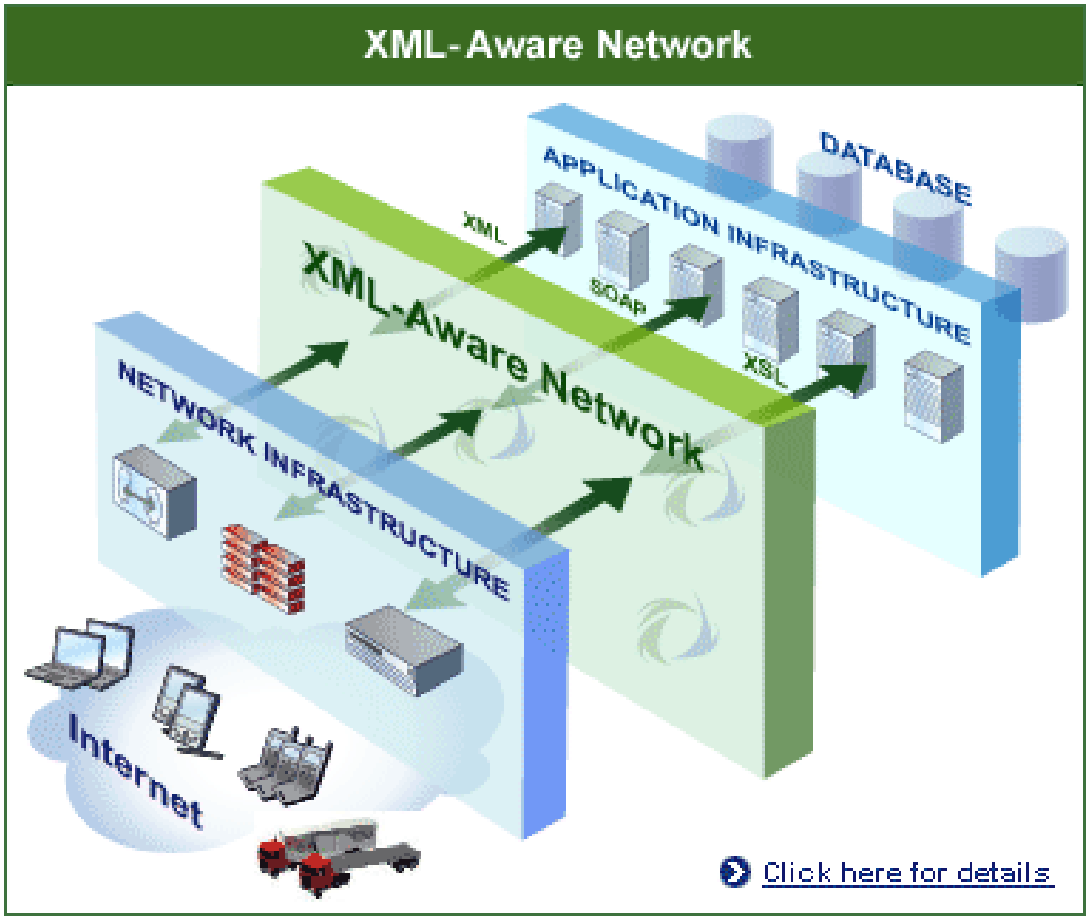
XML is the foundation of SOA, but brings new challenges:

- Scalability: XML is bandwidth, CPU, and memory intensive
- Performance: some XML apps literally grind to a halt
- Security: connecting systems never before connected
- Security: clear text over HTTP with no inherent security
- Integration: connecting Web services to legacy applications
- Standards are still in flux



- **Businesses want to move to standards-based XML…**but XML is bulky which can cause performance bottlenecks.
- **Businesses want to deploy secure XML-based applications**…but security adds further bulk to the application that slows it down.
- **Businesses want to integrate their new Web Services to each other and to existing legacy applications…**but they don't want to do it point to point because that diminishes the flexibility that SOA is supposed to bring.

What is XML-aware Networking

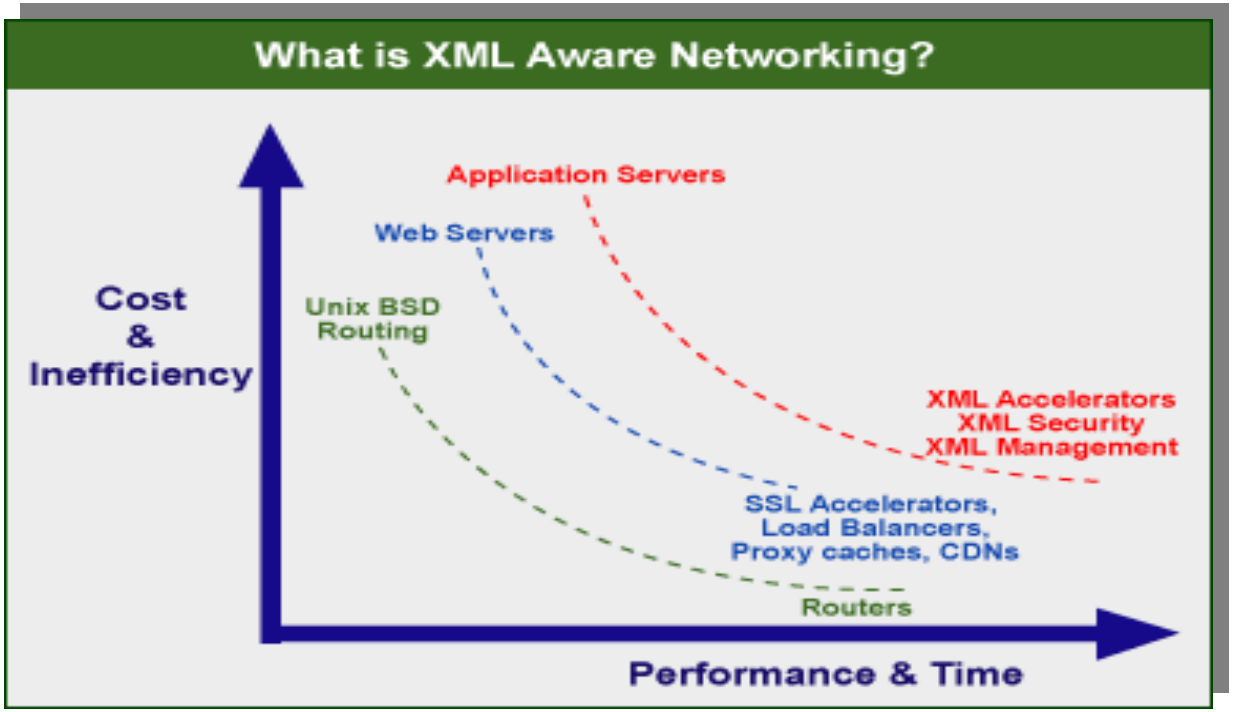


Offload XSLT processing, XPath routing, legacy-XML conversions and other resource-intensive tasks from servers to the network layer.

This reduces latency, improves throughput, and frees up computer resources.

Result:
The Performance, Security, & Manageability that you expect from your IP network is available for your XML applications.

"Commodity" Processes Migrate to Appliances



- Historical trend is for software functions that are simple, yet require a lot of computing power, to move into dedicated appliances.
- Part of a larger trend that initially started by moving functions such as Traffic Routing and Load Balancing into hardware.
- XML/Web Services processing tasks such as Security, Application Routing, Transformation, Management are rather simple, but very CPU intensive.

Why an Appliance for SOA?

- Hardened, specialized hardware for helping to integrate, secure, and accelerate SOA.
- Many functions integrated into a single device.
- Higher levels of security assurance certifications require hardware.
  - Government FIPS Level 3 HSM
  - Common Criteria
- Higher performance with hardware acceleration.
  - Enables use of processor intensive functionality without burdening business servers.
- Simplified deployment and ongoing management.

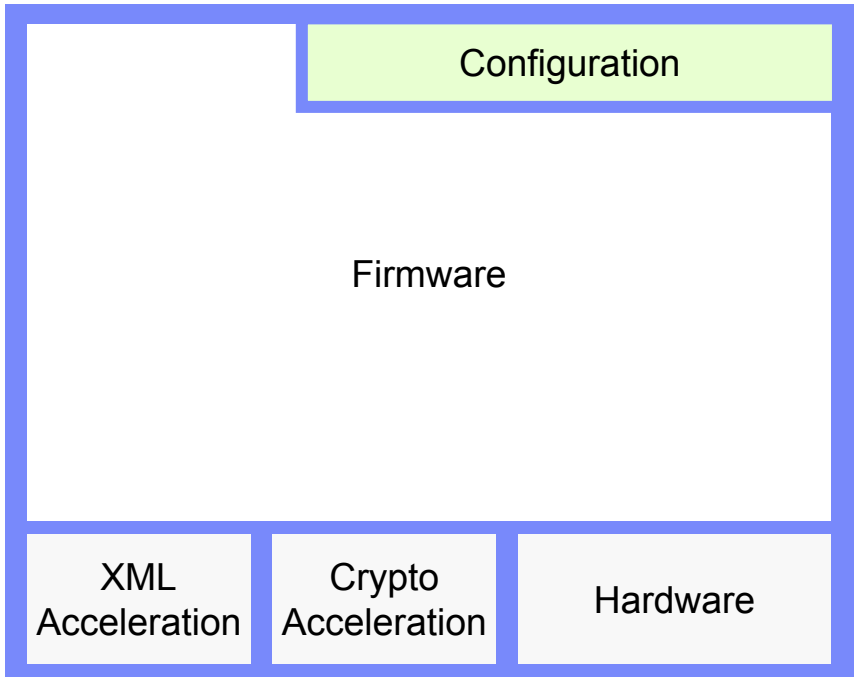
What Does DataPower Address ?

- XML Performance
  - How ? – by offloading XML processing from the Application Server to DataPower in optimised hardware
  - Thereby greatly reducing the required number of Application Servers
- XML Security
  - How ? – by offloading XML security to DataPower
  - Provide standards based security – WS Security
- Integrating XML and legacy systems
  - How ? – by using DataPower to transform XML to legacy message formats and protocols e.g
    - XML < > Cobol Copybook (brings a Mainframe into SOA Architecture)
    - XML > HMTL (renders HTML content to Portal very rapidly)
    - XML < > MQ Messaging

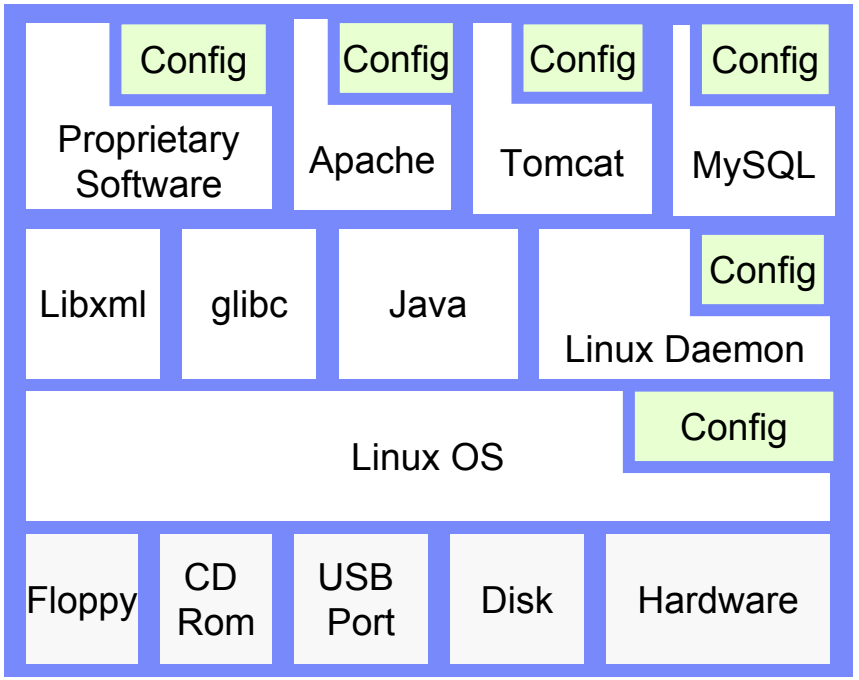
All of this is done at WIRESPEED

Advantages of an Appliance vs. Software Only Solution

WebSphere DataPower Appliance

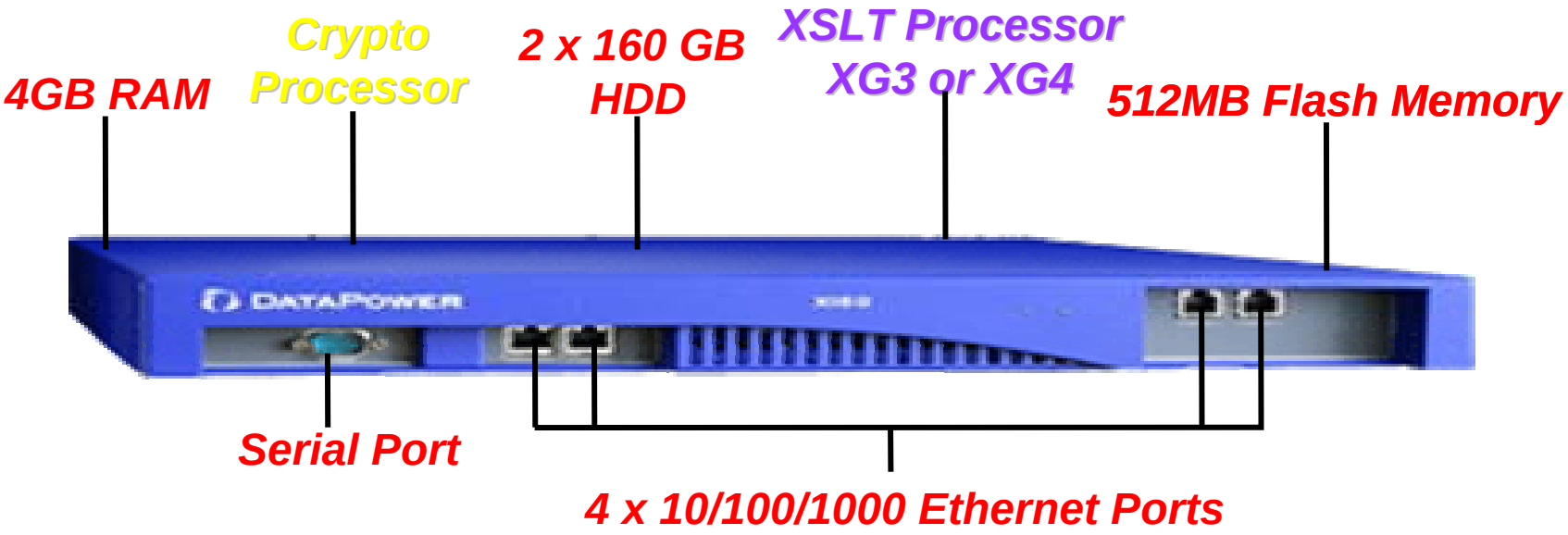


Software Stack on a Typical Server



- Optimized hardware, firmware, embedded OS
- Significantly less moving parts, no complicated software stack
- Security vulnerabilities eliminated (e.g. no open source, Trojan horses, Java/C++ libraries)
- No drives/USB ports, tamper-proof case, lock-down configuration
- Much higher performance, easier to configure, more secure, and cheaper to maintain

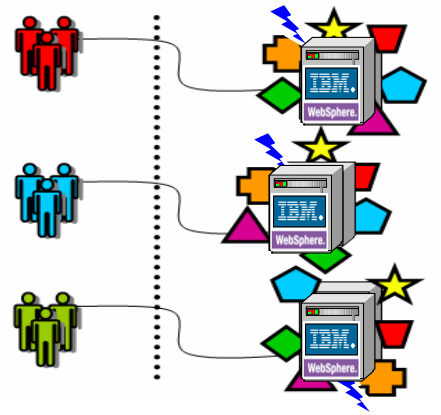
Specifications



SOA Appliances Centralize and Simplify Key Functions

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

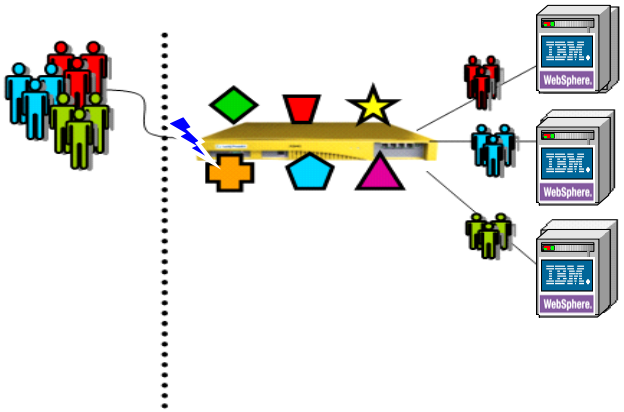
Before SOA Appliance



Update application servers individually

- **Security Processing**
- **Routing**
- **Web services management**
- **Transformation**
- **New XML standard**
- **Access control update**
- **Schema validation**

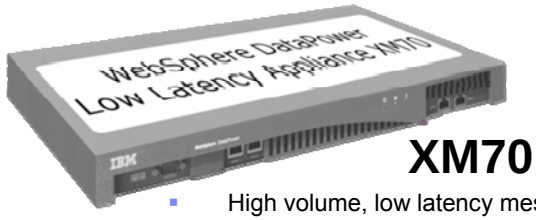
After SOA Appliances



Secure, route, transform for all applications readily

No changes to applications

WebSphere DataPower SOA Appliance Product Line



XM70

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

XB60

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

XA35

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

XS40

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

XI50

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

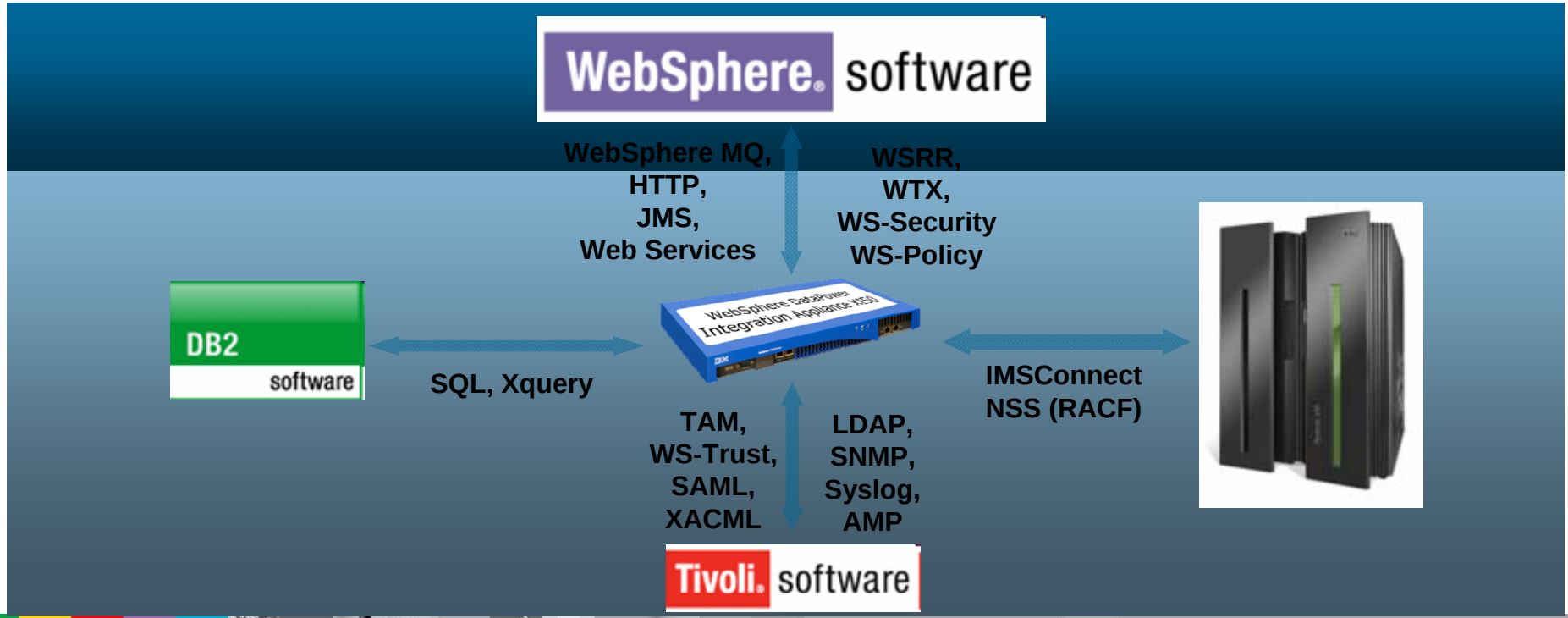
Configuration & Administration

Fits into existing environments

- **Depth of functionality to scale to full operational complexity.**
- **Multiple administration consoles.**
  - WebGUI – 100% availability of functions in all consoles.
  - CLI – Familiar to network operators.
  - SOAP interface – Programmatic access to all config for easy scripting.
- **IDE integration.**
  - Eclipse/Rational Application Developer.
  - Altova XML Spy.
- **WAS 7 Admin Console for Multi-box Management.**
- **Easy export/import for configuration promotion.**
- **Standard operational interfaces.**
  - SNMP, syslog, etc.
- ***Industry leading integration support across IBM and 3rd party application, security, identity management, and networking infrastructure.***

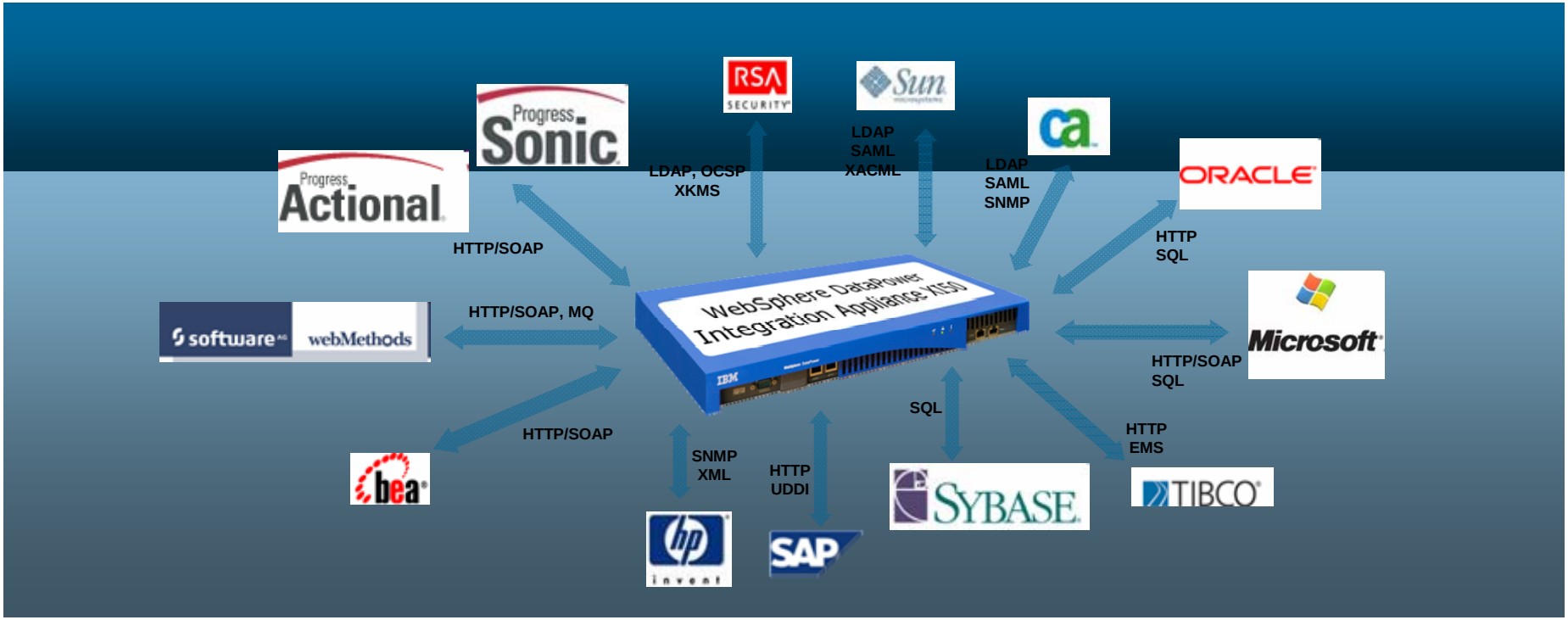
Integration within the IBM Software Portfolio

- Mature integration within WebSphere software portfolio.
  - *WebSphere MQ with WebSphere DataPower: 4+ years.*
  - *Industry-leading SOA Runtime Governance with WSRR + DataPower.*
  - *Limitless ESB: Support for WTX for data maps, WS-Security for WMB.*
- Complete SOA Security and Management solution with Tivoli products.
- Robust enterprise integration through native DB2 and IMSConnect.



Integration with Third Party vendors

- Standards-based integration with third party vendors.
- Tight integration with some notable vendors.
- No platform dependencies – hardware or software.
- Exceptional interoperability through industry profiles and testing.



Standards

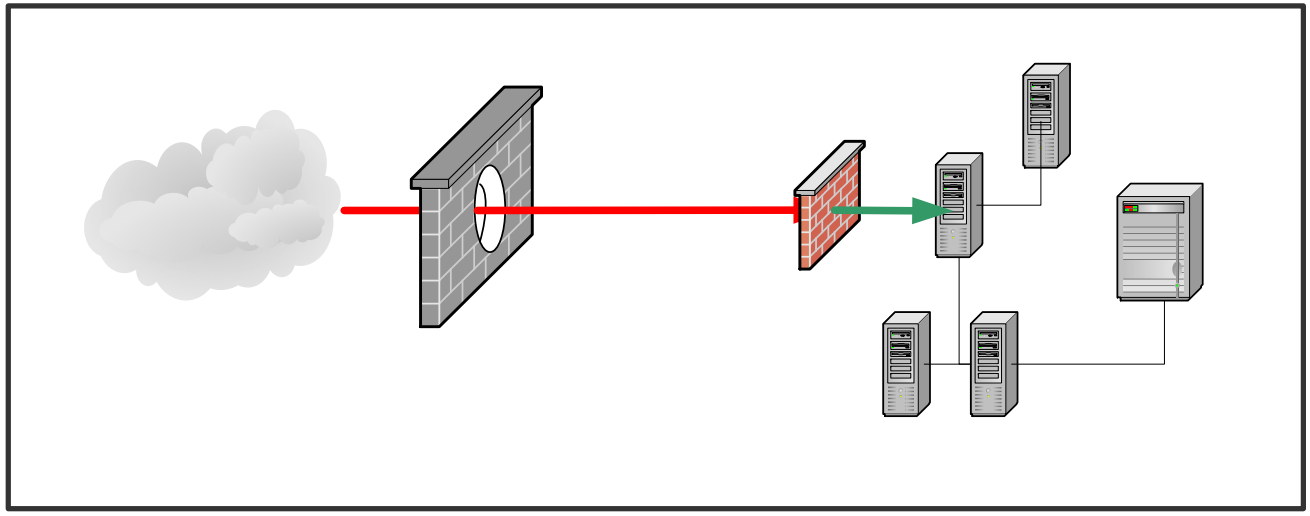
DataPower and the Standards

- **OASIS:**
  - Web Services Security (WSS) TC
  - Web Services Distributed Management (WSDM)
  - Security Services (SAML)
  - XACML
  - Reliable Exchange, Web Services Transactions
  - XSLT/XPATH Conformance
  - Digital Signature Services
  - ebXML Messaging TC
- **WS-I:**
  - Basic Security Profile Working Group
  - MC Committee
  - SOAP with Attachments Working Group
- **W3C:**
  - XML Protocol WG for SOAP
  - XML Binary
  - WS Addressing
  - XML Key Management Services (XKMS) WG
  - XML Encryption WG
  - XML-DSig WG
- **OMG (Object Management Group):**
  - CORBA Security specification
- **ACORD**
  - Joint Architecture Group [Framework][Security]

Security Features

Security: Top Concern for SOA

- XML Web services easily expose backend systems to customers, partners
- Traditional security devices do not secure XML/SOAP



Solution: Multiple level of defense

- First Level: XML Security Gateway for enhanced security, scalability, and simplicity
- Second level: Application server for additional processing

SOAP request

HTTP tunnelli

Gartner: Web Services Security Best Practices

- Provide System Security
  - **Inspect ALL traffic**
  - **Transform all messages**
  - **Mask internal resources**
  - **Implement XML filtering**
  - **Secure logging**
  - **Protect against XML DoS**
  - **Require good authentication mechanisms**
- Provide Message Security
  - **Sign all messages**
  - **Validate messages (Inbound+Outbound)**
  - **Time-stamp all messages**
- Ask for Compatibility
  - **SSL, SAML, x.509.**
  - **WS-Security**
  - **WS-* extensions**
- Build Expertise/Design From Strength
- Educate Business Leaders
- Build Centralized Infrastructure
  - **SSL is key**
  - **Use management/security platforms**
  - **Manage your identities**
  - **You may need PKI**
- Trust (Really) Your Partners
- Monitor and Control

"Therefore, enterprises should investigate tools such as security gateways, SSL concentrators and accelerators, and wire-speed SOAP/XML inspection hardware**."**

-- John Pescatore, Gartner

SSL Termination & Acceleration; HTTP Features

- Two-way SSL
  - Server and client authentication capture
- Unlimited identities
  - Enabled for scalability
- SSL acceleration
  - Offloads processor intensive cryptography to device
- SSL dump & SSL debugging features
- HTTP compression
- HTTP 1.0 or 1.1, HTTP multiplexing
- Load balancing for outbound connections
- HTTP header rewrite

XS40 – XML Security Gateway

Purpose-Built for SOA Security

- XML/SOAP Firewall
  - Filter on any content, metadata or network variables
- Data Validation
  - Approve incoming and outgoing XML and SOAP with minimal latency.
- Message and Field Level Security
  - WS-Security: Encryption, decryption, digital signatures, etc.
- XML Web Services Access Control/AAA
  - SAML, LDAP, RADIUS, etc.
- Web Services Management
  - Service Level Management, Service Virtualization, Policy Management
- Content-based Message Routing
- Web Application Firewall Capabilities
  - Security proxy, threat mediation & content processing services for HTTP-based web applications.

XML and SOAP Firewall

- Highly Configurable Request and Response Filtering
  - IP-layer parameter filtering (client IP address, etc.)
  - SSL parameter filtering (client certificate, etc.)
  - HTTP header filtering
  - XPath filtering of any part of SOAP envelope or XML payload
  - Filtering by Service, URL, etc.
- Easy “point and click” XPath Filtering

XML Threats

- 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
- Falsified Message
- 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
- Replay Attack

XML and SOAP Data Validation

- Raw XML and SOAP message inspection (inbound and outbound)
- Well-formed XML validation
- SOAP protocol checks
- XML Schema validation
  - Explicitly set XSD in validate step
  - Fetch “trusted” copy of XSD based on XSD self-declared by incoming XML document
  - Validate directly from WSDL for SOAP web services
- Business logic and other arbitrary validation:
  - XSLT transformations to extract or validate business-level information contained in XML/SOAP payload.
- Schemas can be cached on the device

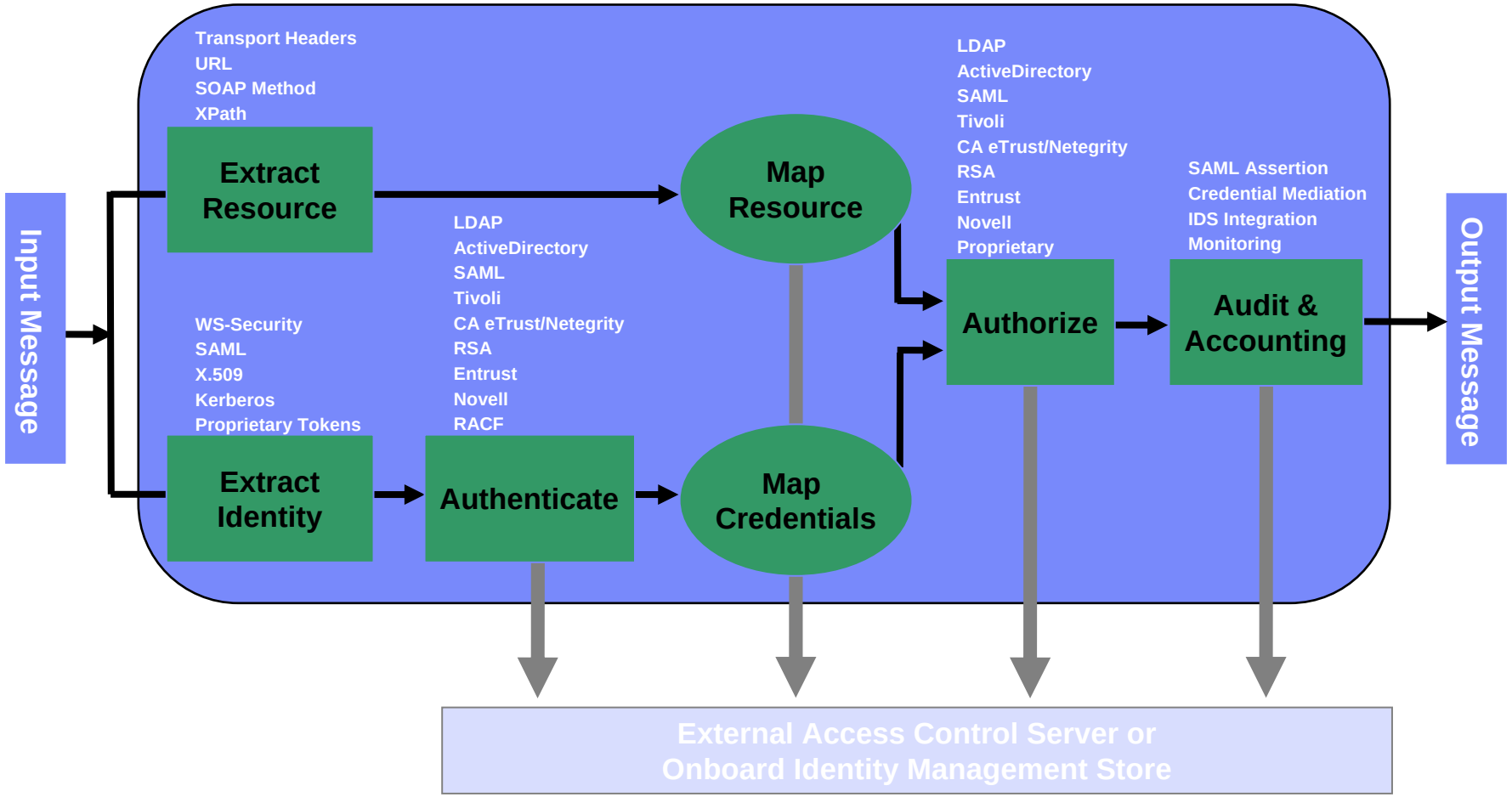
Access Control

Leading Standards and Third-party Integration Support

- Access control policy
  - On-board: certificates, XML file, XACML
  - External access control servers
- Standards-based integration
  - LDAP
  - RADIUS
  - XKMS
  - SAML
  - WS-Security, WS-Trust, etc.
  - Extensible Access Control Markup Language - XACML
- Integration with access management solutions:
  - Tivoli Access Manager
  - Tivoli Federated Identity Manager
  - RSA ClearTrust
  - Microsoft Active Directory
  - Sun Identity Server
  - Netegrity SiteMinder or TransactionMinder
  - Oblix
  - CA eTrust
- Fully customizable in every respect

Access Control Integration Framework (AAA)

Authenticate, Authorize, Audit



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
- Wizard-driven configuration
- Cross-site scripting and SQL Injection protection
- AAA framework support for web applications
- General name-value criteria boundary profiles for:
  - Query string and form parameters
  - HTTP headers
  - Cookies

- HTML Input Conversion Maps for form processing and handling
- Cookie watermarking (sign and/or encrypt)
- Rate limiting and traffic throttling/shaping
- HTTP header stripping, injection and rewriting
- HTTP protocol and method filtering
- Content-type filtering
- Dynamic routing and load balancing
- Session handling policies
- SSL Acceleration & Termination (Link)
- XML and non-XML processing policies
- Customizable error handling

Web Application Security

- HTTP web application protection
- Protection for static or dynamic HTML-based applications
- Supports browser-based clients and HTTP/HTTPS backend servers
- Cross-site scripting and SQL Injection protection
- Authentication and Authorization (AAA)
- General name-value criteria boundary profiles for:
  - Query string and form parameters
  - HTTP headers
  - Cookies
- HTML Input Conversion Maps for form processing and handling
- Cookie watermarking (sign and/or encrypt)
- Rate limiting and traffic throttling/shaping
- HTTP Header stripping, injection and rewriting
- HTTP protocol and method filtering
- Content-type filtering
- Dynamic routing and load balancing
- Session handling policies
- SSL Acceleration & Termination
- Customizable error handling

MultiStep and XML Routing

Flexible Drag & Drop Message Processing and Policy Creation

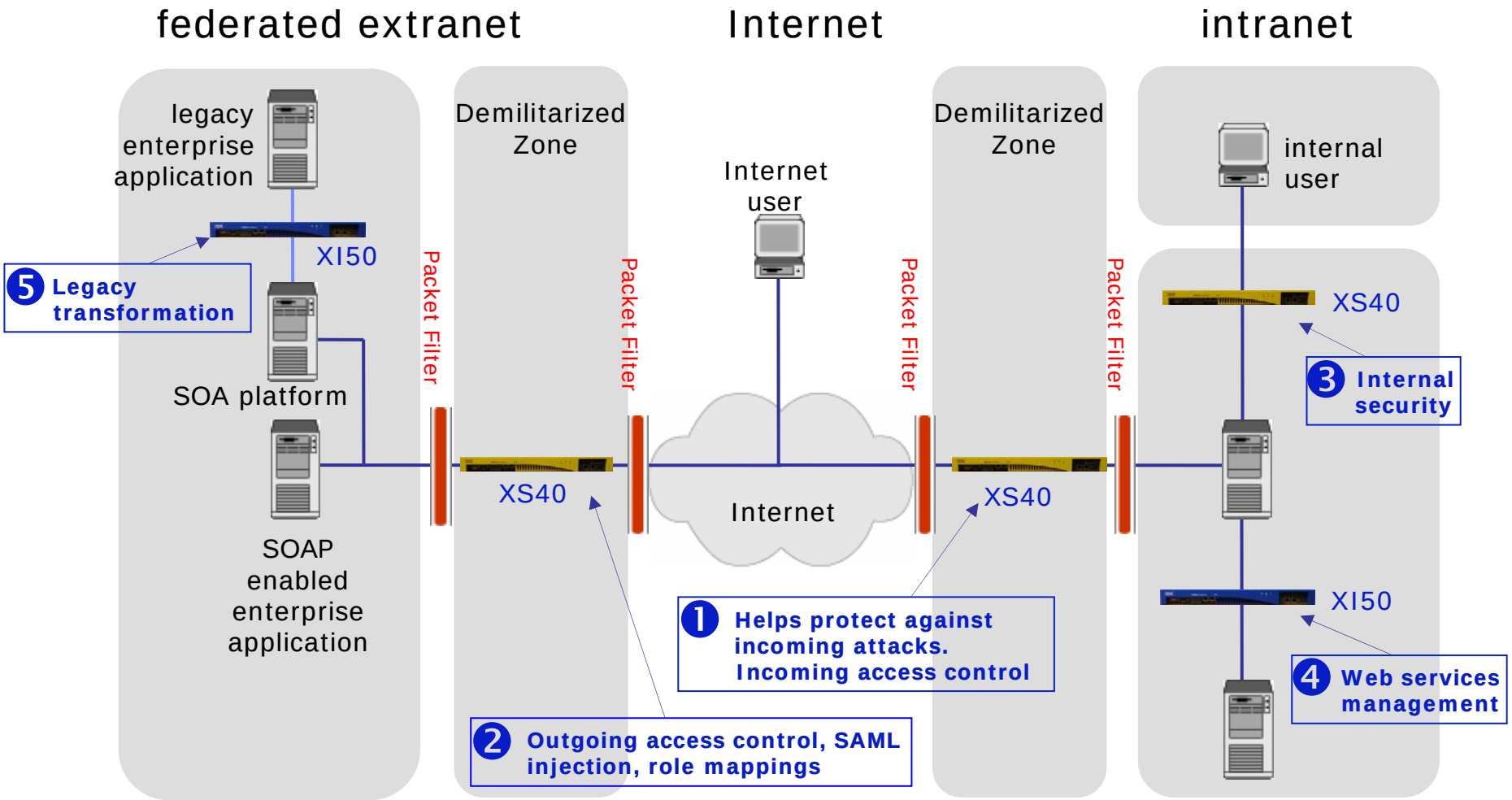
- MultiStep is a general term that describes the customizable processing pipeline that executes when a message arrives or when an error occurs.
- MultiStep actions are applied, in a user-defined sequence, against a message. Actions include:
  - Encrypt, Decrypt, Sign, Verify
  - Access control (AuthN, AuthZ), Filter, Validate
  - Route, URL or Header Rewrite
  - Call out or Fetch artifacts such as XSLT, XSD, XML, WSDL, etc.
  - Transform (XML or legacy data)
  - Logging – log individual transactions (including message) for analysis and archiving
  - Service Level Management – shape and monitor traffic and/or send alerts based on transactional data and context
  - XPath extract
- Custom error handling policies

Web Services Management

Service Level Management

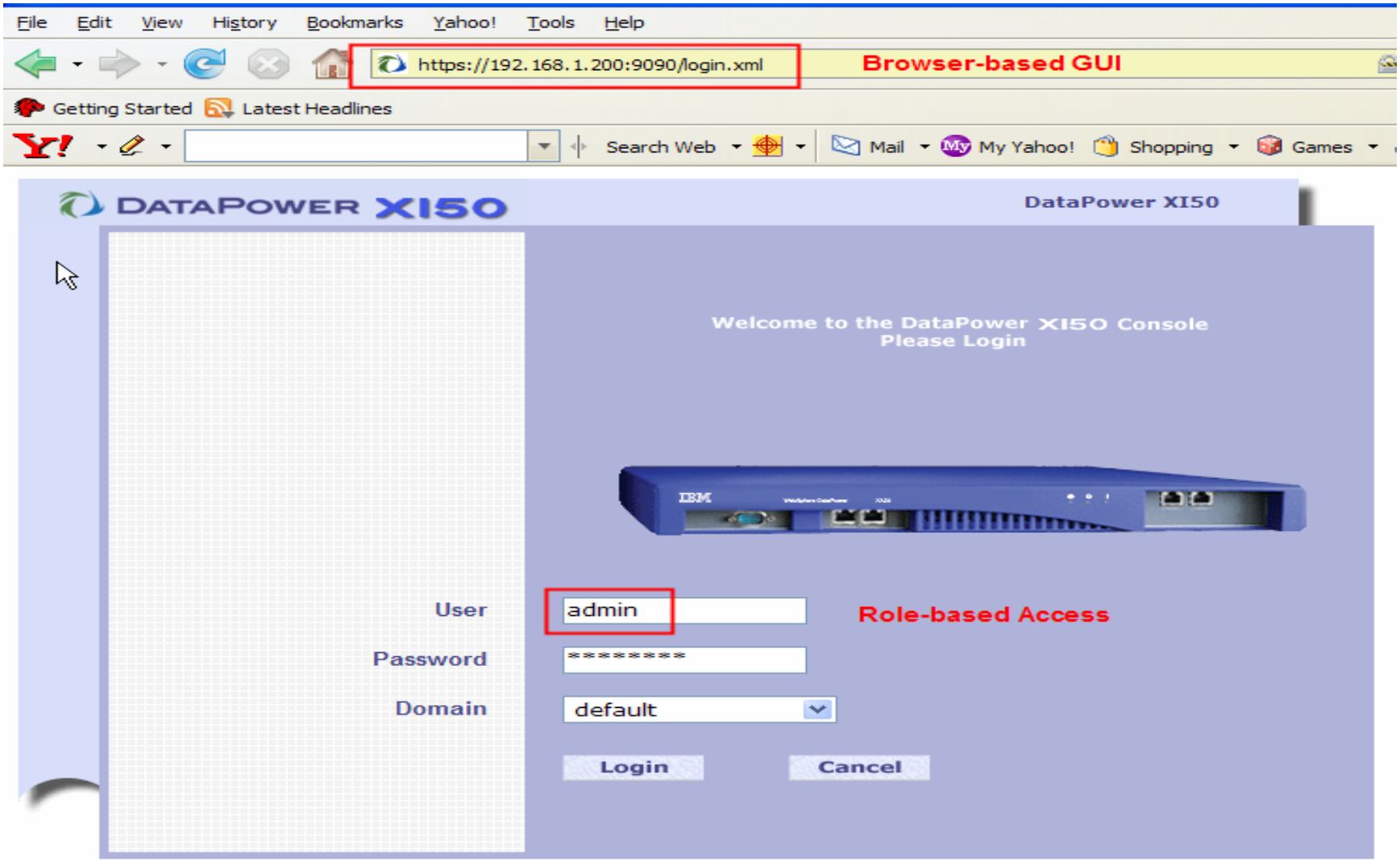
- Hierarchical service level management at WSDL, service, port, or operational level
- Flexible actions when reaching a threshold
  - Notify/Alert - Log a message; send an e-mail or pager alert, etc.
  - Shape – hold the request until the next timed interval (n transactions per second)
  - Throttle – reject the request once the threshold has been achieved
- Configure custom policies based on:
  - Rate (TPS) or count by time
  - Request, Response, Fault, or XPath
- Support for enforcement across a pool of devices

Deployment Scenarios



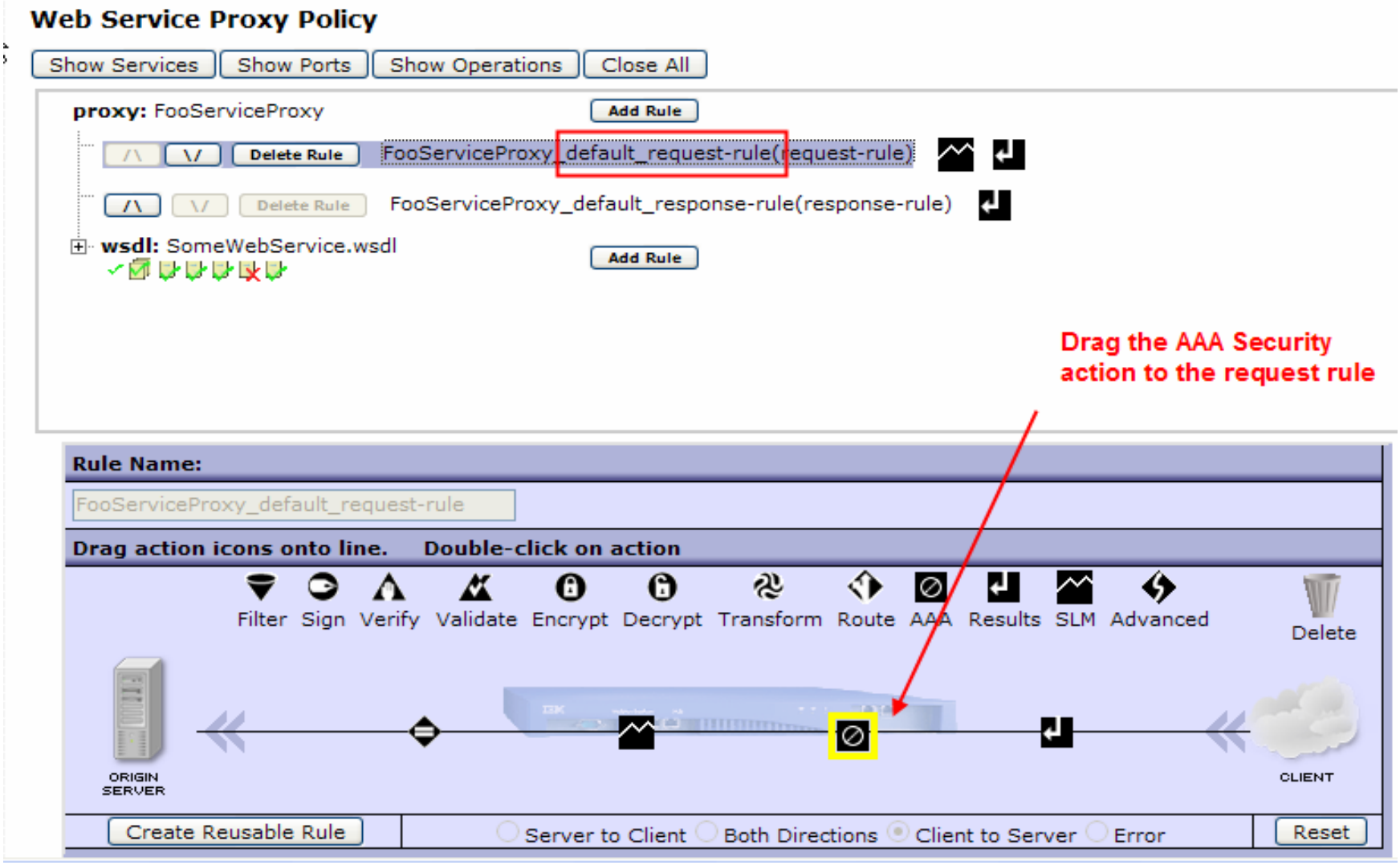
Screen Shots

Configuration Driven, NO Programming

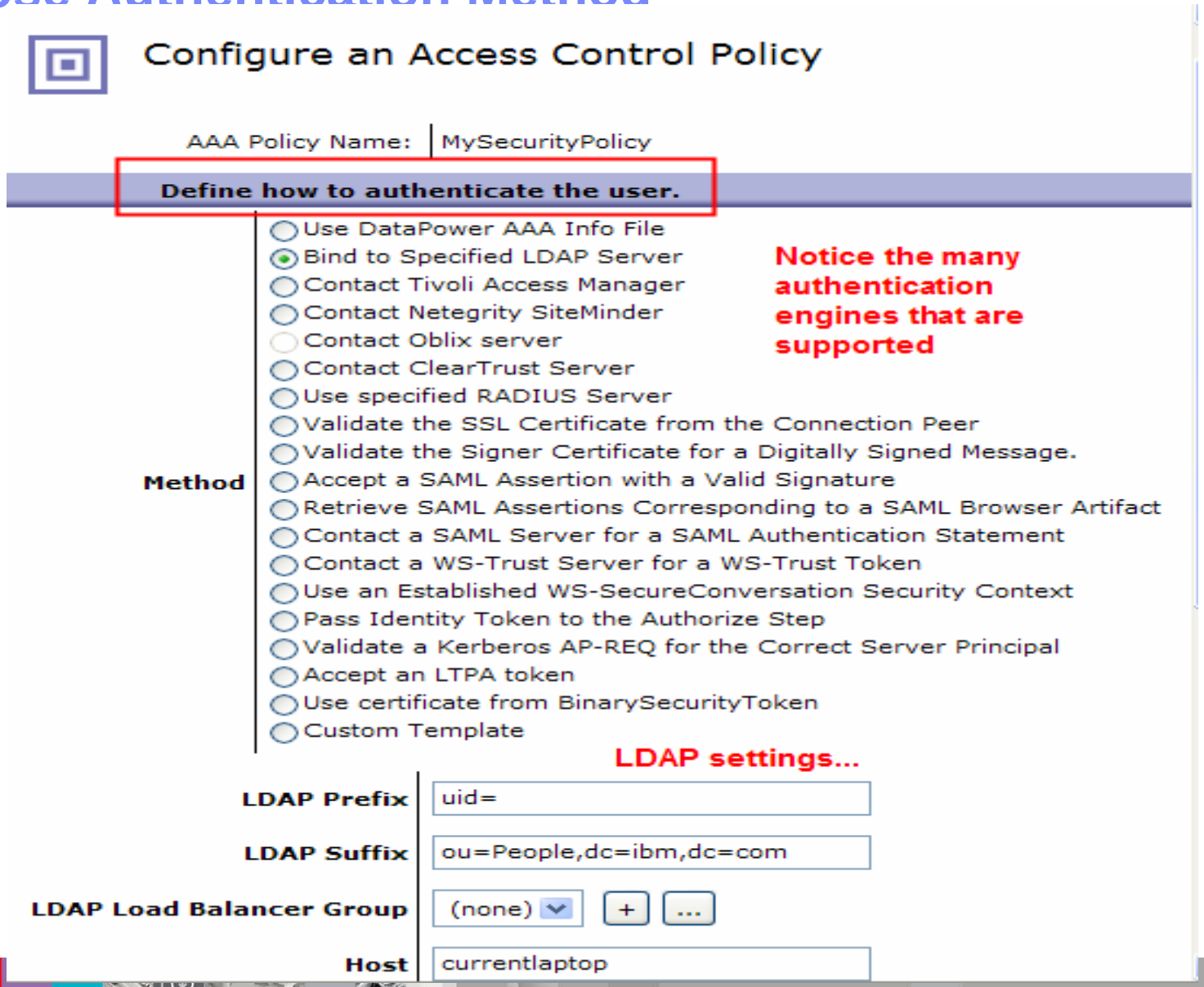


Example: Build Web Service Proxy with AAA

Add a AAA Security Action



Choose Authentication Method



Customer Examples

World's Leading Companies Have Deployed DataPower

Banking/Finance

- AG Edwards
- Bank of America
- Banco Commercial
- CIBC
- Capital One
- Charles Schwab
- Citigroup
- Federal Reserve
- Fidelity
- First American
- JP Morgan Chase
- Principal Financial Group
- Royal Bank of Scotland
- Standard Bank
- UBS
- US Bank
- Vanguard
- Visa International
- Wachovia

Insurance

- Aetna
- AIG
- Allianz Life
- AXA/Equitable
- Cigna
- Farmers
- Hanover
- Mercury Insurance
- Nationwide Mutual
- NY Life
- The Hartford
- United Health Group
- 21st Century

Telecom

- Alltel
- Avaya
- Bell South
- CableOne
- France Telecom
- Japan Telecom
- Nortel
- Sprint/Nextel
- T-Com
- T-Mobile
- Telefonica Chile
- US Cellular
- Verizon
- Vodafone

Public Sector

- EPA
- Los Angeles County
- Maricopa County
- National Security Agency
- NATO
- US Dept of Defense
- US Dept of Education
- US Dept of Energy
- US Dept of Homeland Security
- US Dept of Treasury
- Veterans Affairs

Travel/Hospitality

- Avis
- KLM
- CheapTickets
- InterContinental Hotels Group
- Starwood Hotels (Sheraton)
- Travelport/Galileo
- Worldspan

Business Services/Technology

- ADP
- CapGemini Energy
- Deutsche Post
- Intuit
- KPMG
- Macrovision Corporation
- McGraw Hill
- NEC
- Reuters
- RSA Security

Aerospace/Automotive/Media

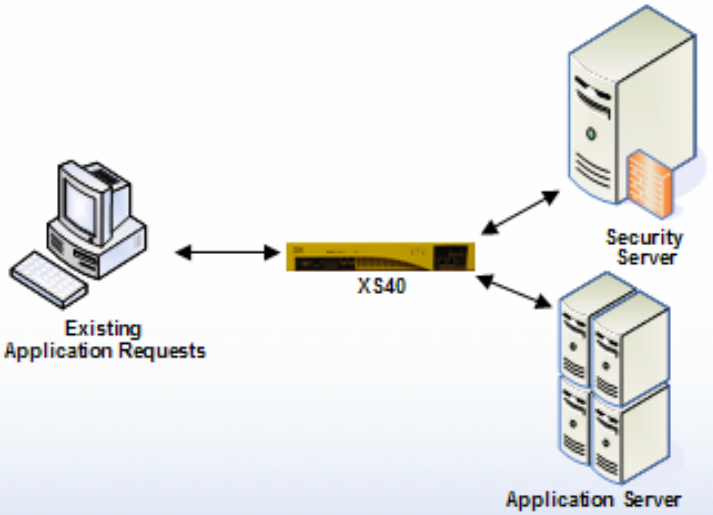
- BAE Systems
- Carquest
- Fox Interactive Media
- GM
- Honda
- Lockheed
- Northrop Grumman
- Live Nation
- Pfizer
- Renault

InterContinental Hotels Group
Secure SOA Integration of Web Services

Challenge
- Decrease management costs by implementing an SOA for B2B transactions with online partners, while increasing XML processing and security.

Solution
- Deployed WebSphere DataPower XML Security Gateway XS40
- The XS40 acts as:
  - Policy enforcement point
  - Including encryption
  - Firewall filtering
  - Digital signatures
  - Schema validation
  - WS-Security
  - XML Access Control

Benefits
- Ability to handle high transaction transformation
- Reduced customer response times for e-business transactions
- Reduced IT costs & overall maintenance of SOA



WebSphere DataPower XML Security Gateway XS40

VISA International

Standard Security Across All Platforms

Challenge

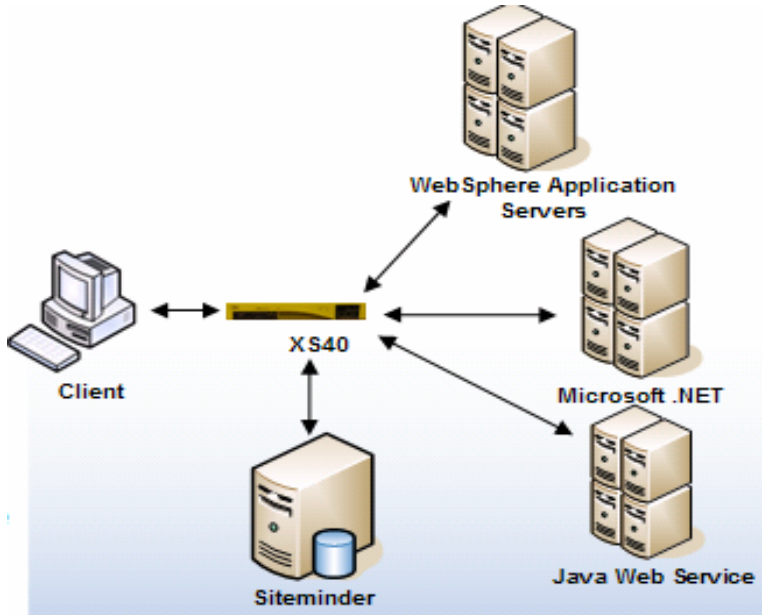
- Consistently & securely delivery of online services to members that could be shared, integrated & flexible to meet specific needs
- Web services infrastructure needed to support highly secure data routing with daily high volume & sensitive nature of information

Solution

- Implemented WebSphere DataPower XML Security Gateway XS40 to form the backbone of Web services infrastructure
  - Content-based message routing
  - Security policy enforcement & data encryption
  - Helps to ensure safe & efficient flow of confidential customer data
- Integrated seamlessly into existing heterogeneous environment increasing interoperability & promoting reuse

Benefits

- Secure SOA on standards-based platform
- Easily reuse Web services throughout enterprise
- Boosts productivity of IT staff
- Substantially shorten time to market for new services



- **WebSphere DataPower XML Security Gateway XS40**
- **WebSphere Application Server**

Bank of America
Web Services Management

Bank of America

Challenge

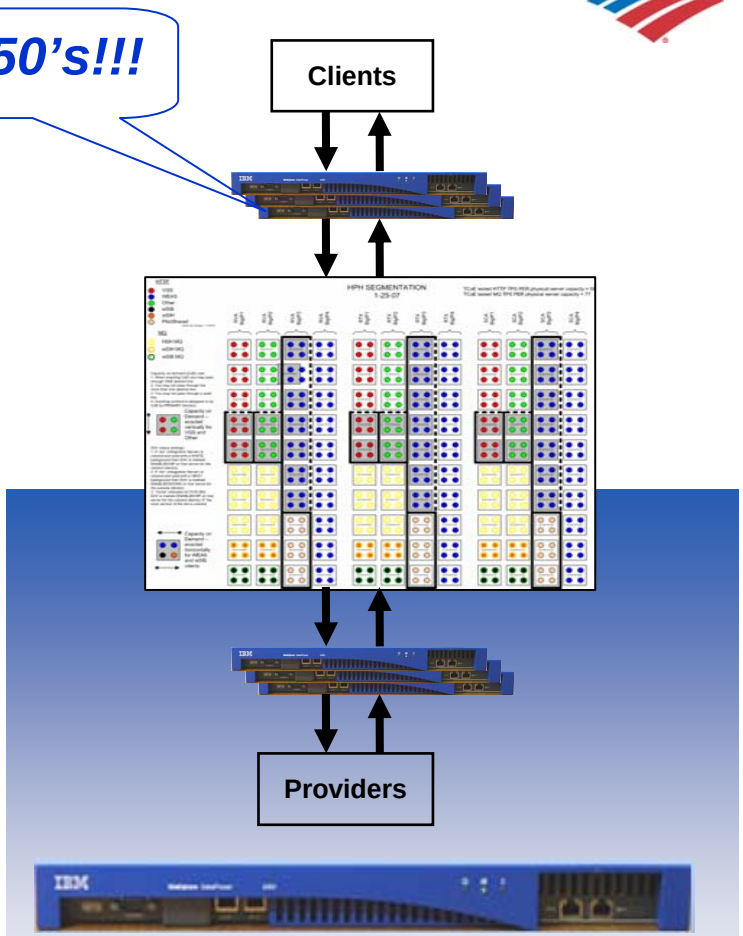
- Existing shared integration infrastructure for Retail Bank unstable and unscalable (120 servers, 480 JVM's!!!)
- Require content-based load balancing solution to be extended to offload functionality from existing solution

Solution

- Implemented WebSphere DataPower Integration Appliance XI50:
  - Primary function of XI50 is content-based load balancer for HTTP(s) and MQ traffic
- Additional tier of XI50's planned for proxying to backend services (MQ, HTTP and IMSConnect)

Benefits

- Able to handle traffic bursts from third party partners
- Enhanced security on existing message flows
- Sophisticated mechanism for proactive identification and "route away" from degrading JVM's
- Broken through their "scaling barrier", able to do more with less cost



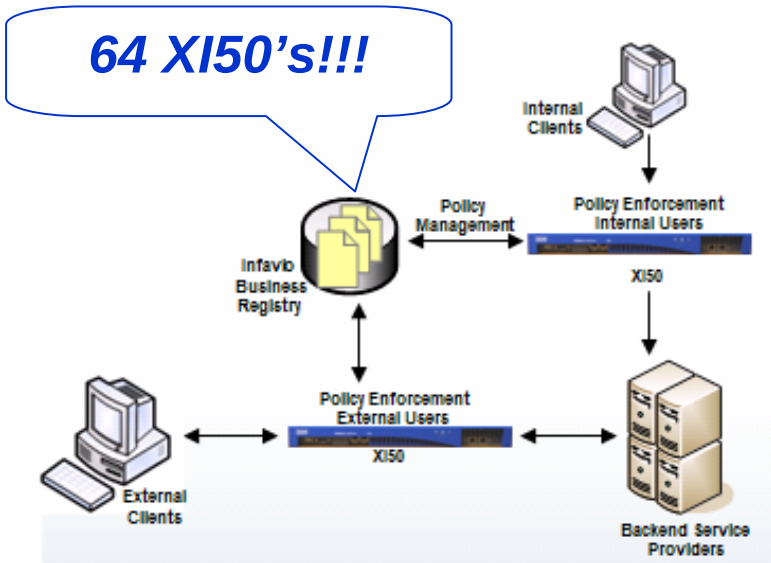
- **WebSphere DataPower Integration Appliance XI50**
- **WebSphere MQ**

Sprint
ESB & Policy Enforcement of SOA

Challenge
- To deploy an ESB that provides message security & mediation functions in a highly reliable & scalable fashion, while keeping capital expenditures, development & minimal ongoing management costs

Solution
- Implemented WebSphere DataPower Integration Appliance XI50 in the DMZ & the Enterprise Network
- The XI50s accepts HTTP/SOAP traffic and provides policy enforcement for external users
  - Filtering & validating incoming XML traffic
  - Authentication & authorizing users
  - Routing messages to appropriate end points based on defined rules
  - Converting XML to binary
  - Mediating between HTTP, SOAP, MQ

Benefits
- ESB that is scalable, easy-to-deploy, quick to configure & simple to manage
- Faster time to market enables Sprint to meet project deadlines



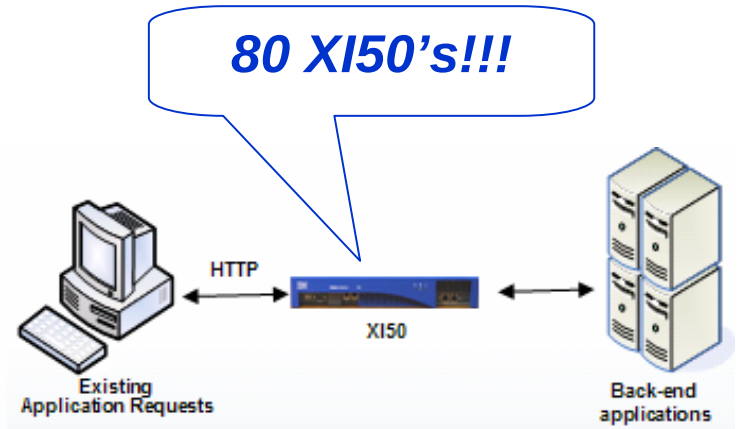
- **WebSphere DataPower Integration Appliance XI50**
- **WebSphere MQ**

Wachovia
Secure legacy systems integration

Challenge
- High profile initiative to leverage SOA
- Enhance ATM message integration
- Replace legacy system to reduce cost, enhance security

Solution
- Deployed WebSphere DataPower Integration Appliance XI50
- Message-level security & XML threat protection

Benefits
- Improved efficiency with on-demand routing of remote deposits from branch office ATMs
- SOA message-level security, content validation, & threat protection
- Reduced VAN charges by using HTTP without sacrificing security compliance
- Reallocated resources to focus on core business tasks



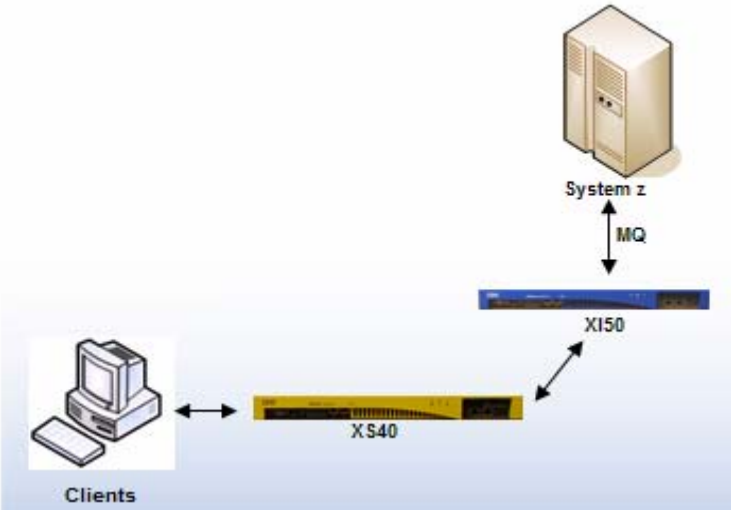
WebSphere DataPower Integration Appliance XI50

AIG Agency Auto
Integration of Web Services and Legacy Systems

Challenge
- Implementing an SOA to share mission-critical applications with affiliated offices & direct customers opens numerous vulnerabilities if not properly secured
- Security method based on SSL encryption contained security flaws that exposed unauthorized external access & XML threats

Solution
- Implemented WebSphere DataPower Integration Appliance XI50 performing as an ESB for simple orchestration, transformation & routing of XML messages to WebSphere MQ
- Implemented WebSphere DataPower XML Security Gateway XS40 to increase the security XML Web services transactions.

Benefits
- Substantially increased security of SOA without causing any throughput issues
- Cost savings by reducing size of existing application server farm



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