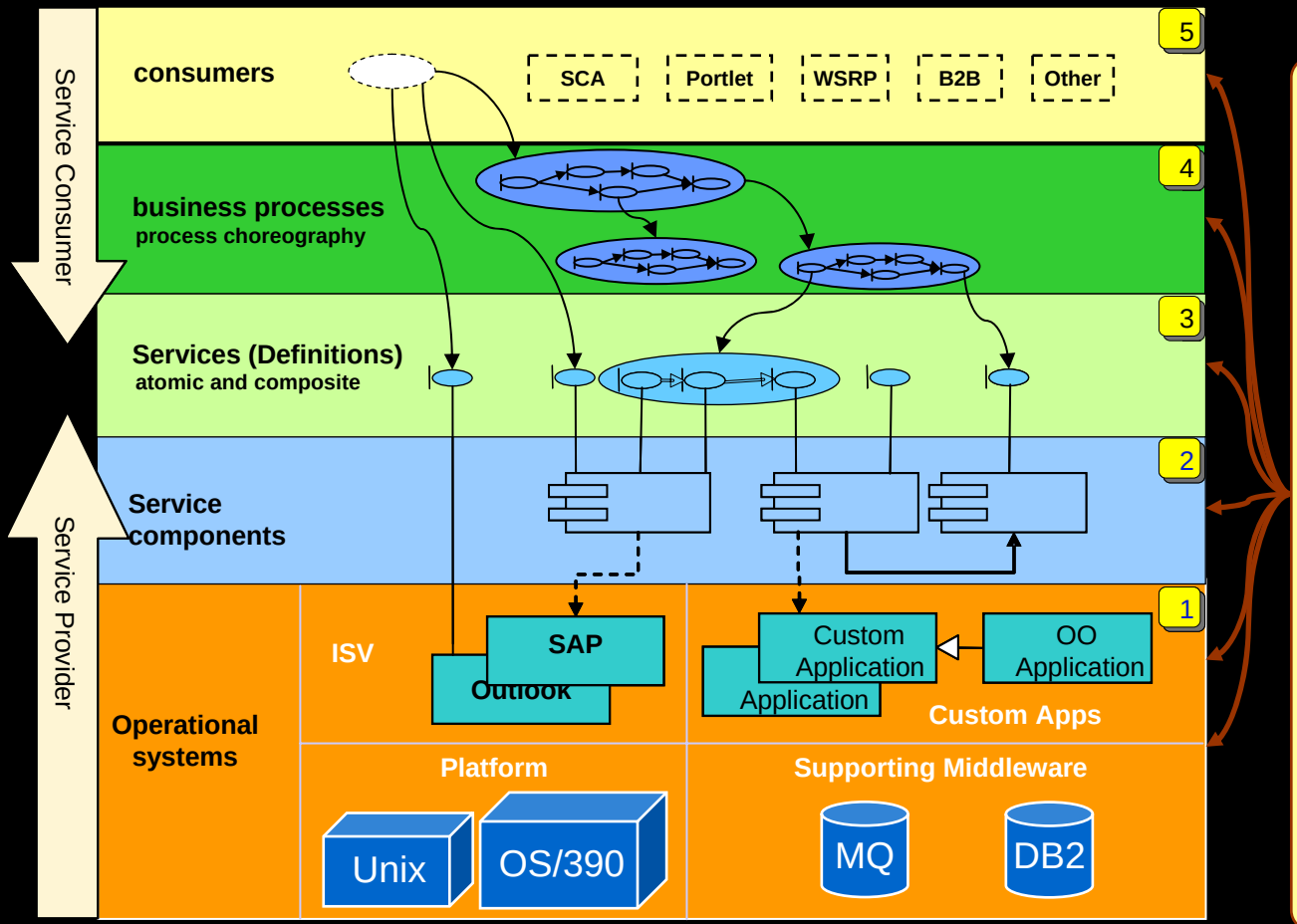
IBM Software Group

Smart SOA in Action

SOA Security

Simon Chan
SOA Architect
hychan@hk1.ibm.com

SOA Security Encompass all Aspects of Security

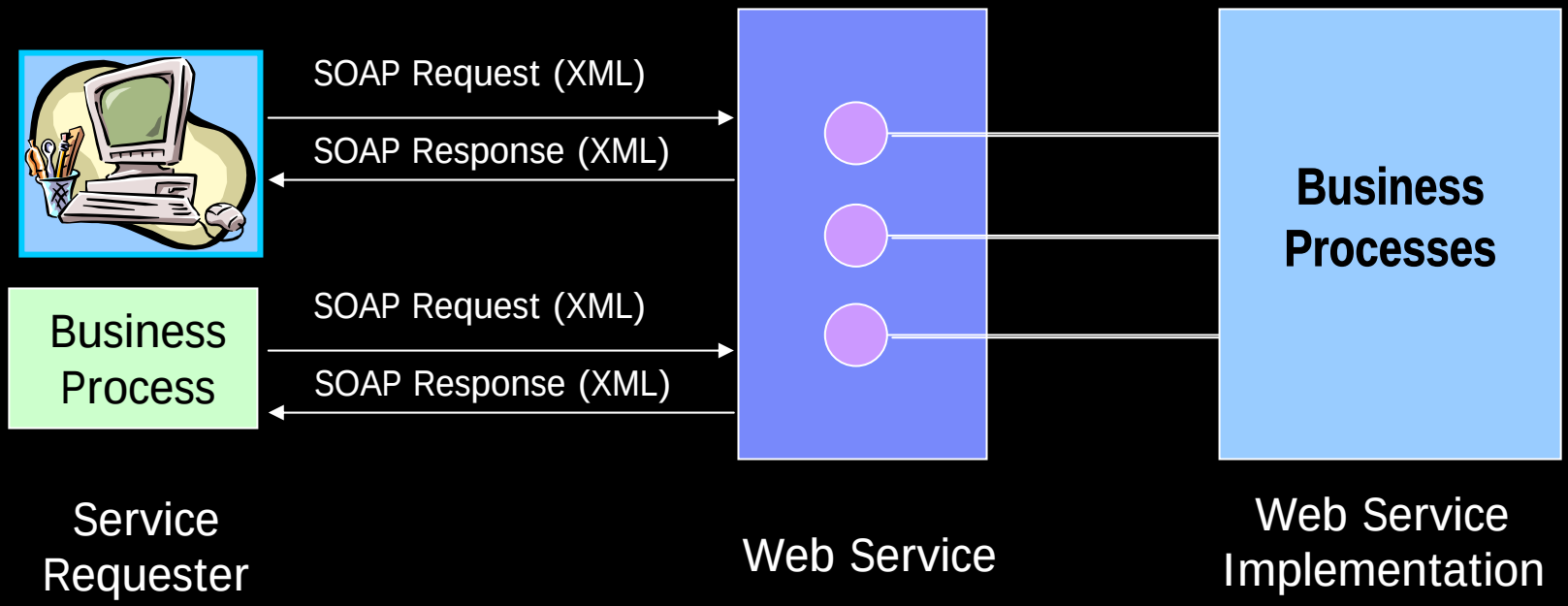


SOA Security

- ✓ Identity
- ✓ Authentication
- ✓ Authorization & Privacy
- ✓ Auditing
- ✓ Confidentiality, Integrity and Availability
- ✓ Compliance
- ✓ Administration and Policy Management

Web Service enables invocation of business functions using standardized protocol

- A new model for using the Web (e.g. app to app)
- An interface that describes a collection of operations that are network accessible through standardized XML messaging
- Standards-based (SOAP, WSDL, UDDI)



SOAP and WSDL are key standards involved in Web Services

SOAP ***Simple Object Access Protocol.*** A simple, lightweight and extendable XML-based wire protocol for exchanging business messages between applications using standard Internet technologies

WSDL ***Web Services Description Language.*** A language for describing the function and interface of a Web service.

There are new types of security threats for Web Services

- **Threats to Message Level Security**
  - **Message Alteration** – Clear text messages may be changed.
  - **Confidentiality** – Messages may be read by external parties.
  - **Man-in-the-middle** – Original Requestor and Service Provider believe they are talking to each other, when in fact they are talking through a third party.
  - **Spoofing** – External party impersonates an authorized user and makes an unauthorized request.
  - **Denial of Service** – Preventing legitimate users from using a web service.
  - **Replay** – An external party copies and later resends a message.

Security measures has to be implemented to guard against Web Services Security threats

In any architectural solution, the following security requirements must be addressed, with no exceptions when it comes to Web services:

- **Identification**: The party accessing the resource is able to identify itself to the system.
- **Authentication**: There exists a procedure to verify the identity of the accessing party.
- **Authorization**: There exists a set of transactions the authenticated party is allowed to perform.
- **Integrity**: The information is not changed on its way.
- **Confidentiality**: Nobody is able to read the information on its way.
- **Auditing**: All transactions are recorded so that problems can be analyzed after the fact.
- **Non-repudiation**: Both parties are able to provide legal proof to a third party that the sender did send the information, and the receiver received the identical information.

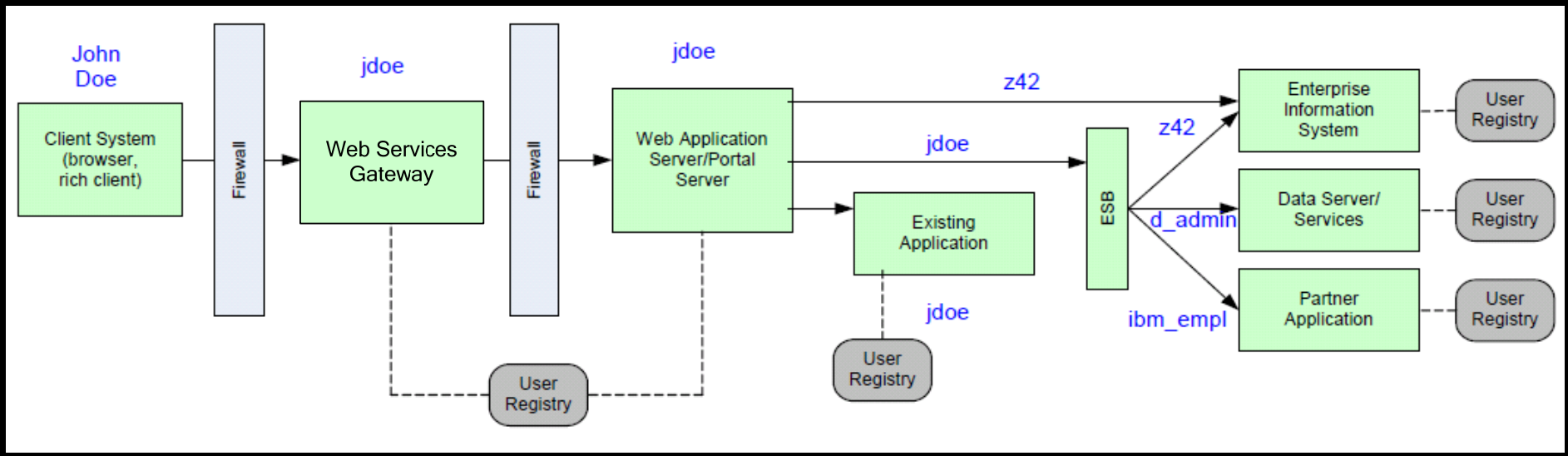
There are many new security standards for each of the security services

Service	Relevant Standards
Identity Services	IdAS, SPML, SAML, WS-Federation
Authentication Service	WS-Trust, Kerberos, SAML, PKI
Authorization and Privacy Services	XACML, JACC, WS-Authorization, WS-Privacy, WS-Policy, IDEMIX
Audit Service	CBE extensions, Audit web service (in progress), WS-BaseNotification
Message Protection	WS-Security, WS-SecureConversation, PKI, XKMS, WS-SecurityPolicy, SSL/TLS, JSSE/JCE

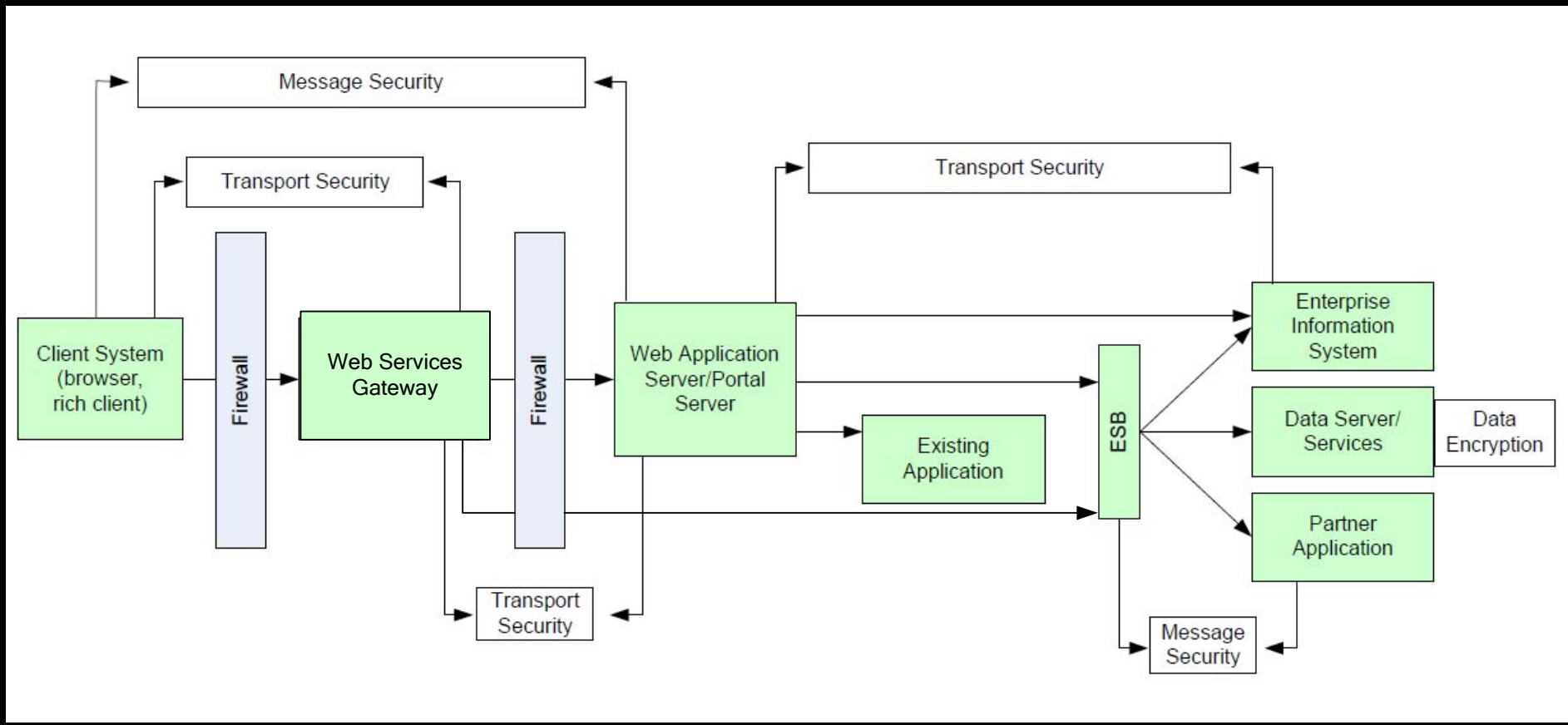
Some of the frequently used security standards are WS-Security, WS-Trust, SAML, XACML and WS-Policy

- WS-Security (Web Services Security) is a communications protocol providing a means for applying security to Web services. It is developed by IBM, Microsoft, and VeriSign.
- SAML - Security Assertion Markup Language. It is an XML-based standard for exchanging authentication and authorization data between security domains.
- WS-Trust is a WS-* specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens.
- XACML - eXtensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.
- WS-Policy is a specification that allows web services to use XML to advertise their policies (on security, Quality of Service, etc.) and for web service consumers to specify their policy requirements.

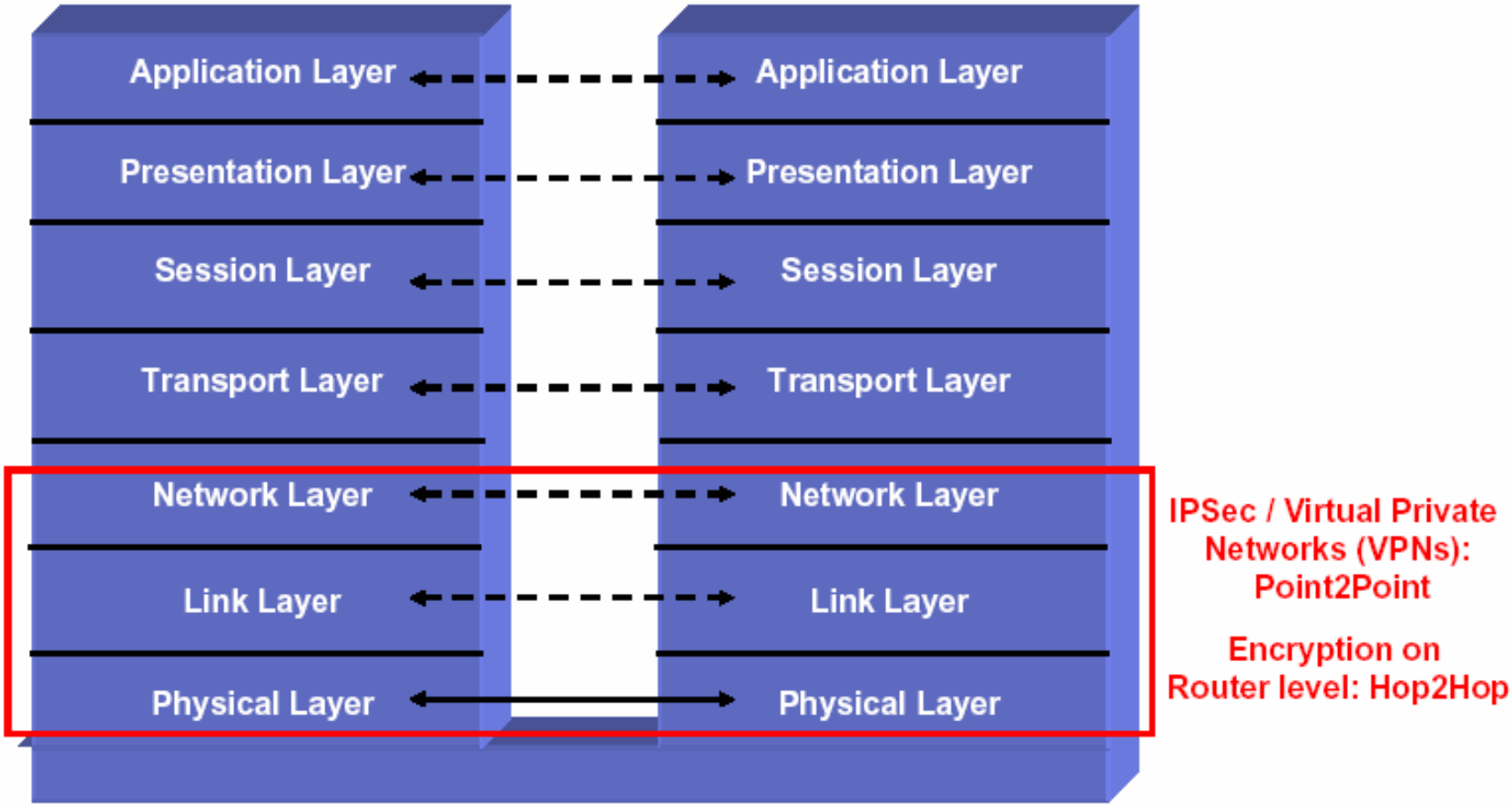
During a service invocation, it is necessary to propagate user identify for access to the authorized services



Data security is also necessary via encryption, transport and message level security

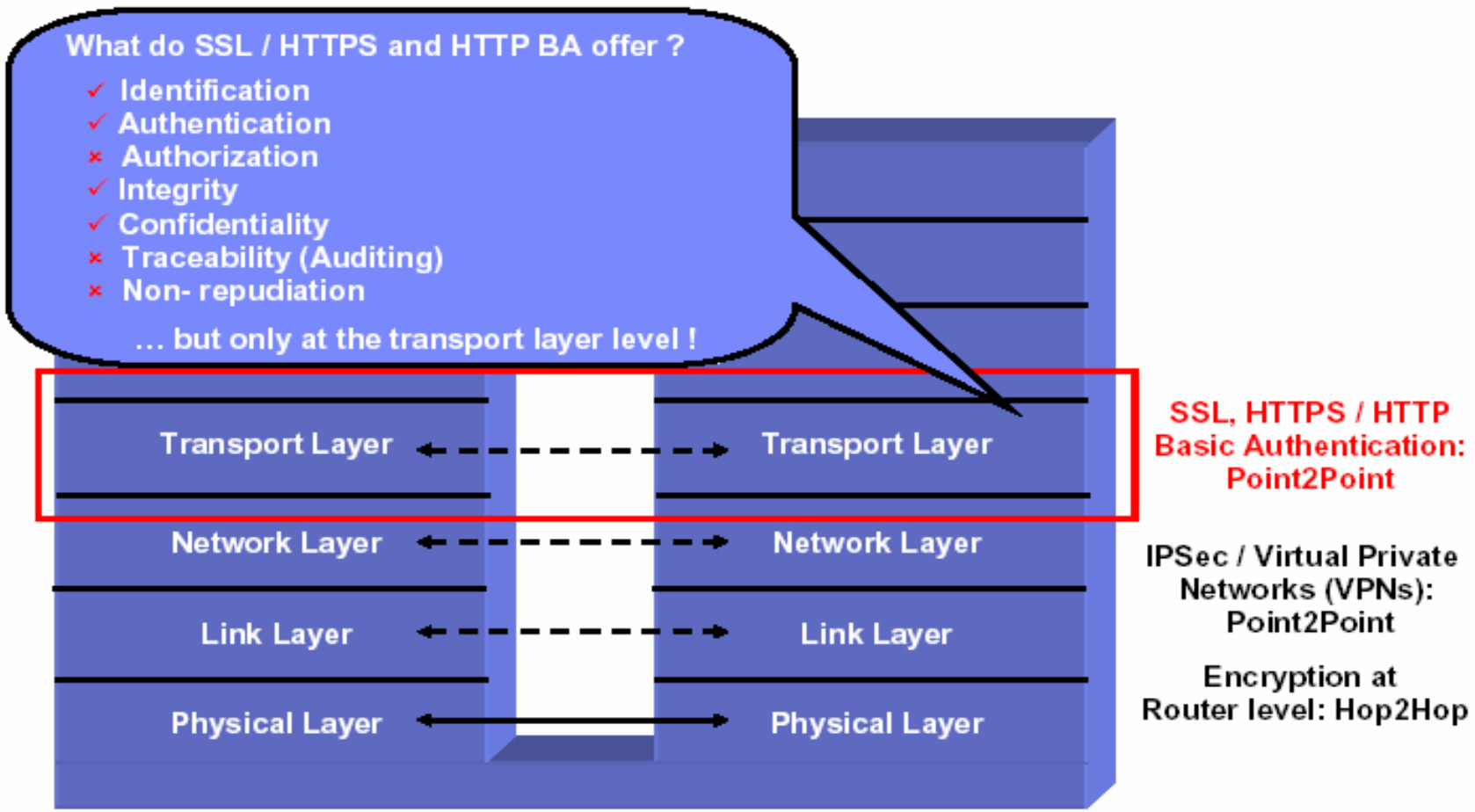


Low level network layer provide basic security protection via encrypted traffic



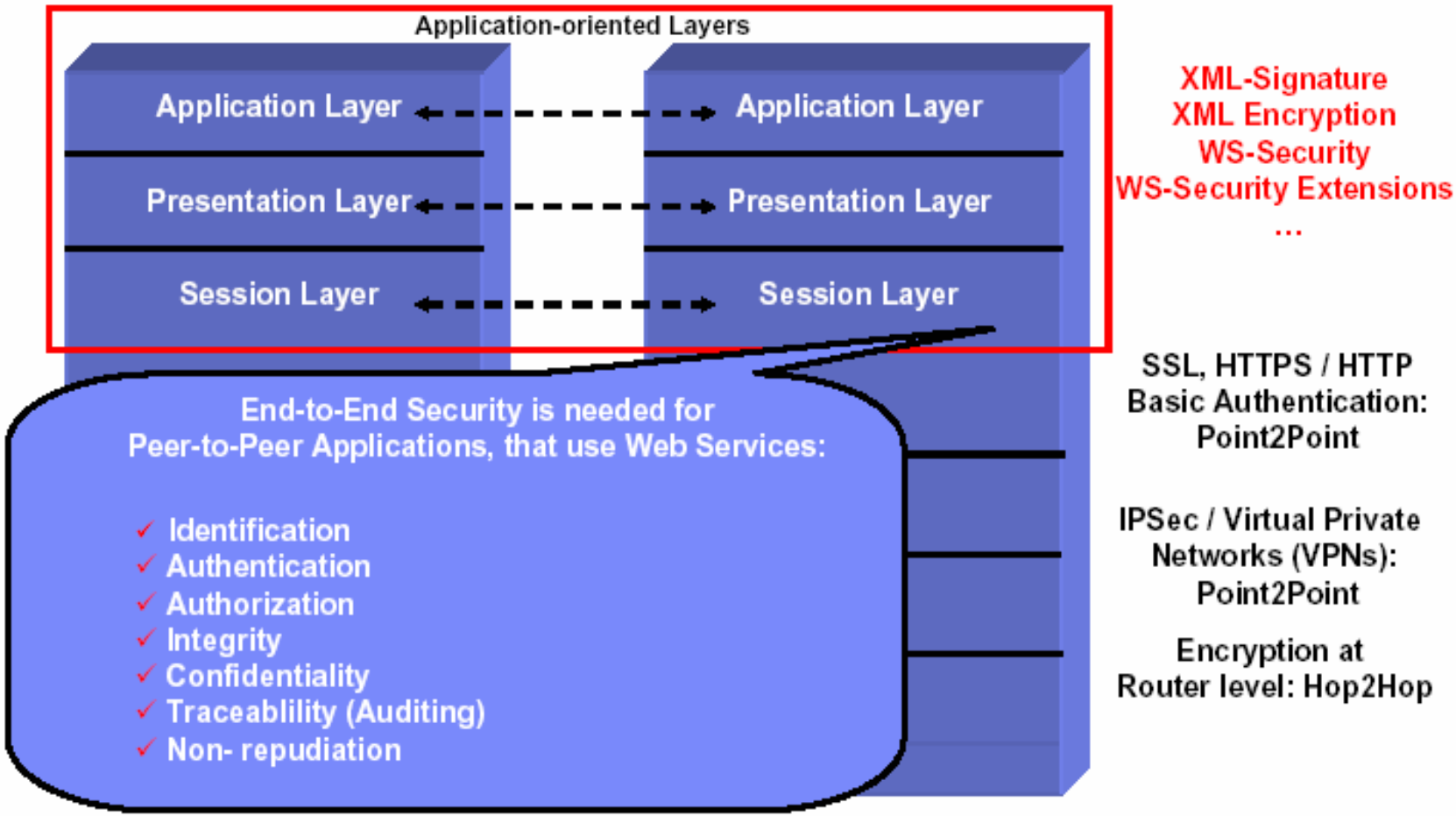
ISO OSI Model and Security Mechanisms

Transport level protocol provides authentication, authorization and data security



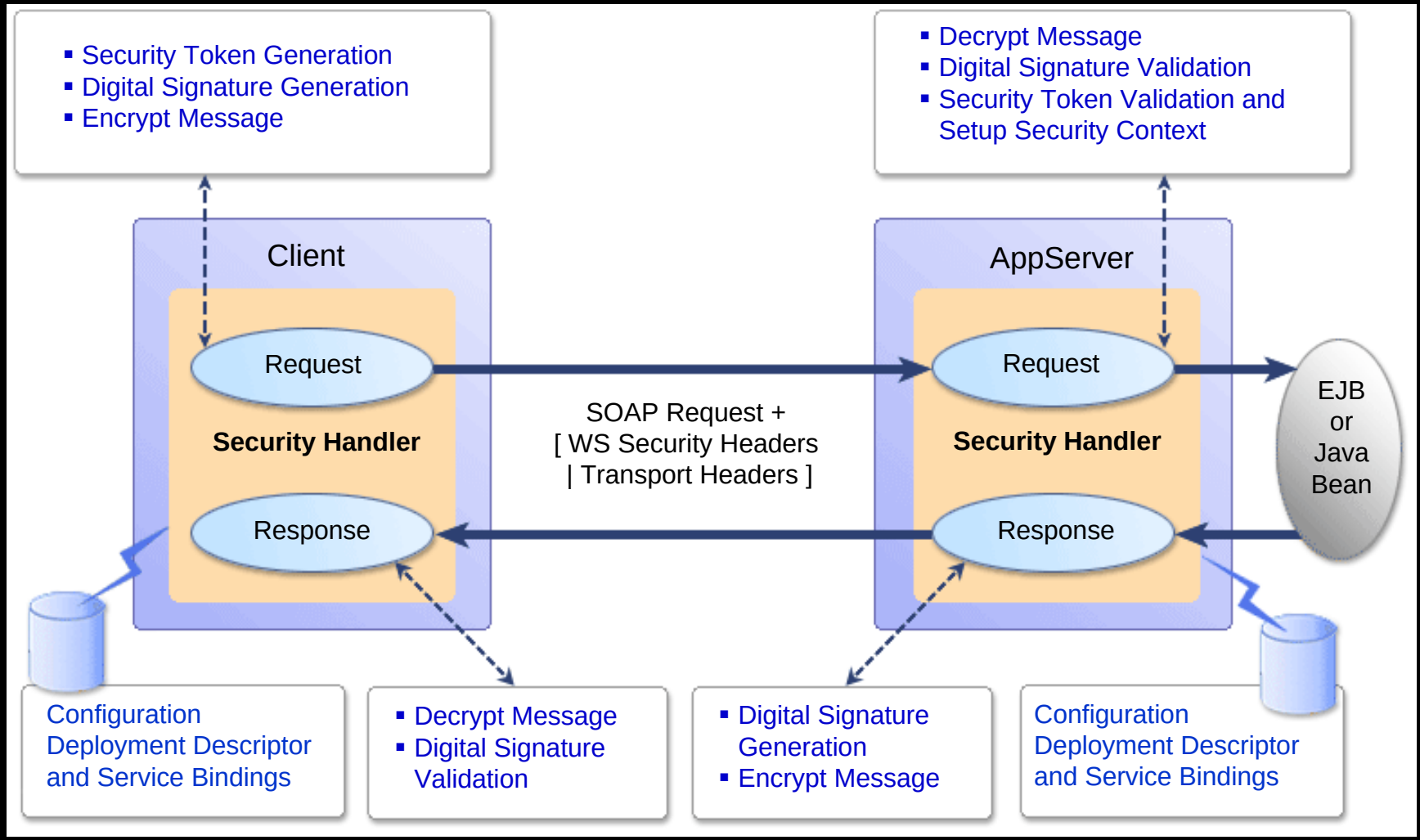
ISO OSI Model and Security Mechanisms

Application-oriented layers provide most comprehensive security services from identification to non-repudiation

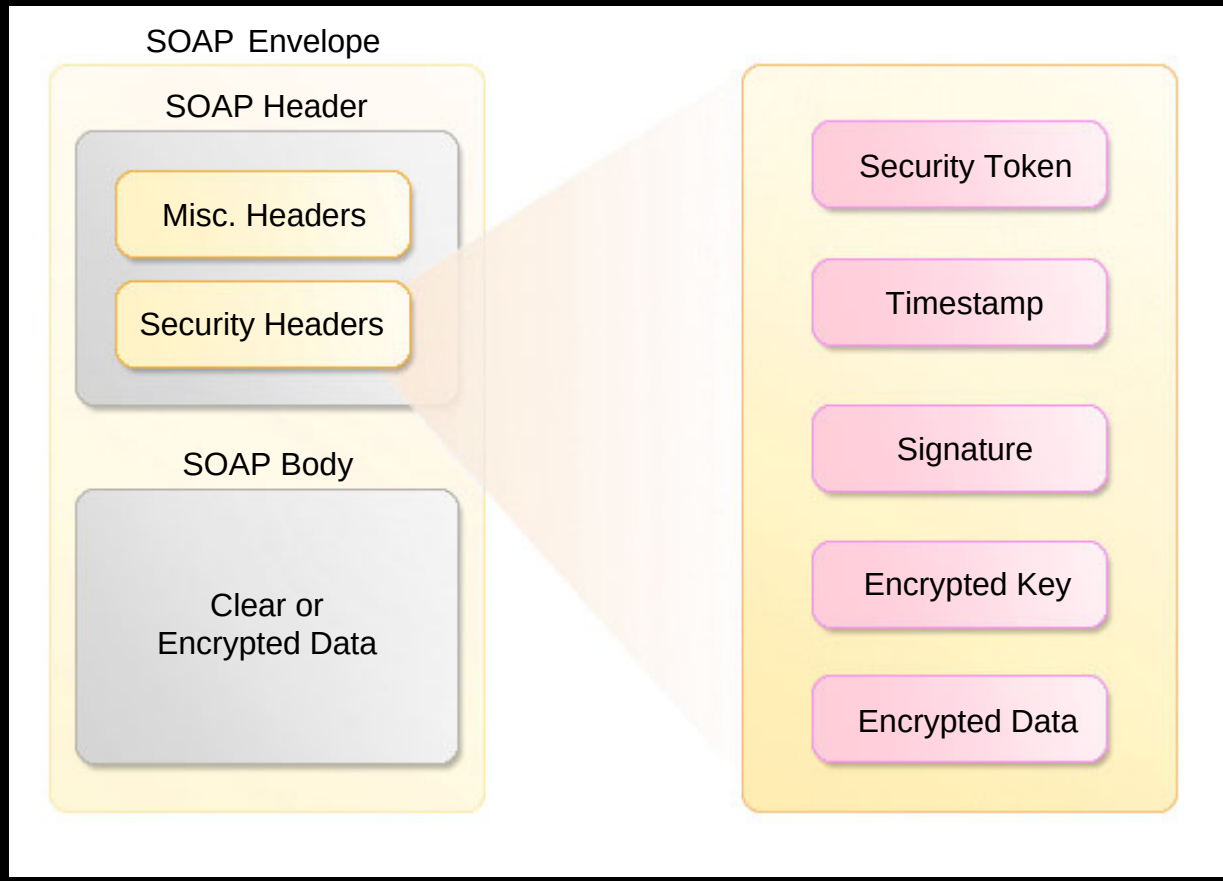


ISO OSI Model and Security Mechanisms

There are multiple security tasks involved in a Web Service invocation



Most of the Web Service security concepts are applied on the SOAP protocol



Web Services Security Message Example

Message example with a username security token (1 of 3):

```
(001) <?xml version="1.0" encoding="utf-8"?>
(002)   <S:Envelope xmlns:S="http://www.w3.org/2001/12/soap-envelope"
                    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
(003)       <S:Header>
(004)           <m:path xmlns:m="http://schemas.xmlsoap.org/rp/">
(005)               <m:action>http://fabrikam123.com/getQuote</m:action>
(006)               <m:to>http://fabrikam123.com/stocks</m:to>
(007)                 <m:id>uuid:84b9f5d0-33fb-4a81-b02b-5b760641c1d6</m:id>
(008)           </m:path>
```

Lines 001-002:
Start SOAP message

Lines 004-008:
Define how to route this message

Web Services Security Message Example

Message example with a username security token (2 of 3):

```
(009)       <wsse:Security
              xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext">
(010)         wsse:UsernameToken Id="MyID">
(011)               <wsse:Username>Zoe</wsse:Username>
(012)         </wsse:UsernameToken>
(013)         <ds:Signature>
(014)             <ds:SignedInfo>
(015)                 <ds:CanonicalizationMethod
                      Algorithm=
                            "http://www.w3.org/2001/10/xml-exc-c14n#"/>
(016)                 <ds:SignatureMethod
                            Algorithm=
                            "http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
(017)                 <ds:Reference URI="#MsgBody">
(018)                     <ds:DigestMethod
                              Algorithm=
                              "http://www.w3.org/2000/09/xmldsig#sha1"/>
(019)                   <ds:DigestValue>LyLsF0Pi4wPU...</ds:DigestValue>
(020)                 </ds:Reference>
```

Line 009:
Start of Security header

Lines 010-012:
Specify the security token

Lines 013-028:
Specify a digital signature. This example uses a signature based on the security token.

Web Services Security Message Example

Message example with a username security token (3 of 3):

```
(021)                </ds:SignedInfo>
(022)                <ds:SignatureValue>DJbchm5gK...</ds:SignatureValue>
(023)                <ds:KeyInfo>
(024)                     <wsse:SecurityTokenReference>
(025)                       <wsse:Reference URI="#MyID"/>
(026)                     </wsse:SecurityTokenReference>
(027)               </ds:KeyInfo>
(028)            </ds:Signature>
(029)       </wsse:Security>
(030)    </S:Header>
(031)    <S:Body Id="MsgBody">
(032)       <tru:StockSymbol xmlns:tru="http://fabrikam123.com/payloads">
                  QQQ
            </tru:StockSymbol>
(033)    </S:Body>
(034) </S:Envelope>
```

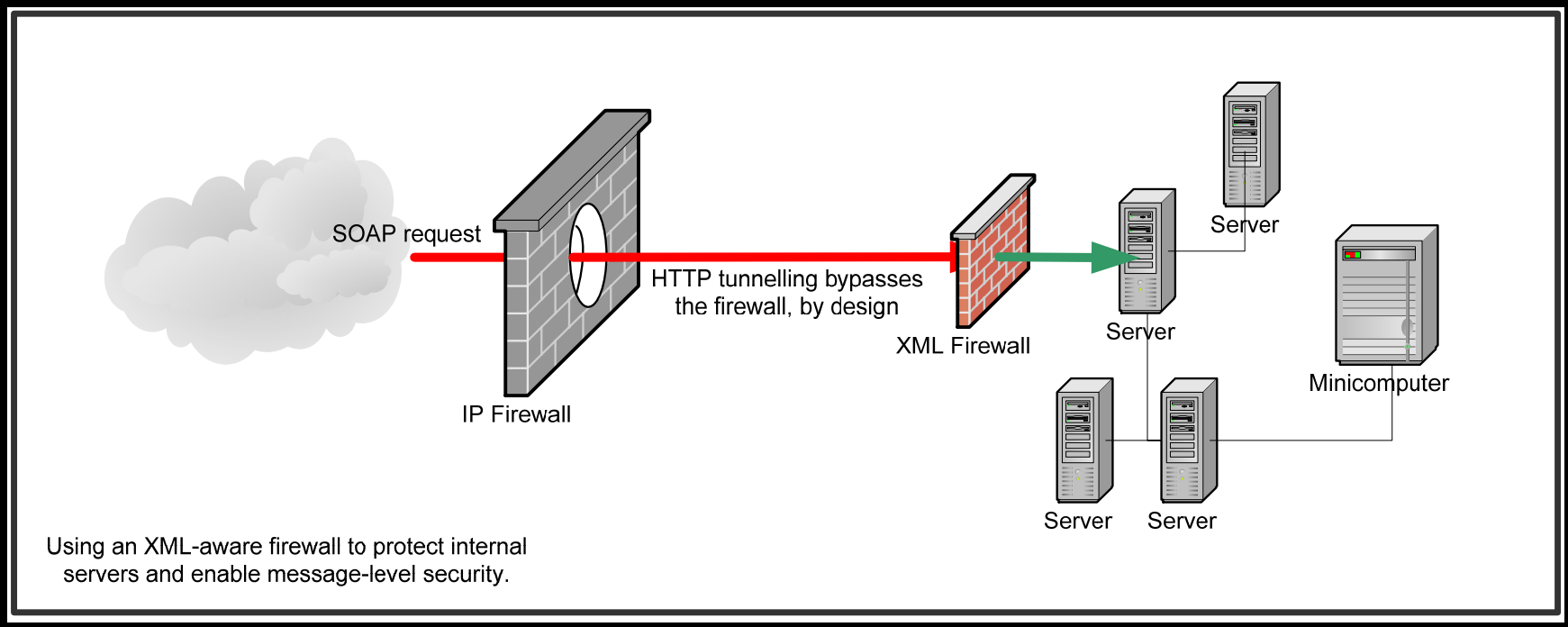
Lines 031-033:
Contain the body of the SOAP message

IBM Software Group

SOA Security Implementation

Traditional security measures are not sufficient to secure against threats on SOA

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



Using an XML-aware firewall to protect internal servers and enable message-level security.

Solution: Multiple levels of defense

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

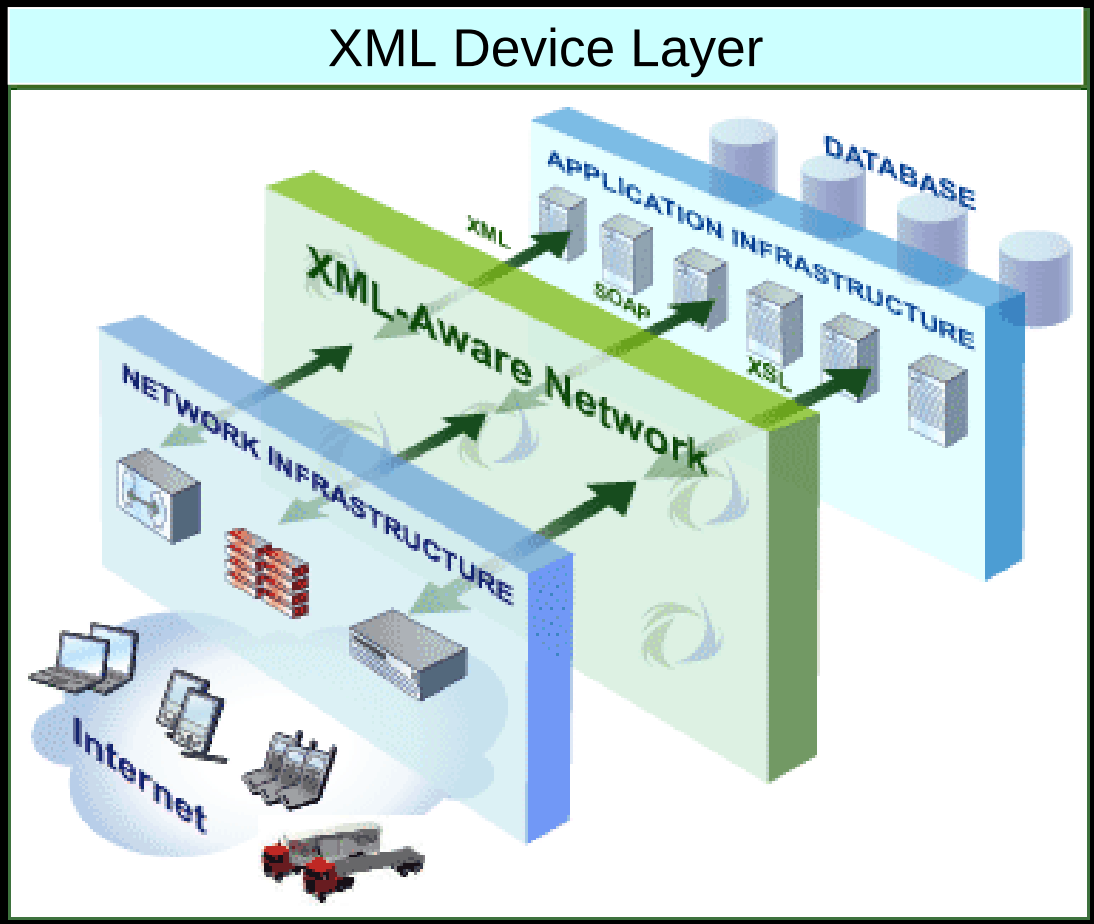
Gartner advises to implement a comprehensive set of security measures for SOA

- **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 MA
  - SAML, x.509, Passport, etc.
  - 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**
- **Use OTS Web Services With Caution**
- **Monitor and Control**

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

-- John Pescatore, Gartner

IBM approach is to adopt a XML device layer for SOA security



SOA Appliances

- Simpler to manage
- Higher level of security
- More scalable
- Quicker to deploy
- Reduced cost

The IBM DataPower product line implements most of the functions for SOA security and operates at the transport and application-oriented level

Specialized network devices simplify, help secure & accelerate SOA

XML Accelerator XA35

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

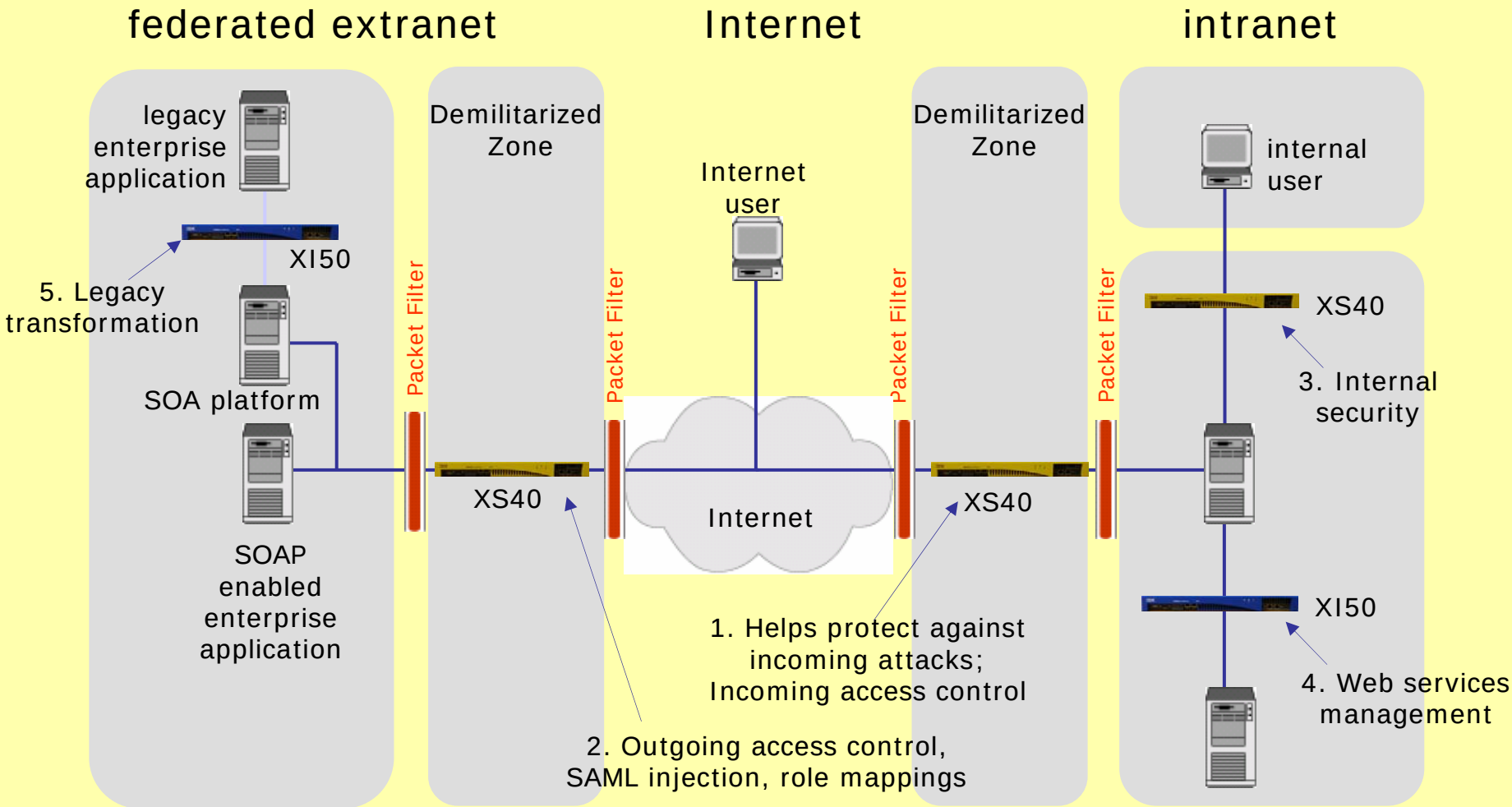
XML Security Gateway XS40

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

Integration Appliance XI50

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

SOA appliance can be deployed in both extranet and intranet as security policy enforcement points to protect SOA against potential attacks



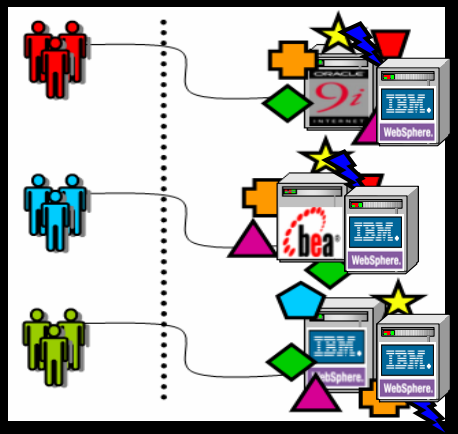
There are many good reasons for using an appliance for SOA security

- **Higher performance** with hardware acceleration**:**
  - Impact: ability to perform more security checks without slow downs
- **Hardened,** specialized hardware for helping to integrate, secure & accelerate SOA
- Multiple security and related 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
- **Simplified deployment** and ongoing management:
  - Impact: reduces need for in-house SOA skills & accelerates time to SOA benefits
- Addresses the divergent needs of different groups:
  - Example: enterprise architects, network operations, security operations, identity management, web services developers

One of the key benefits is that SOA appliances centralize and simplify key security functions

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

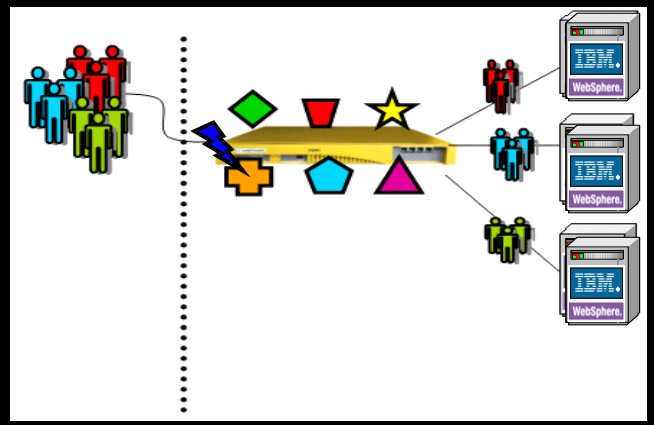
Before SOA Appliance



Update application servers individually

- **Security Processing**
- **Routing**
- **Web services management**
- **Transformation**
- **New XML standard**
- **Access control update**
- **Change purchase order schema**

After SOA Appliances

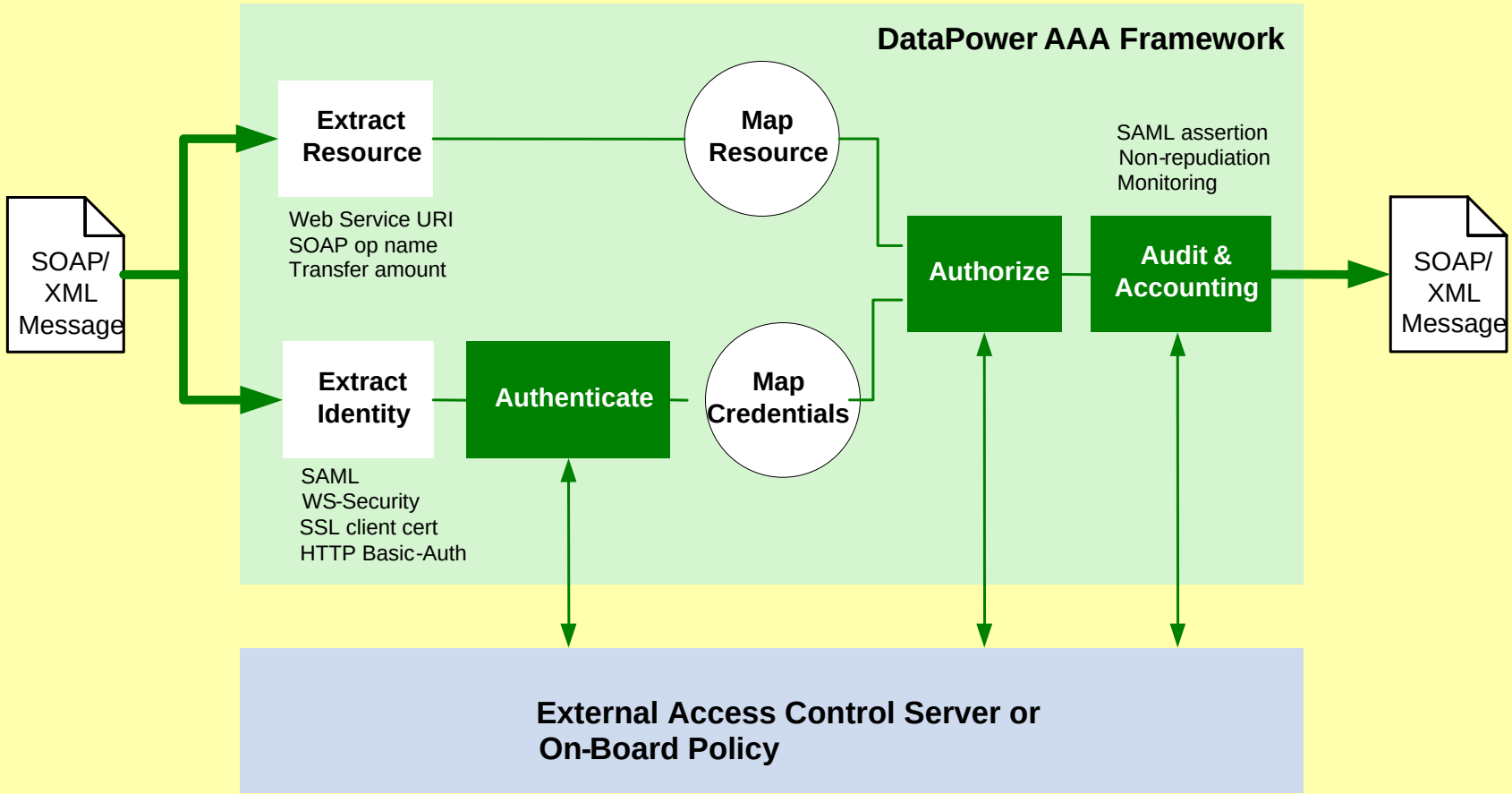


Secure, route, transform for all applications readily

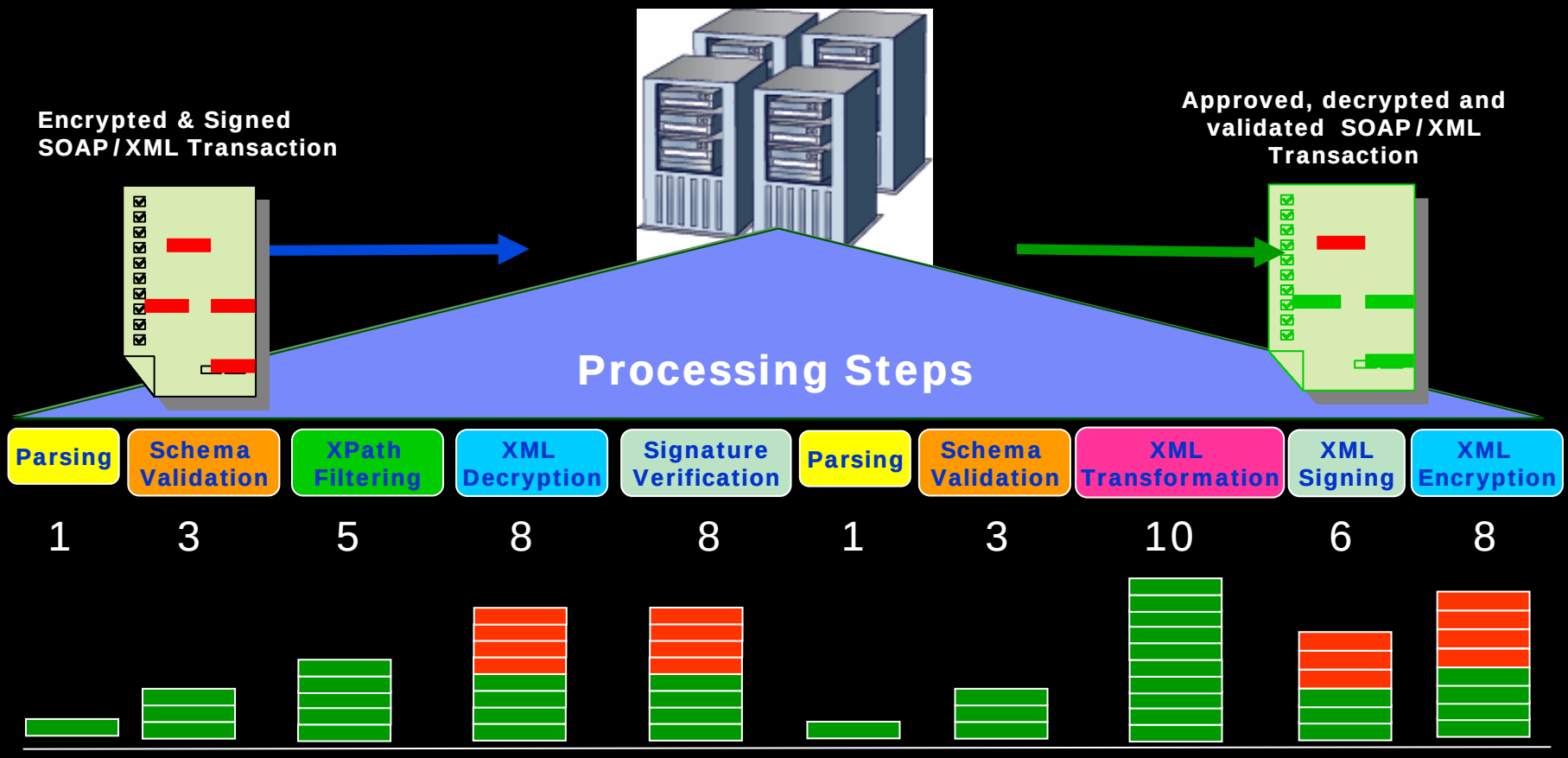
No changes to applications

DataPower SOA appliance implement authentication, authorization and audit

AAA Framework Diagram - Authenticate, Authorize, Audit

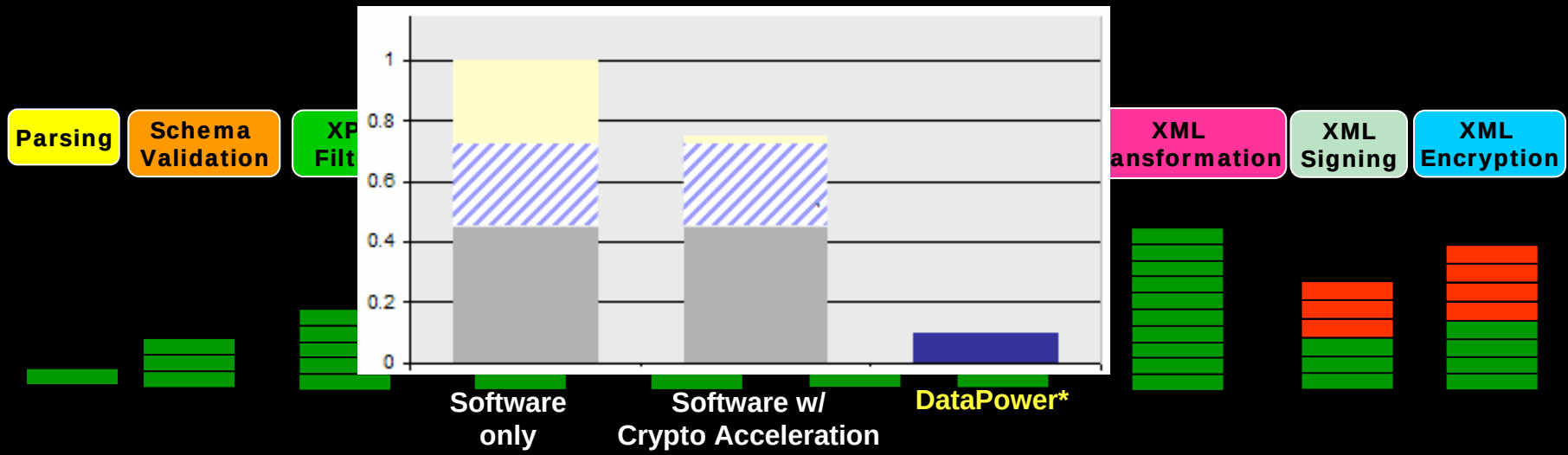


Web Service invocation involves heavy XML processing which consume a lot of server resources



SOA appliance make use of special purpose chips and can handle XML processing at a much faster speed and offloads server workload

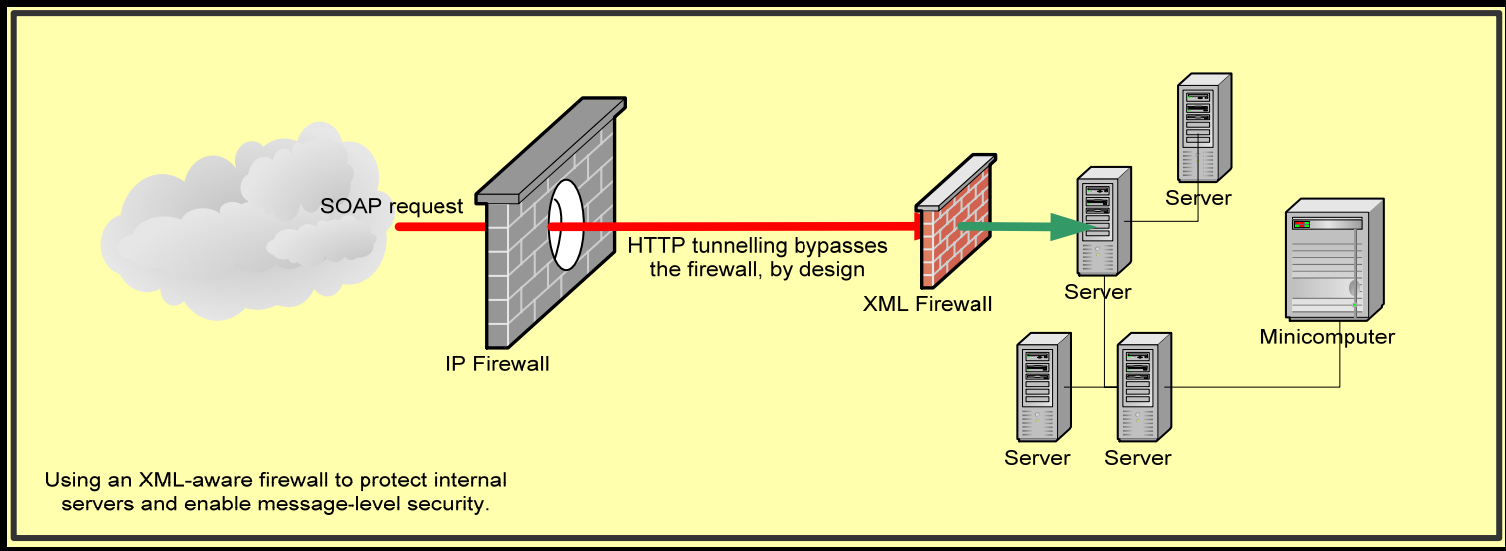
Performance is key to security & mediation



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

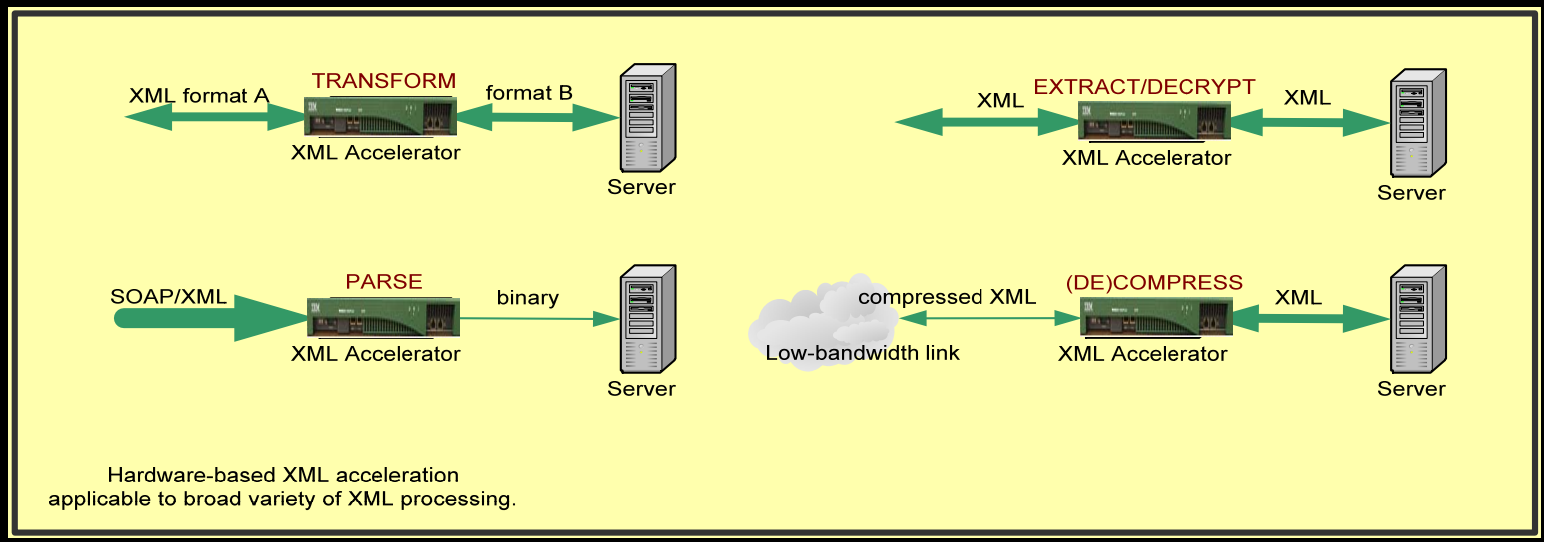
Usage scenario: XML Security Gateways / XML Firewalls

- XML Firewall, XML threat protection
- WS-Security, WS-Trust, digital signature, encryption
- Fine-grained access control
- Security policy enforcement point
- Service level management
- Service virtualization



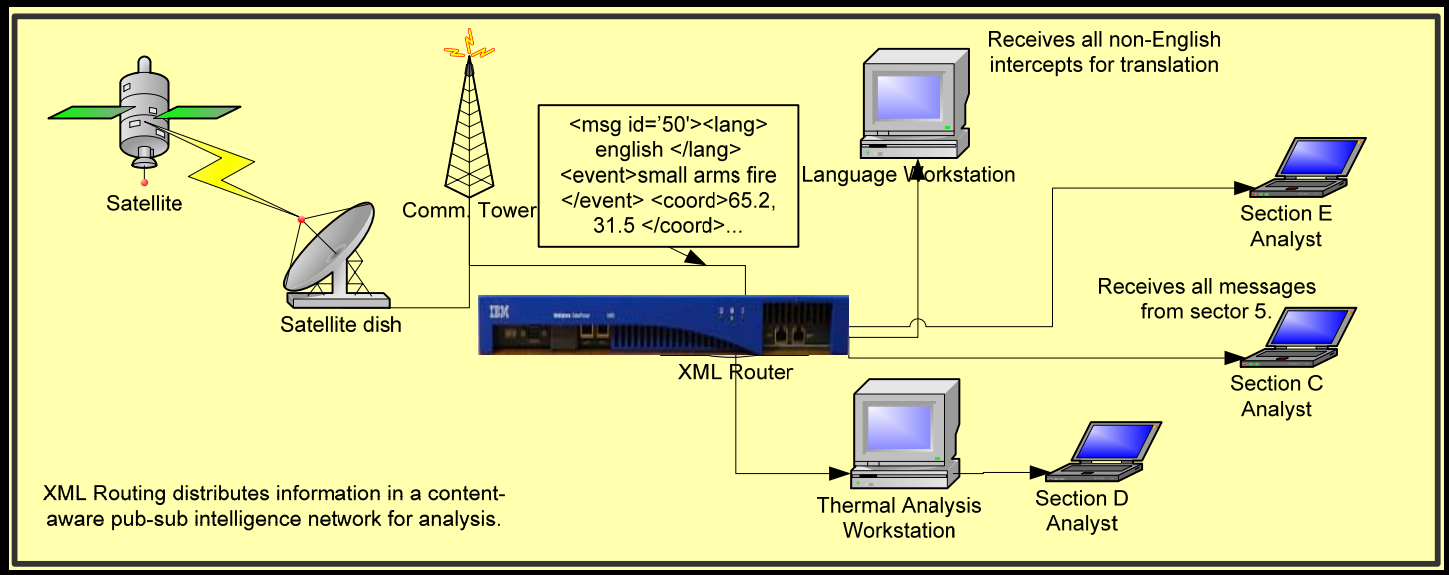
Usage scenario: XML Accelerators

- Offload XML Processing to dedicated Network Hardware
- Schema Validation
- XML Transformation, XSLT
- Compression
- Format Conversion
- XML Parsing / Object Marshalling Acceleration



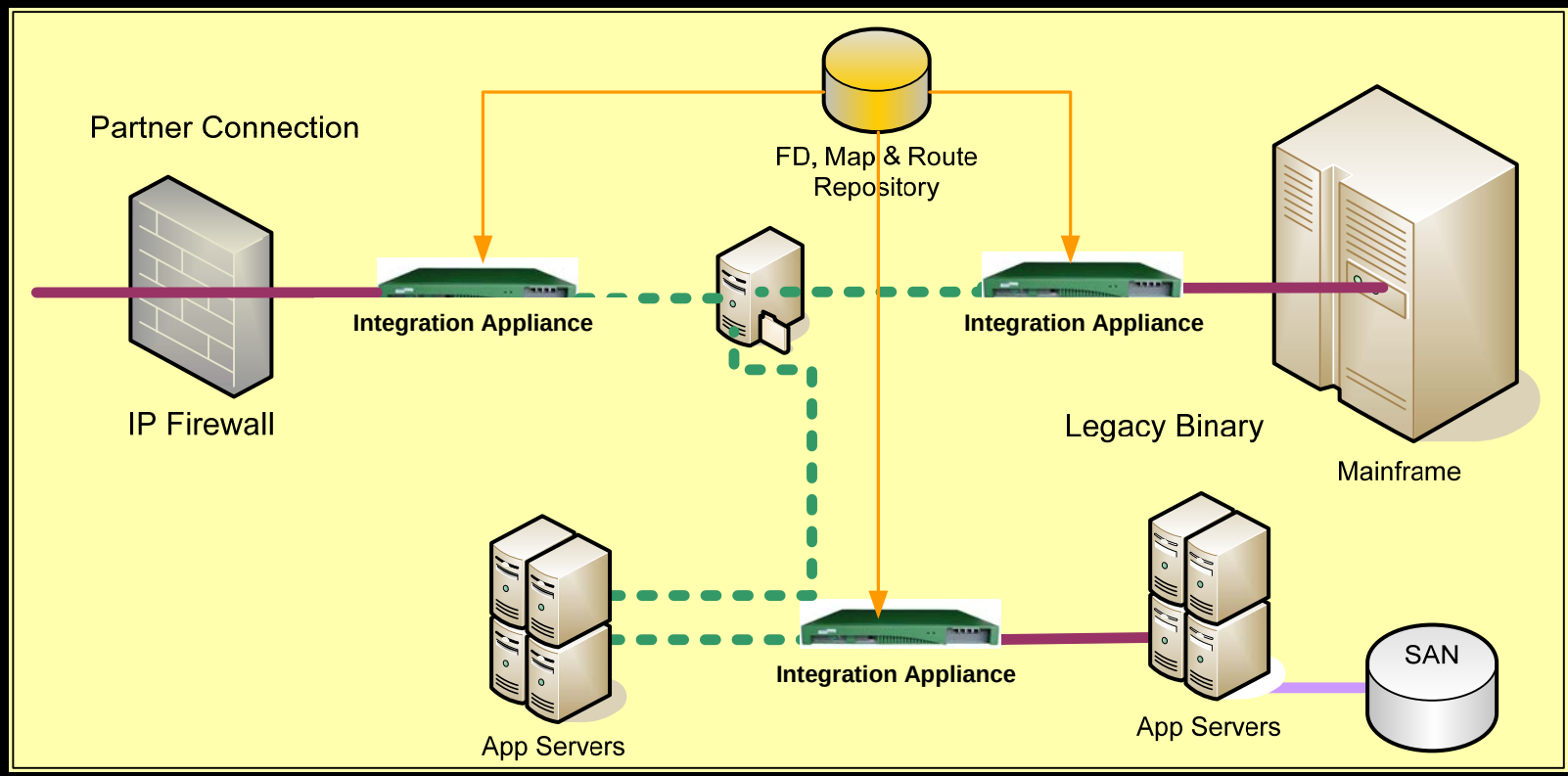
Usage scenario: XML Routers

- Content-based routing based on dynamic XPath tables
- SOAP protocol routing and load balancing
- Message enrichment via headers
- Publish-Subscribe based on content in messages
- Message duplication & relay
- QoS and QoP based on message content
- Routing and delivery independent of producers or consumers



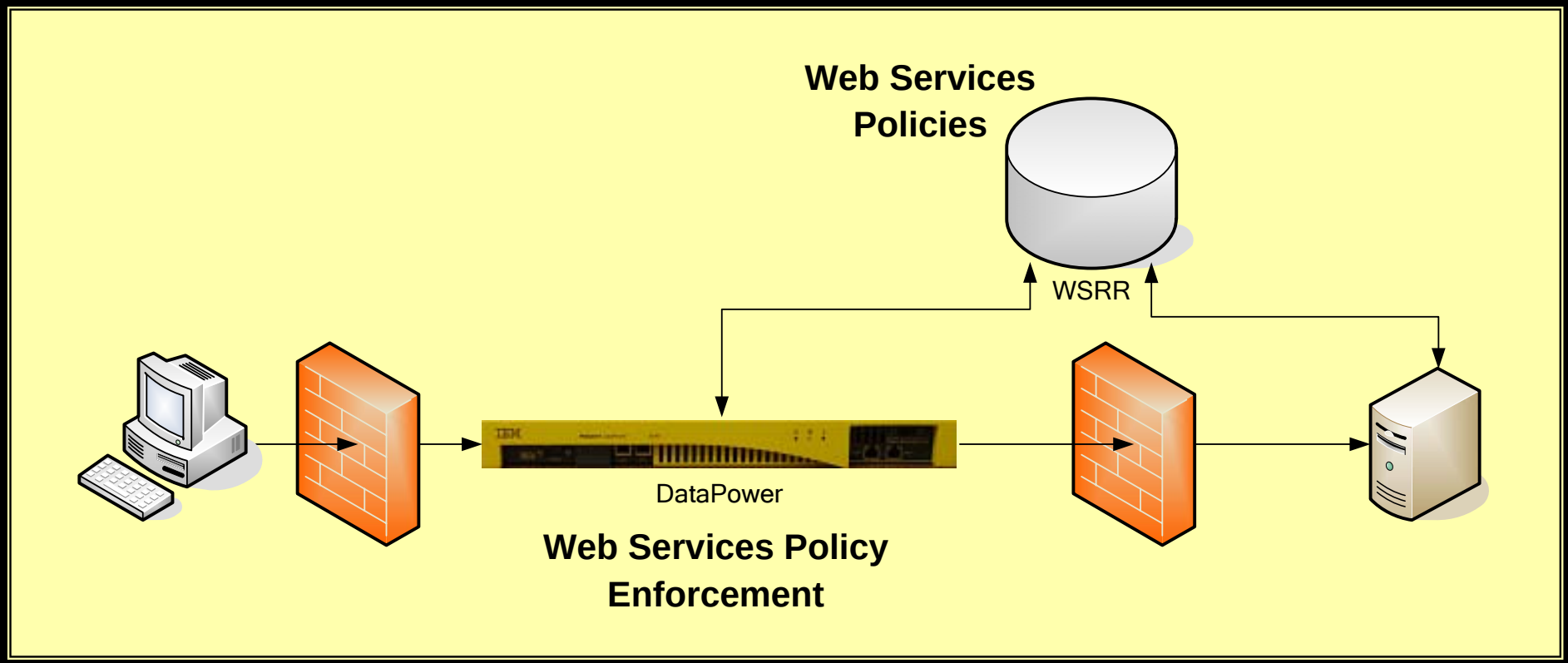
Usage scenario: Integration Appliances

- Support for non-XML messages (e.g. COBOL or EDI)
- For both external (B2B) and internal (EAI) integration
- Enhance ESB's, SOA-enable existing systems
- Business logic and apps continue to reside on servers



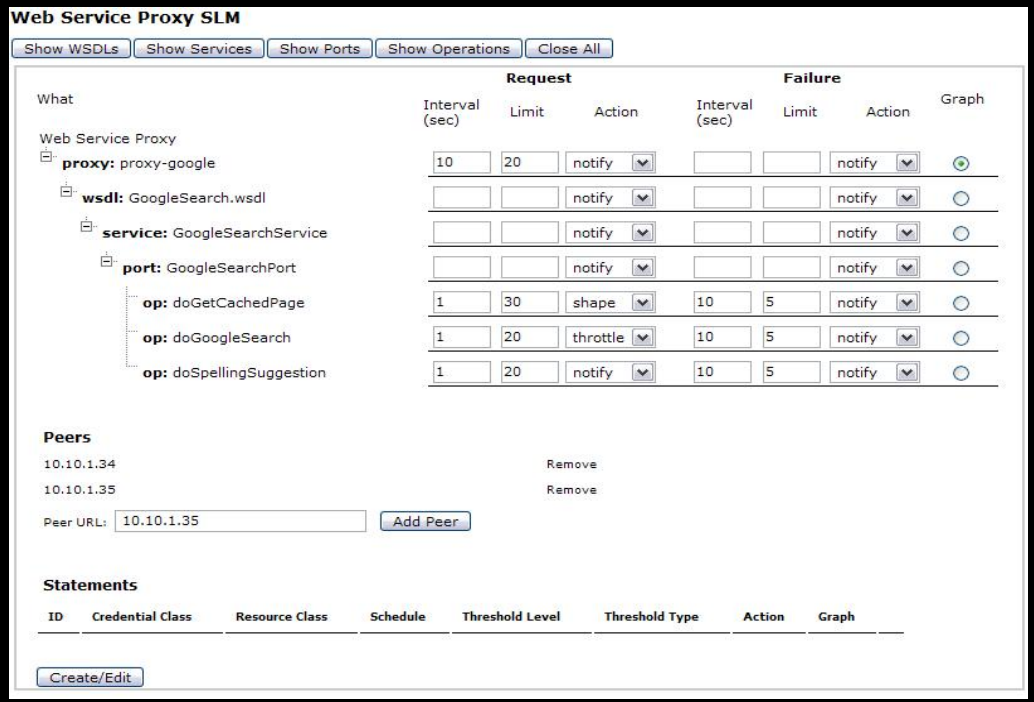
Usage scenario: Implement SOA Governance Policy

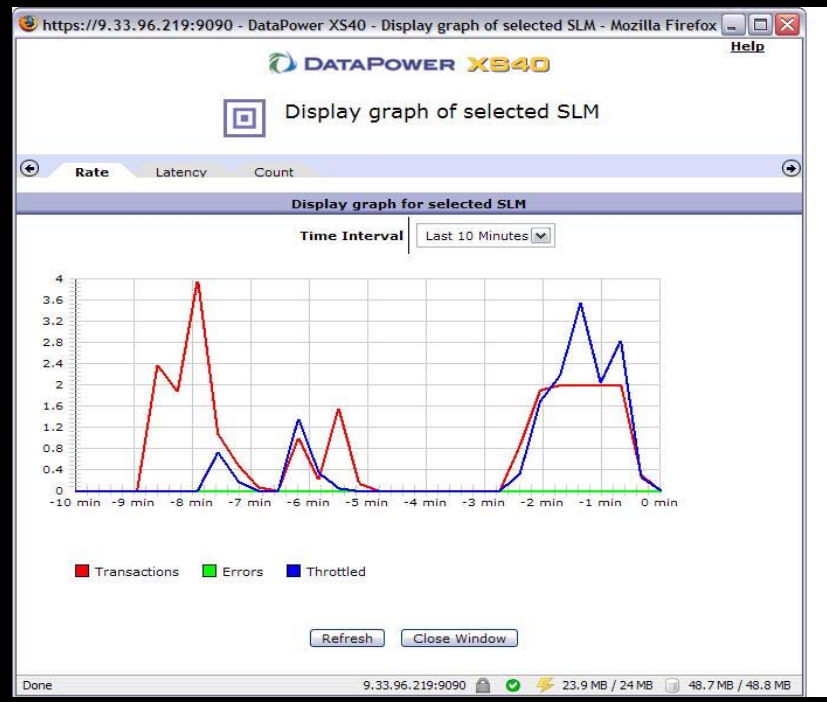
- Access to service policy, metadata and states stored in WebSphere Registry and Repository (WSRR)
- Serves as policy enforcement point to implement security and SOA governance policies at runtime



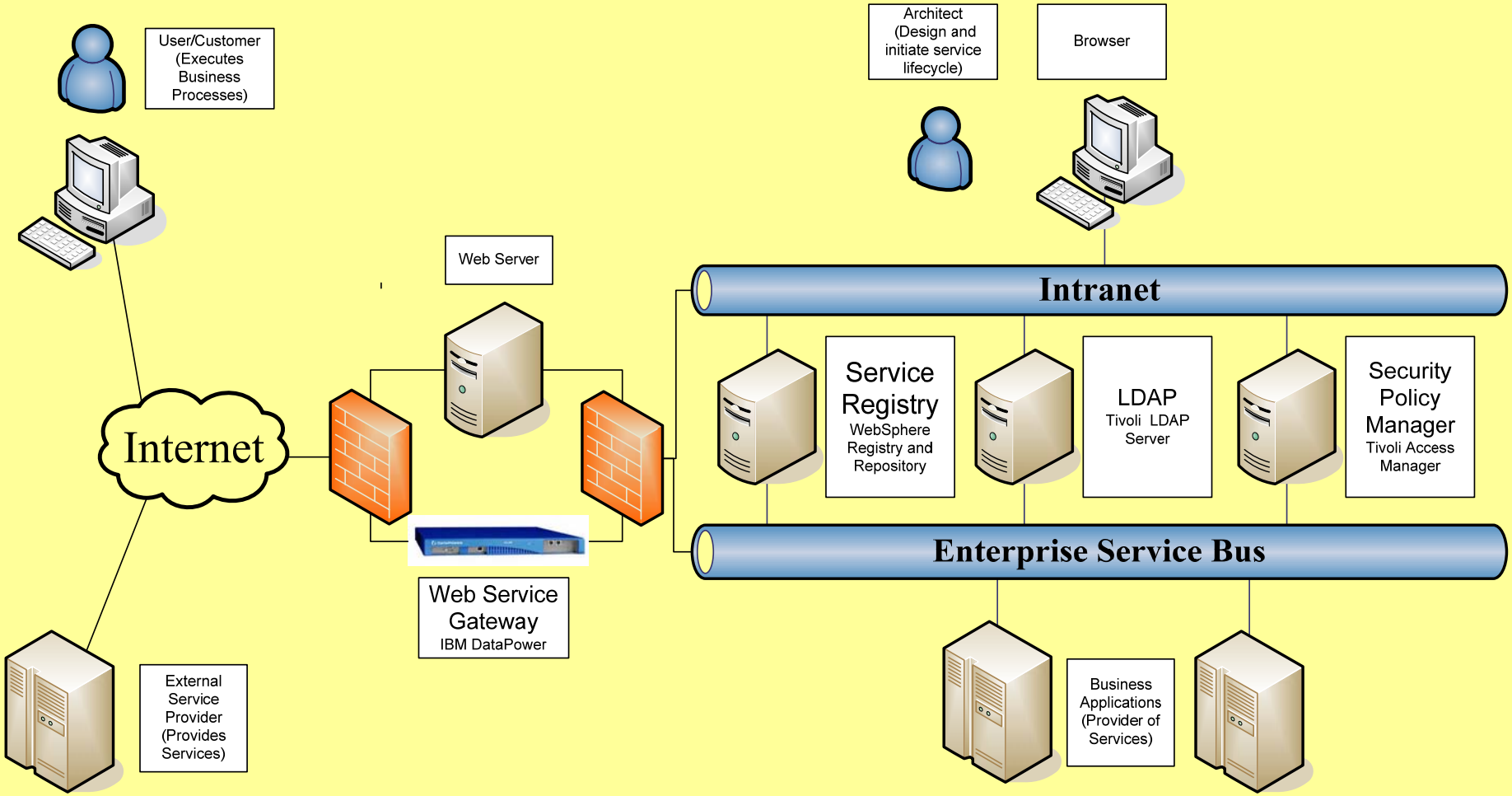
Usage Scenario: Service Level Management

- Hierarchical Service Level at WSDL, service, port, operational level
- Flexible actions when reaching a threshold: notify/alert, shape, throttle
- Threshold for both overall requests and failures
- Graphical display

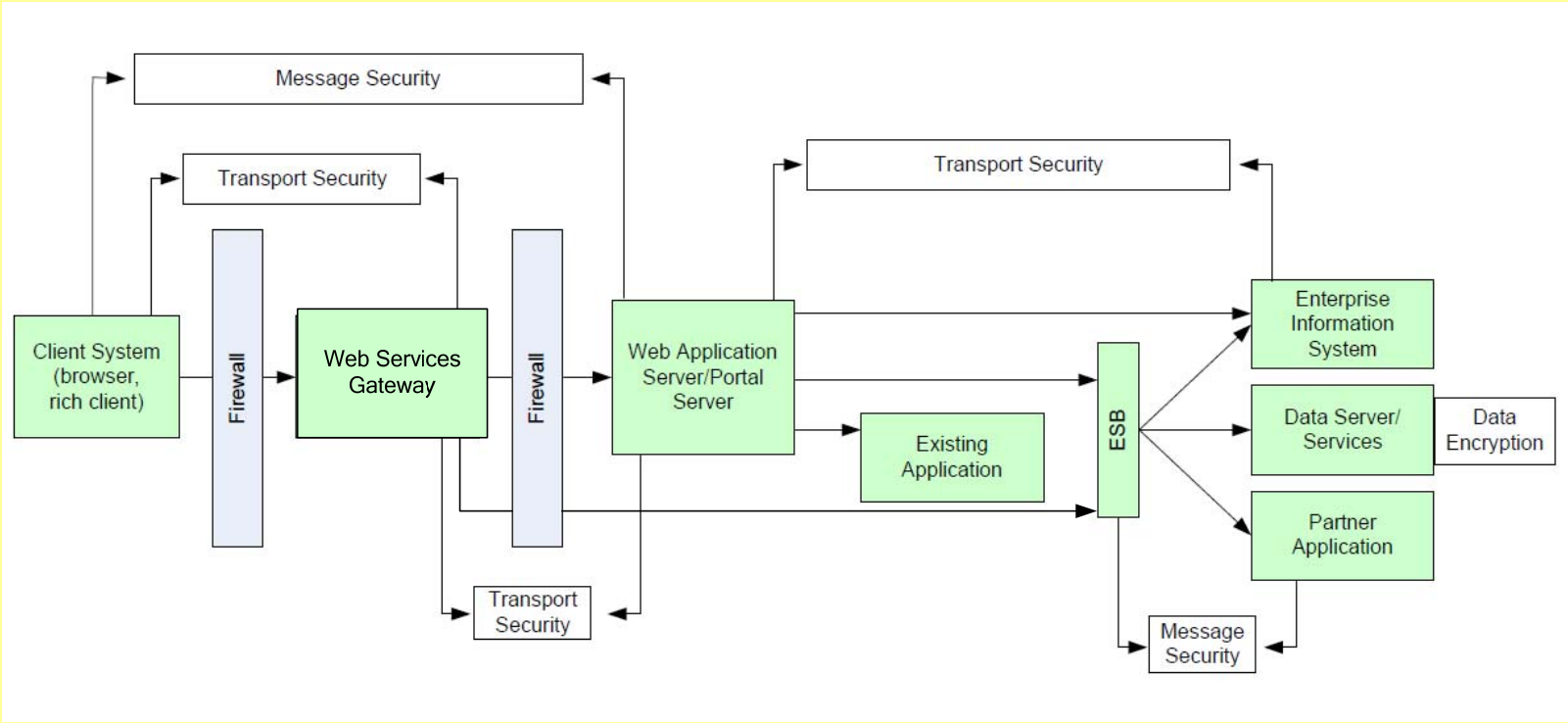




Architecture for SOA Security



SOA Security Logical Architecture



Useful Information

1. IBM Smart SOA Insight White Papers
   http://www-935.ibm.com/services/us/gbs/bus/html/soa-industry-series-tl.html

2. IBM Redbook: Understanding SOA Security Design and Implementations
   http://www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf

3. IBM SOA Portal
   http://www-01.ibm.com/software/solutions/soa/

4. SOA and WebServices Technical Papers
   http://www.ibm.com/developerworks/webservices