C11: Power your IMS Performance and Connectivity with DataPower

Shyh-Mei F. Ho
IBM Distinguished Engineer
IMS Integration SOA Chief Architect
SVL, San Jose, CA. USA

IMS Technical Symposium 2015

Agenda

- DataPower Overview
- IBM API Management and DataPower
- DataPower Virtual Editions
- Newly announced DataPower
- IMS Integration with DataPower
  - Integration with IMS Database
  - Integration with IMS Transactions
- Use Scenarios

IBM WebSphere DataPower organization makes appliances

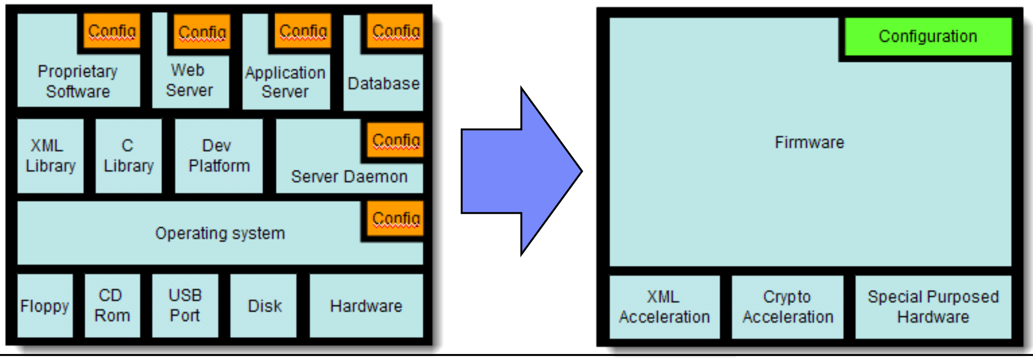
- Simple architecture:
  - microcode firmware + purpose-built hardware
- Delivered from the factory with everything you need to connect to the network and start working
  - No need to provision anything but the Ethernet network and CAT cables to get started
- All computationally-significant components sealed within a tamper-evident casing
  - Chips
  - Memory
  - Boards and cards
  - Flash-based file system (signed and encrypted)
  - Parsing and xform accelerator
  - Cryptographic accelerator

- Guiding philosophy is to take rote, repeatable security / integration tasks and lock them down in the appliance form factor, including:
  - Security gateway functions
  - Integration functions
  - B2B gateway functions
  - Application optimization functions

Purpose-built HW/SW combo

Appliance “lock down” means:

- Removing need for commodity code
- Removing reliance on general purpose operating systems and run times
- Porting to purpose-built firmware
- Simplicity = BIG TCO SAVINGS

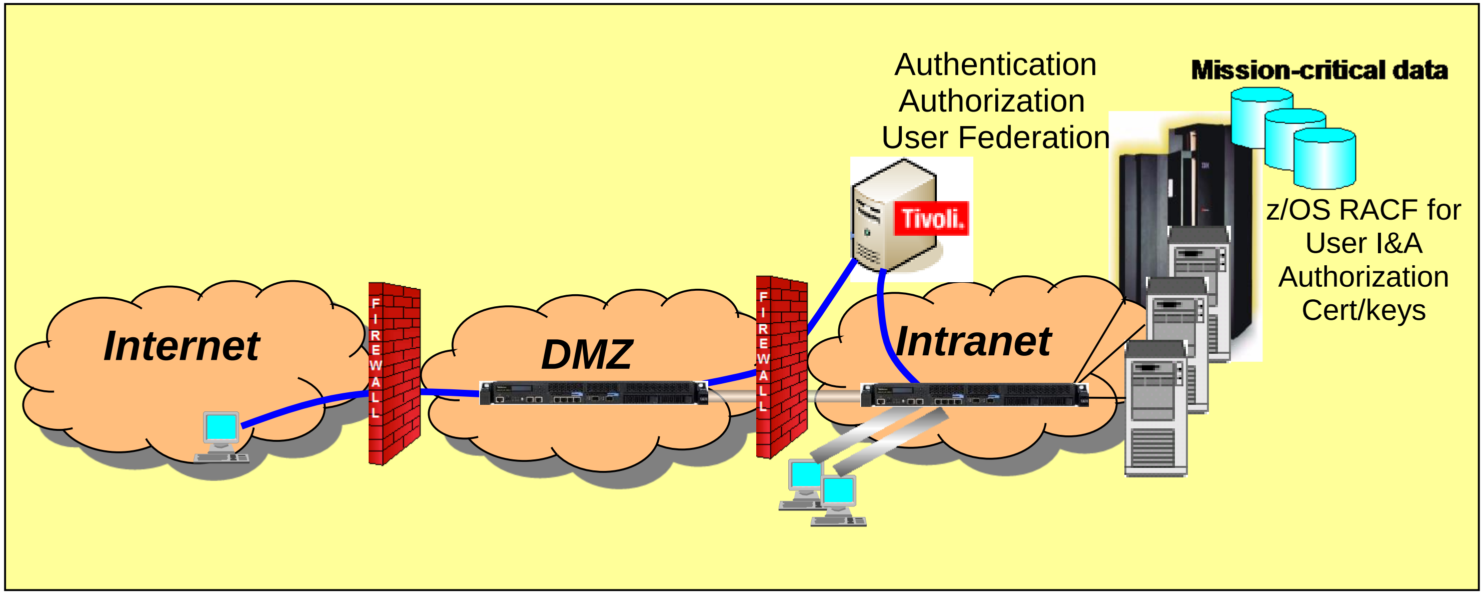


Config
Proprietary Software
Config
Web Server
Config
Application Server
Config
Database
XML Library
C Library
Dev Platform
Config
Server Daemon
Config
Operating system
Floppy
CD Rom
USB Port
Disk
Hardware

Configuration
Firmware
XML Acceleration
Crypto Acceleration
Special Purposed Hardware

DataPower security roles and objectives

- ✓ ***Secure access to Web and legacy applications***
- ✓ ***Converged security enforcement***
- ✓ ***Rocksolid DataPower platform***
- ✓ ***Leverages enterprise security and policy managers***



- **Protect data and other resources on the appliance and protected servers**
  - ***System availability***
    - Protect against unwanted access, denial of service attacks, and other unwanted intrusion attempts from the network
    - Only allow “valid” messages through
  - ***Identification and Authentication***
    - Verify identity of network users
  - ***Authorization***
    - Protect data and other system resources from unauthorized access

- **Protect data in the network using cryptographic security protocols**
  - ***Data End Point Authentication***
    - Verify who the secure end point claims to be
  - ***Data Origin Authentication***
    - Verify that data was originated by claimed sender
  - ***Message Integrity***
    - Verify contents were unchanged in transit
  - ***Data Confidentiality***
    - Conceal clear-text using encryption

DataPower: Supported standards & protocols

- **Data format & language**
  - **JavaScript**
  - JSON
  - JSON Schema
  - JSONiq
  - REST
  - SOAP 1.1, 1.2
  - WSDL 1.1
  - XML 1.0
  - XML Schema 1.0
  - XPath 1.0
  - XPath 2.0 (XQuery only)
  - XSLT 1.0
  - XQuery 1.0
- **Security policy enforcement**
  - **OAuth 2.0**
  - SAML 1.0, 1.1 and 2.0, SAML Token Profile, SAML queries
  - XACML 2.0
  - Kerberos, SPNEGO
  - RADIUS
  - **RSA SecurID OTP using RADIUS**
  - LDAP versions 2 and 3
  - Lightweight Third-Party Authentication (LTPA)
  - Microsoft Active Directory
  - FIPS 140-2 Level 3 (w/ optional HSM)
  - FIPS 140-2 Level 1 (w/ certified crypto module)
  - SAF & IBM RACF® integration with z/OS
  - Internet Content Adaptation Protocol
  - W3C XML Encryption
  - W3C XML Signature
  - S/MIME encryption and digital signature
  - WS-Security 1.0, 1.1
  - WS-I Basic Security Profile 1.0, 1.1
  - WS-SecurityPolicy
  - WS-SecureConversation 1.3

- **Transport & connectivity**
  - HTTP, HTTPS, **WebSocket Proxy**
  - FTP, FTPS, SFTP
  - WebSphere MQ
  - WebSphere MQ File Transfer Edition (MQFTE)
  - TIBCO EMS
  - WebSphere Java Message Service (JMS)
  - IBM IMS Connect, & IMS Callout
  - NFS
  - AS1, AS2, AS3, ebMS 2.0, CPPA 2.0, POP, SMTP (XB62)
  - DB2, Microsoft SQL Server, Oracle, Sybase, IMS
- **Transport Layer Security**
  - SSL versions 2 and 3
  - TLS versions 1.0, 1.1, and 1.2
- **Public key infrastructure (PKI)**
  - RSA, 3DES, DES, AES, SHA, X.509, CRLs, OCSP
  - PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
  - XKMS for integration with Tivoli Security Policy Manager (TSPM)
- **Management**
  - Simple Network Management Protocol (SNMP)
  - SYSLOG
  - IPv4, IPv6
- **Open File Formats**
  - Distributed Management Task Force (DMTF) Open Virtualization Format (OVF)
  - Virtual Machine Disk Format (VMDK)
  - Virtual Hard Disk (VHD)

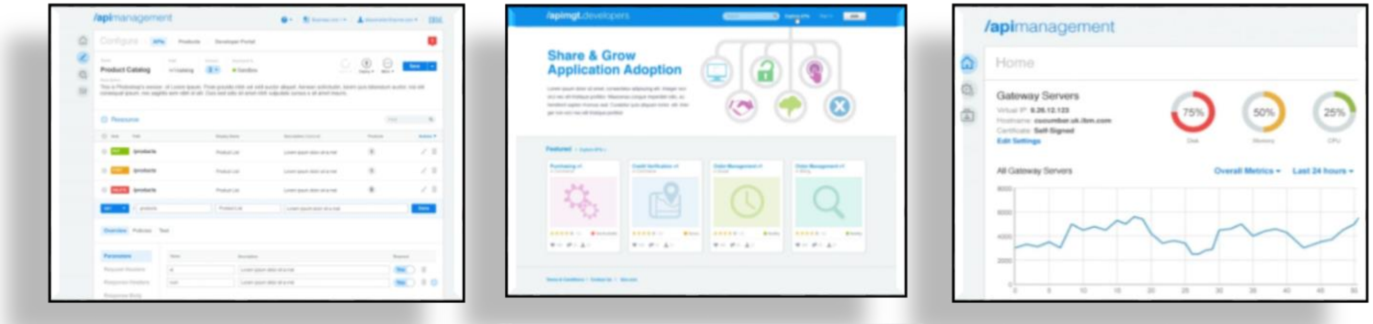
- **Web services**
  - WS-I Basic Profile 1.0, 1.1
  - WS-I Simple SOAP Basic Profile
  - WS-Policy Framework
  - WS-Policy 1.2, 1.5
  - WS-Trust 1.3
  - WS-Addressing
  - WS-Enumeration
  - WS-Eventing
  - WS-Notification
  - Web Services Distributed Management (WSDM)
  - WS-Management
  - WS-I Attachments Profile
  - SOAP Attachment Feature 1.2
  - SOAP with Attachments (SwA)
  - Direct Internet Message Encapsulation (DIME)
  - Multipurpose Internet Mail Extensions (MIME)
  - XML-binary Optimized Packaging (XOP)
  - Message Transmission Optimization Mechanism (MTOM)
  - WS-MediationPolicy (IBM standard)
  - Universal Description, Discovery, and Integration (UDDI versions 2 and 3), UDDI version 3 subscription
  - WebSphere Service Registry and Repository (WSRR)

Link to DataPower Information Center

A single, comprehensive solution to design, secure, control, publish, monitor & manage APIs

IBM API Management

Fully on-premise, multi-tenant solution, for API providers



IBM DataPower

API Gateway for security, control, integration & optimized access to a full range of Mobile, Web, API, SOA, B2B & Cloud workloads

Over a decade of innovation, 10,000+ units sold, 2000+ customer installations worldwide

Easily manage your APIs

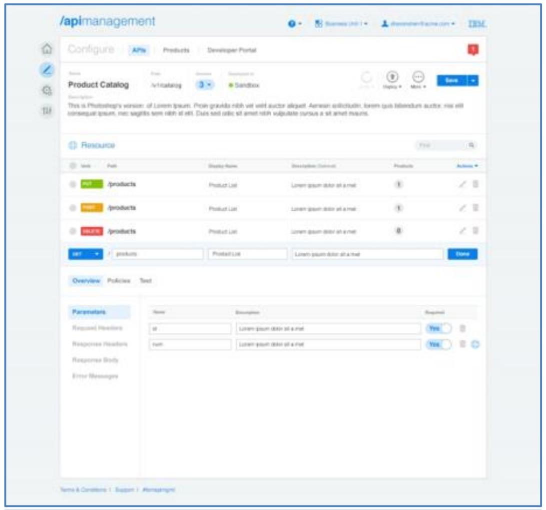
design, secure, control, publish, monitor & manage

Developer Portal

Explore API documentation

Provision application keys

API Manager

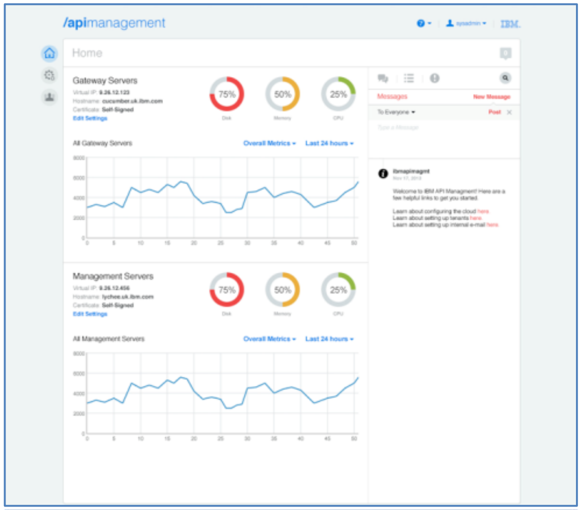


Define and manage APIs

Explore API usage with analytics

Manage API user communities

Management Console



Provision system resources

Monitor runtime health

Scale the environment

IBM DataPower Virtual Edition (VE)

Deployment flexibility plus reduced cost for development & test environments

Business Value:

- Industry-leading workload security, optimization, and integration **functionality similar** to the corresponding physical DataPower appliance models
- A **flexible, cost effective** Security & Integration Gateway for non-production environments
- A **production solution** for environments not suitable for physical appliance deployment

Features:

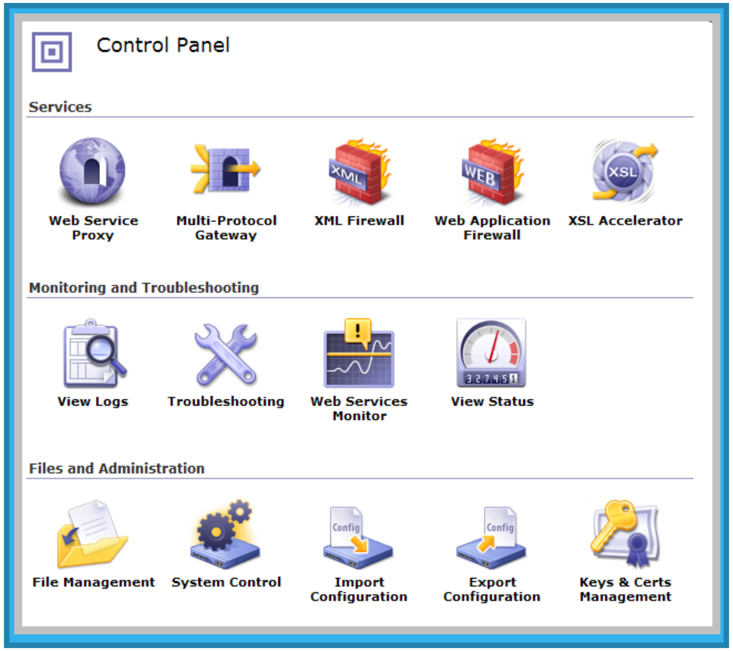
- WebSphere DataPower XG45 & XI52 physical appliance functionality in a "virtual appliance" form-factor running on **VMware** or **Citrix XenServer** hypervisor on **x86 servers**, IBM **PureApplication System** W1500**,** & **SoftLayer** dedicated server or bare metal instance platforms
- Ability to **upgrade & downgrade** firmware similar to physical appliances
- **Seamless configuration migration** between physical and virtual appliances
- Powered by a **purpose-built platform** including an embedded, optimized DataPower Operating System

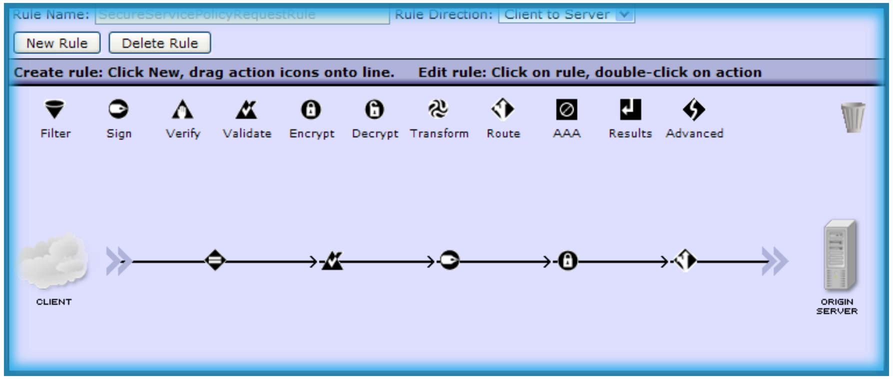
SOFTLAYER®
an IBM Company

DataPower Appliances extends its market leading Security & Integration Gateway functionality into Virtual Appliances providing deployment flexibility

VE Design Points

- Make virtual DataPower a new deployment option
  - •Once deployed, it should behave like any other DataPower appliance
- Where applicable, maintain full functionality
  - •New features on physical, become new features on virtual
- Maintain the same firmware upgrade/downgrade philosophy and capability
- Provide for configuration import/export between virtual-to-virtual and virtual-to-physical appliances
- Provide the same workload security as physical appliances
- Overall performance adjustable through the virtual resources allocated by the VM management system
- Architected to allow easy porting to new platforms




Rule Name: SecureServicePolicyRequestRule Rule Direction: Client to Server

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action

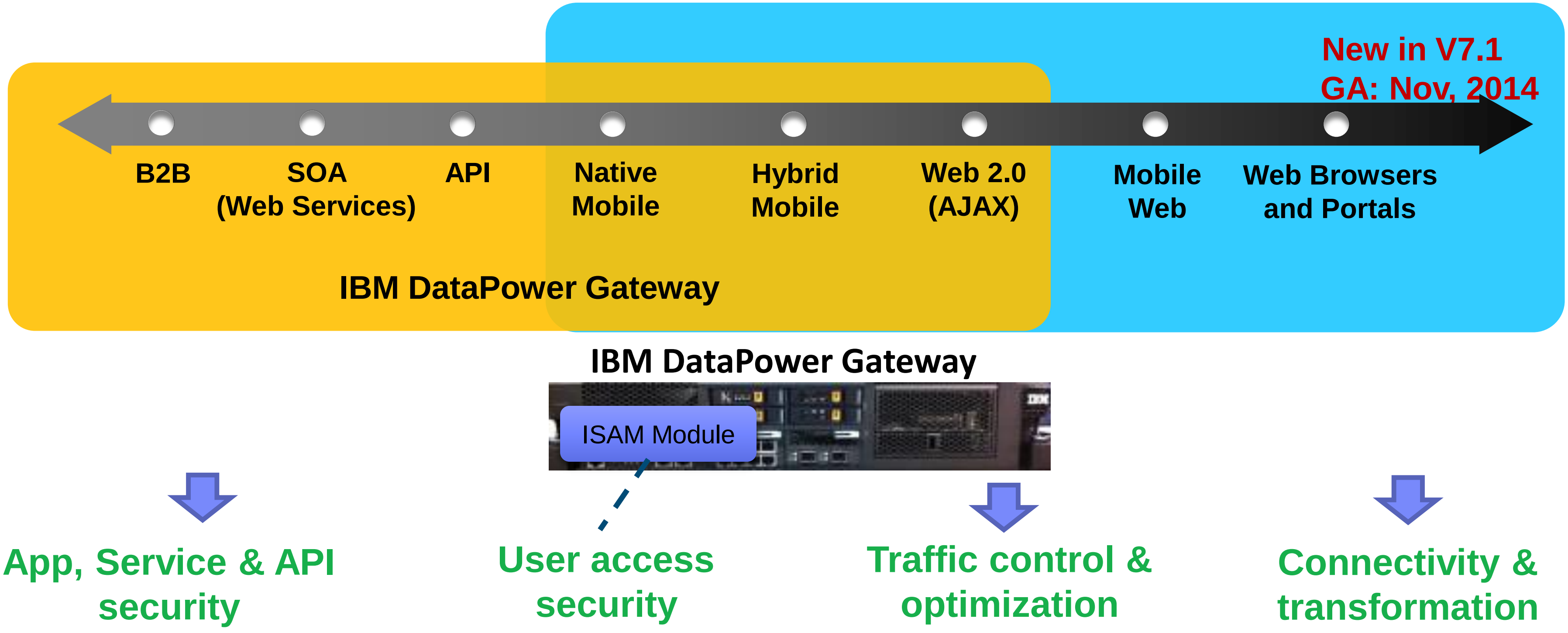
DataPower VE Security

- Once deployed, DataPower Virtual Editions behave like their physical appliance counterparts
    - All DataPower Security Best Practices apply to DP VE as well
- Hardware is virtualized as part of the VM infrastructure so some functions which require HW assist are not supported:
    - Intrusion detection
    - TPM (Trusted Platform Module)
    - Crypto acceleration
    - HSM (Hardware Security Module)
- Secure backup/restore supported for:
    - Backup on virtual, restore to virtual
- Configuration export/import supported for:
    - Export from virtual, import to virtual or physical
    - Export from physical, import to physical or virtual
- Chain of trust down to the hardware requires DataPower physical appliances
    - DataPower Virtual Editions adds deployment options for secure virtual environments

New

IBM *DataPower: Multi-channel gateway (V7.1)*

- **IBM DataPower Gateway**
  - **Is the new name of a consolidated, extensible & modular platform**
    - Converges three existing products, XG45 / XI52 / XB62, into a single modular offering
    - Available in physical and virtual form factor
  - **Is the single Security & Integration gateway platform to provide security, integration, control & optimized access to a full range of Mobile, API, Web, SOA, B2B, & Cloud workloads**



New in V7.1
GA: Nov, 2014

B2B

SOA
(Web Services)

API

Native
Mobile

Hybrid
Mobile

Web 2.0
(AJAX)

Mobile
Web

Web Browsers
and Portals

IBM DataPower Gateway

IBM DataPower Gateway

ISAM Module

App, Service & API security

User access security

Traffic control & optimization

Connectivity & transformation

❑ ISAM: IBM Security Access Manager

DataPower Gateway: Single product with Modules (V7.1)

WebSphere DataPower

3 Products (XG45/XI52/XB62)

2 Physical appliances (1U & 2U)

2 Virtual appliances (XG45/XI52)

IBM DataPower Gateway

1 Product

1 Physical appliance (2U only)

1 Virtual appliance

IBM WebSphere DataPower Service Gateway XG45

(1U Physical, Virtual Edition)

IBM DataPower Gateway

(2U Physical, Virtual Edition)

IBM WebSphere DataPower Integration Appliance XI52

(2U Physical, Virtual Edition)

IBM DataPower Gateway + Integration Module

(2U Physical, Virtual Edition)

IBM WebSphere DataPower B2B Appliance XB62

(2U Physical)

IBM DataPower Gateway + B2B Module

(2U Physical, Virtual Edition)

*** **Integration & B2B** Module are **independent** & can be purchased separately

IBM DataPower Gateway Virtual Edition provides the same functionality & modules as physical appliances with the exception of HSM (that provides **FIPS 140-2 Level 3** certification)

IBM DataPower Gateway 2U rack mount physical appliance is available with optional HSM (FIPS 140-2 Level 3 certified) or without

WebSphere DataPower: Mainframe integration

Offload processing for reduced MIPS
Services Enablement for
IMS, DB2, CICS

WebSphere DataPower deployed in the DMZ

is the first level of security for access control, threat protection, and data validation

Identity & Access Management

Threat Protection

Data Security

IBM DataPower: Multi-channel gateway …

IBM DataPower: Mobile Gateway

for all types (native, hybrid, and browser-based) of mobile applications for both Apple or Android.

IBM DataPower: Cloud Gateway

is the internal Gateway for all Bluemix traffic.
is the enterprise Gateway for "Cloud Integration" .

IBM DataPower is a purpose-built Gateway for IBM API Management

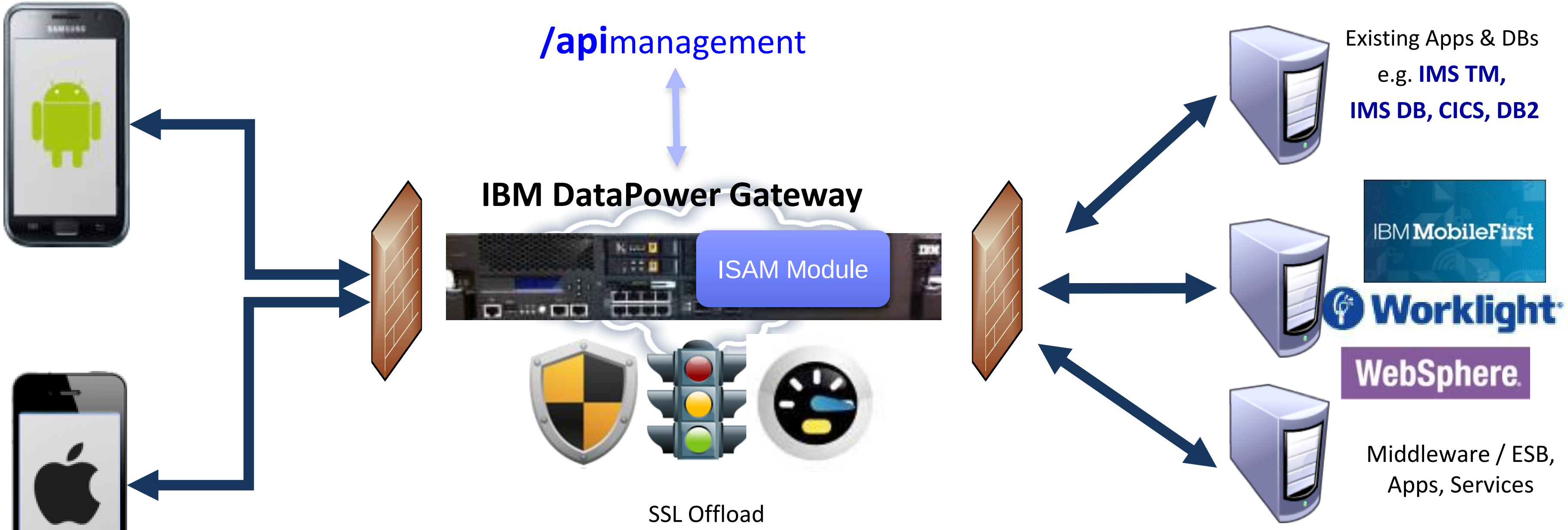
Identity & Access Management

Threat Protection

Data Security

Rapidly Connect Mobile Apps with Enterprise Services

Securely expose enterprise ***data & APIs*** *to Mobile Apps while optimizing delivery*

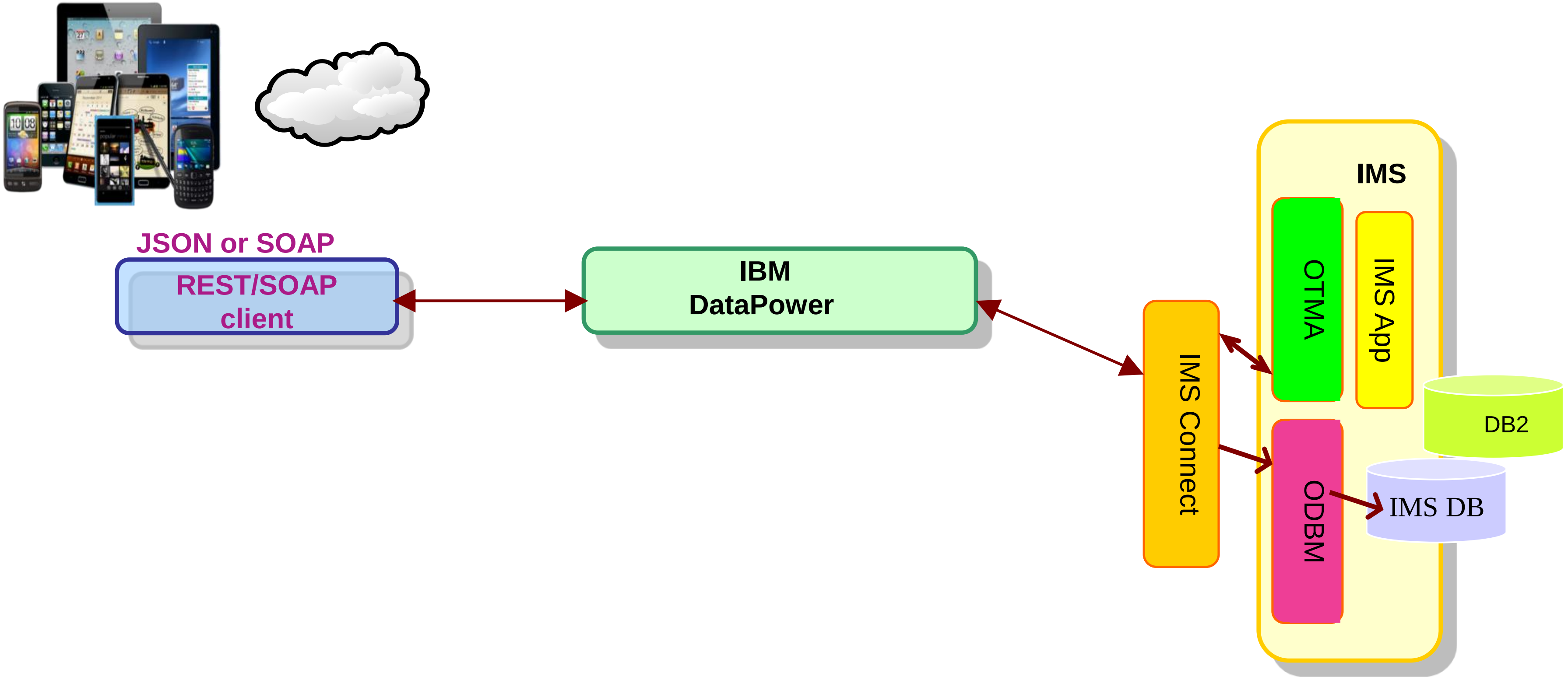


SSL Offload
Threat Protection
Rate Limiting / SLA Enforcement
Validation, Filtering
Authentication
Authorization
Context-based Access
Mobile SSO
Security Token Translation
Message Transformation
Content-Based Routing
Intelligent Load Distribution
Response Caching

Native, Hybrid,
Mobile Web

Mobile Integration with IMS

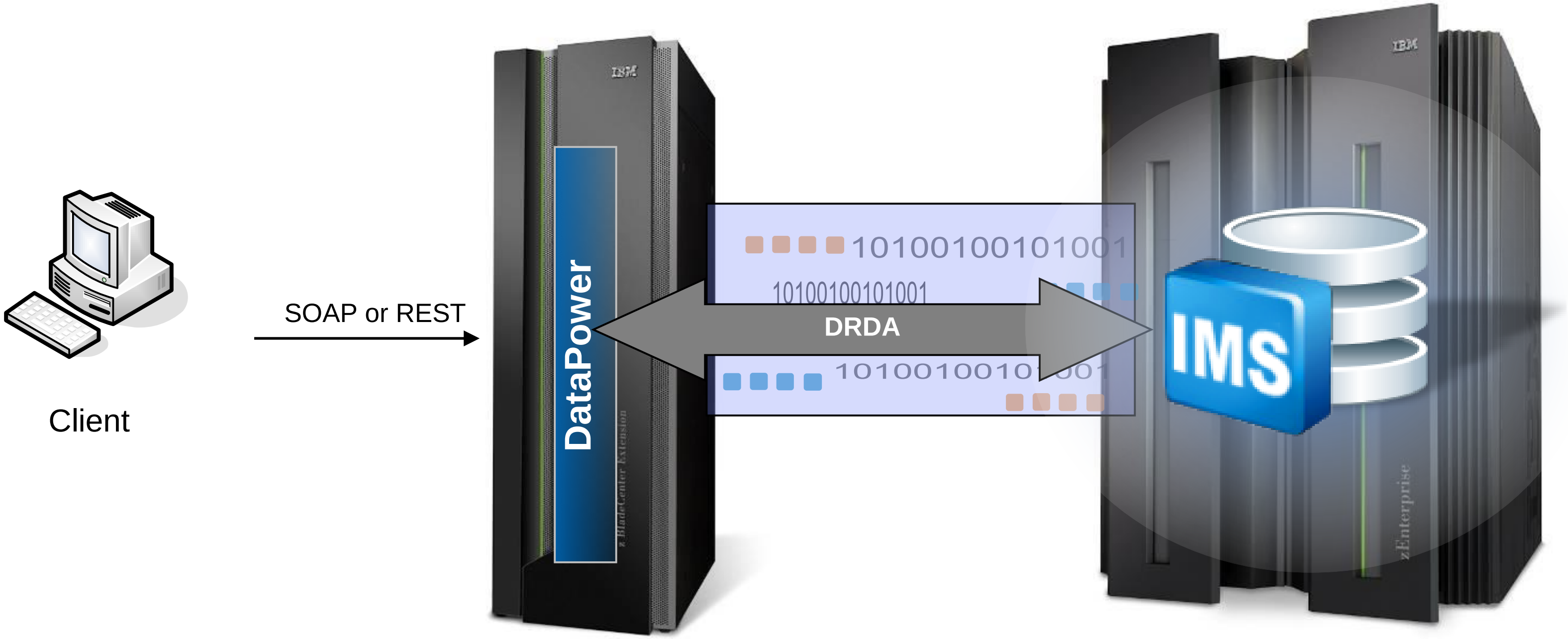
- IBM DataPower as the Web and RESTful service facade
  - DataPower supports bi-directional communications with IMS transactions
  - DataPower supports direct access to IMS database



IMS DB Integration with DataPower

"Information as a Service"

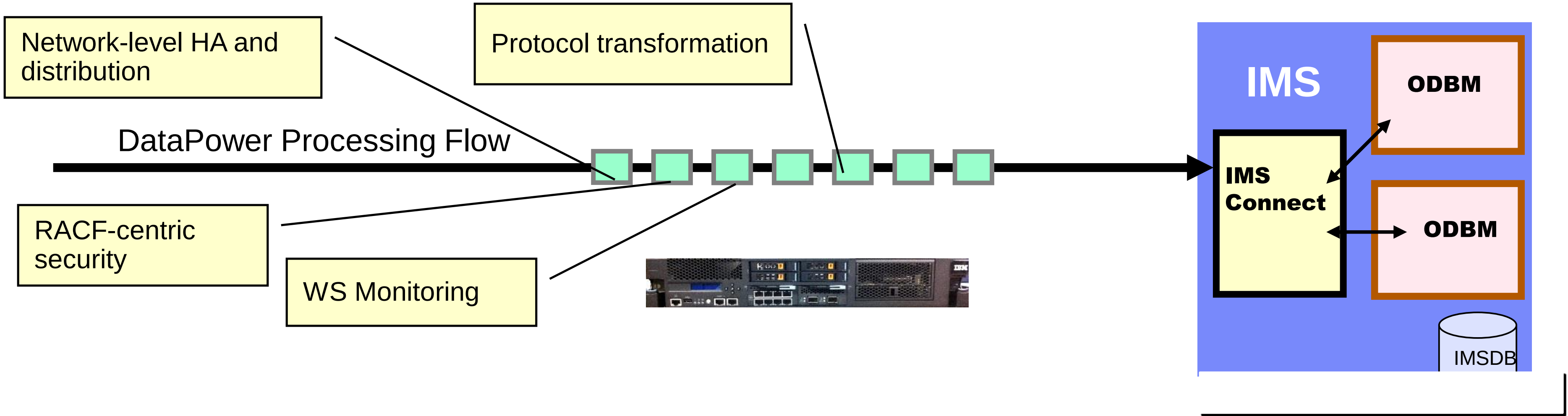
- DataPower provides a standard Web Service façade to IMS database
  - SOAP or REST call is mapped to a JDBC (DRDA) invocation
- Exposes database content (information) *as a service*
- Leverages extensive Web Services security and management capabilities of DataPower to more securely expose critical data to the enterprise



Direct Access IMS database via DataPower 6.0+

- IMS Open Database offers direct access to IMS database resources anywhere in the IMSplex from z/OS and distributed environments
  - Support different APIs to leverage Distributed Relational Database Architecture (DRDA)
    - IMS universal DB resource adapter to support J2EE, e.g. WebSphere
    - IMS universal JDBC driver to make SQL calls
    - IMS universal DL/I driver
  - Open Database Manger (ODBM) works together with IMS Connect as a DRDA server for IMS data

- DataPower to access IMS database directly via the Open Database capability, i.e. via IMS Connect and ODBM
  - An IMS database is defined to DataPower as an SQL data source. For each IMS database that you will access, you need to configure a separate SQL data source

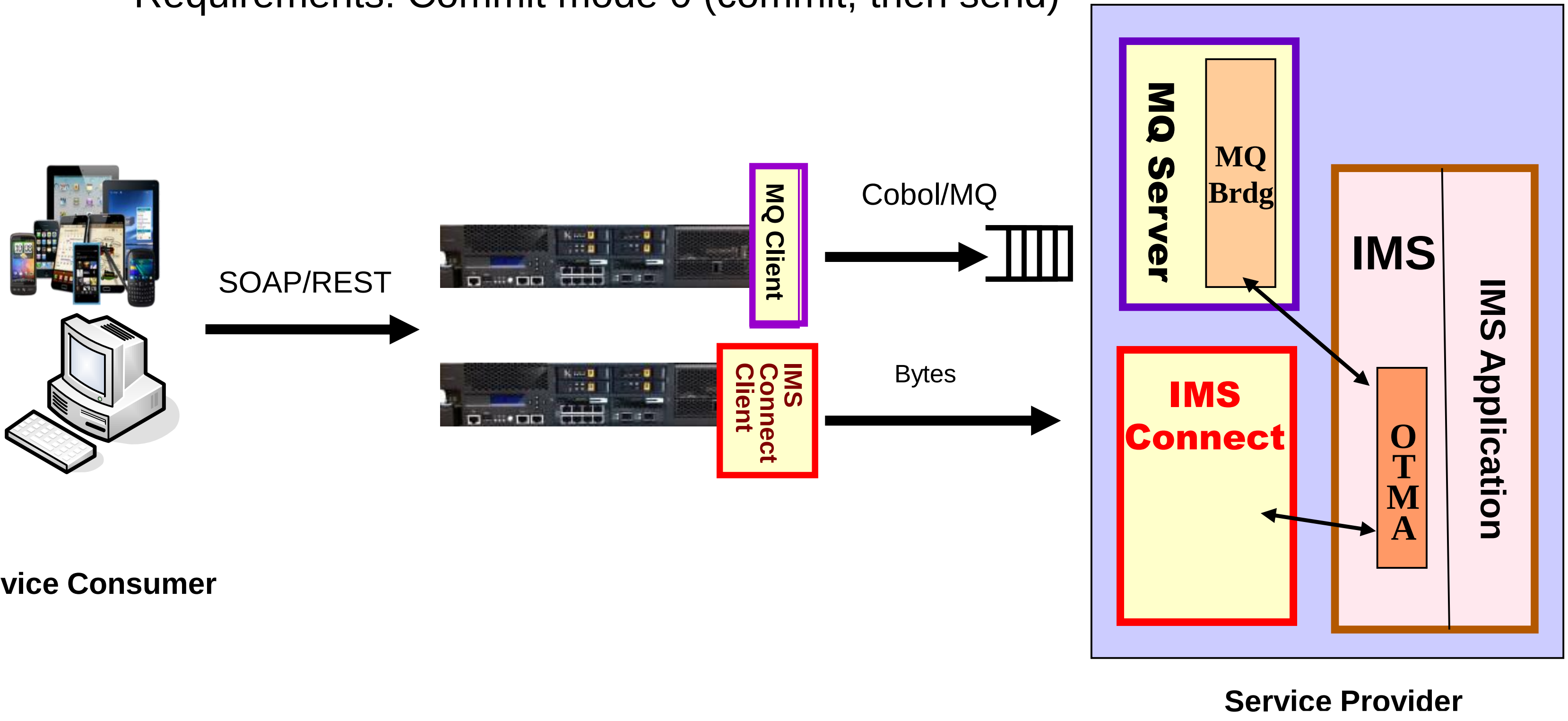


Prerequisites for IMS DB

- Software requirements
  - IMS V12, IMS Catalog, ODBM and SCI
    - – IMS Catalog to access to metadata of IMS programs and databases resources .
    - – IMS Connect
      - ODACCESS statement in HWSCFGxx member of a concatenated PROCLIB data set
  - DataPower Firmware 6.0.0.0 or higher
- Hardware requirements
  - WebSphere DataPower appliance XI52, XB62, XG45
  - IBM DataPower Gateway

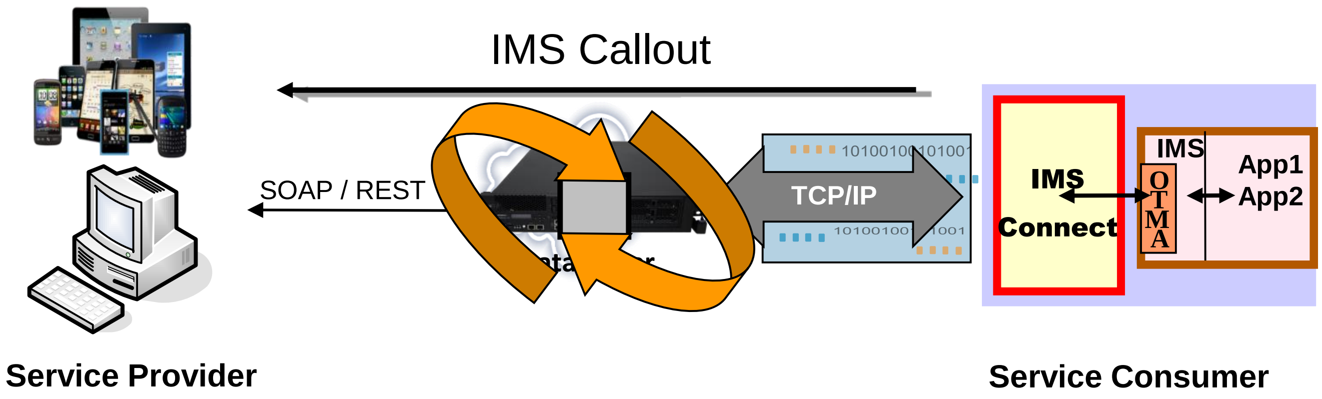
IMS TM Integration with DataPower

- **MQBridge to interface with IMS transactions**
  - MQ client is embedded in DataPower
- **IMS Connect to drive IMS transactions (inbound requests)**
  - IMS Connect client in DataPower natively connects to IMS Connect
    - Inbound support only
    - Commit mode 1, Sync Level NONE or Confirm
    - Requirements: Commit mode 0 (commit, then send)



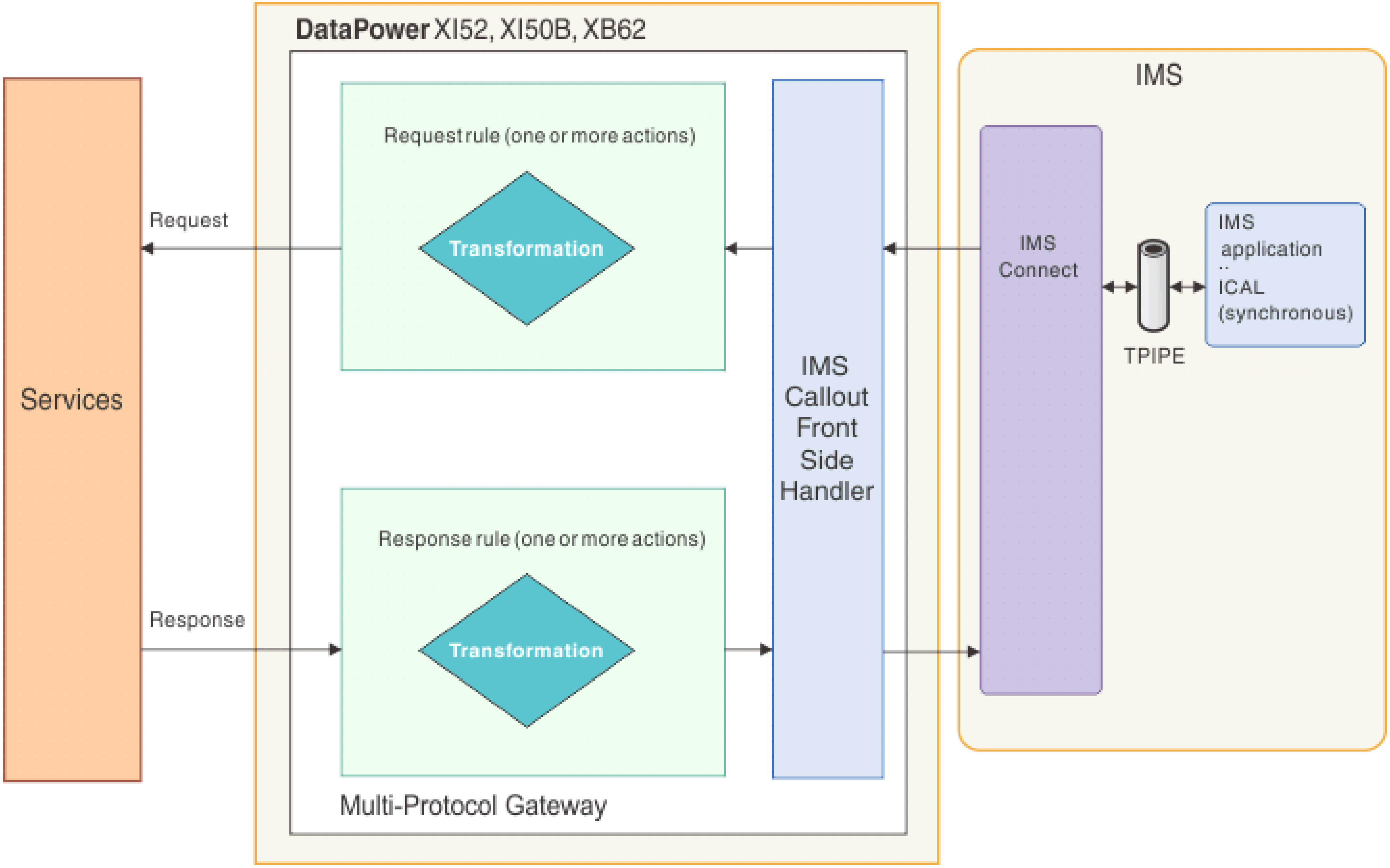
IMS Synchronous Callout with DataPower 6.0+

- ❖ IMS synchronously go outbound to external servers via DataPower
  - ❖ Implement IMS RESUME TPIPE and SEND-ONLY w/ACK protocols
  - ❖ Use WTX Design Studio tooling, XSLT, Gateway JavaScript for data transformation
  - ❖ Use a dedicated IMS Connect user message exit, HWSDPWR1
  - ❖ Socket listening redesign to detect & terminate stale socket connection
- ❖ Requirements on enhanced security & scalability



Documentation: DataPower IMS Implementation Guide: http://www-01.ibm.com/support/docview.wss?uid=swg27038927&aid=1

Data Power Configuration in supporting IMS Callout


Services
Request
Response
DataPower XI52, XI50B, XB62
Request rule (one or more actions)
Transformation
Response rule (one or more actions)
Transformation
IMS Callout Front Side Handler
Multi-Protocol Gateway
IMS
IMS Connect
TPIPE
IMS application
ICAL (synchronous)

Synchronous Callout Solution Highlights

- The IMS callout connection is a DataPower “Front Side Handler” that can retrieve IMS callout messages and send response data.
- The handler internally creates one or more IMS Connect dedicated persistent socket connections to the host system, using Enterprise Suite V2.2 IMS Connect API in Java.
- The handler communicates with IMS Connect via a new DataPower dedicated user message exit, HWSDPWR1.
- For shared queue environment, user can choose to create multiple IMS Callout connections, one for each IMS datastore.

Operational Considerations

- Operational Characteristics
  - DataPower administrator can configure an IMS Callout front side handler with the following properties: IMSHost, IMSPort, DataStoreName, TPipe(s), UserID, Password, Group, RetryErrorLimit, RetryInterval, Connection Timeout
  - DataPower administrator can enable/disable an IMS Callout front side handler
  - **IMS Callout Message Header**

    DataPower V6+: IMS Callout Front side handler sets the two headers in the request to DataPower:

    ims-callout-service-id: IMS ICAL AIBMAPNM field
    ims-callout-correlation-token: Hex representation of ICAL correlation token

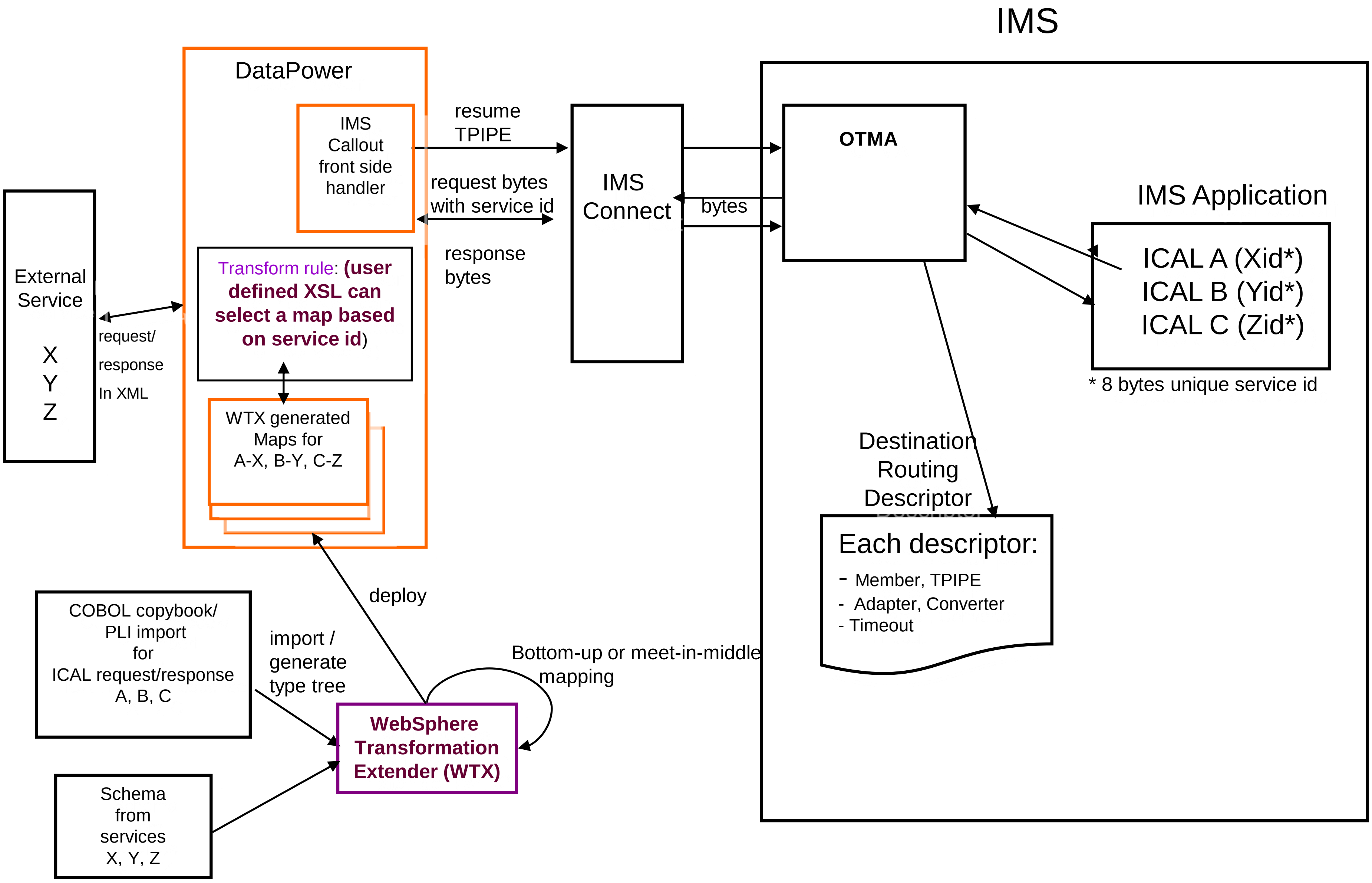
    DataPower administrator can define the XSL in the transform policy to access the header fields in the MPG policy

    - **service ID** as the request identifier to select input/output transformation map; and direct callout messages to goto different routing URLs
    - **correlation token** as the message ID in the outbound HTTP/SOAP request.

    DataPower V6+: IMS Callout Front side handler sets the third header in the request to DataPower:

    - **user ID** to be extracted to create security token, e.g. SAML token

IMS Synchrouns Callout - DataPower Solution Highlights


IMS
DataPower
IMS Callout front side handler
resume TPIPE
request bytes with service id
response bytes
IMS Connect
bytes
OTMA
IMS Application
ICAL A (Xid*)
ICAL B (Yid*)
ICAL C (Zid*)
* 8 bytes unique service id
External Service
X
Y
Z
request/
response
In XML
Transform rule: (user defined XSL can select a map based on service id)
WTX generated Maps for A-X, B-Y, C-Z
Destination Routing Descriptor
Each descriptor:
- Member, TPIPE
- Adapter, Converter
- Timeout
deploy
COBOL copybook/ PLI import for ICAL request/response A, B, C
import / generate type tree
Bottom-up or meet-in-middle mapping
WebSphere Transformation Extender (WTX)
Schema from services X, Y, Z

One copybook has 3 “01” elements -→ 3 maps can be generated..
A service id is used to select one map and also direct the callout msg to different routing URLs, et

DataPower and Data Transformation

- A Transform Action transforms a message from one format to another format
  - For example: from COBOL byte arrays of the copybook of an IMS application program to XML schema used by external service provider
- The Transform Action requires either a WTX map artifact or a stylesheet that maps the data between the two formats.
  - A stylesheet* or JavaScript* can also be used to select between multiple WTX maps.

A Sample Stylesheet

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:dp="http://www.datapower.com/extensions"
extension-element-prefixes="dp">

<xsl:template match='/'>

<xsl:variable name="be"
select="dp:request-header('ims-callout-service-id')"/>

<xsl:choose>

<xsl:when test="$be = 'SERVICE1'">
<dp:set-variable name="'var://context/map/name'"
value="'local://request-250-cp037.dpa'" />
<dp:set-variable name="'var://service/routing-url'"
value="'http:// 192.0.2.0:6221'" />
</xsl:when>

<xsl:when test="$be = 'SERVICE2'">
<dp:set-variable name="'var://context/map/name'"
value="'local://request-8000-cp037.dpa'" />
<dp:set-variable name="'var://service/routing-url'"
value="'http:// 192.0.2.0:6222'" />
</xsl:when>
```

A Sample Stylesheet …

```
<xsl:otherwise>
<dp:reject>unknown backend specified</dp:reject>
</xsl:otherwise>

</xsl:choose>

<xsl:message dp:priority="error">
Correlation token : <xsl:value-of
select="dp:request-header('ims-callout-correlation-token')"/>
</xsl:message>

<xsl:message dp:priority="error">
Service ID : <xsl:value-of
select="dp:request-header('ims-callout-service-id')"/>
</xsl:message>

<xsl:message dp:priority="error">
User ID : <xsl:value-of
select="dp:request-header('ims-callout-user-id')"/>
</xsl:message>

</xsl:template>
</xsl:stylesheet>
```

Write correlation token to the log

Write service ID to the log

Write user ID to the log

DataPower V7.0: GatewayScript™

JavaScript-based gateway runtime which simplifies configuration for developers and provides an easier development paradigm for Mobile, Web, & API

- GatewayScript is a JavaScript-based runtime for processing Mobile, Web, and API workloads
  - Focuses on the “Developer” experience, with familiar and friendly constructs and APIs
  - Why JavaScript?
    - Popular scripting language, large ecosystem, fast moving community driven, used on both client-side and server-side and now Gateway too
  - Performance
    - Compiler technology & native execution
    - Ahead of time compilation with caching, not single threaded
    - Built on intellectual capital and expertise from 10+ years securing and optimizing XSLT parsing/compiler technology
  - Security
    - Transaction isolation
    - Code injection protection
    - Short lived execution
    - Small footprint

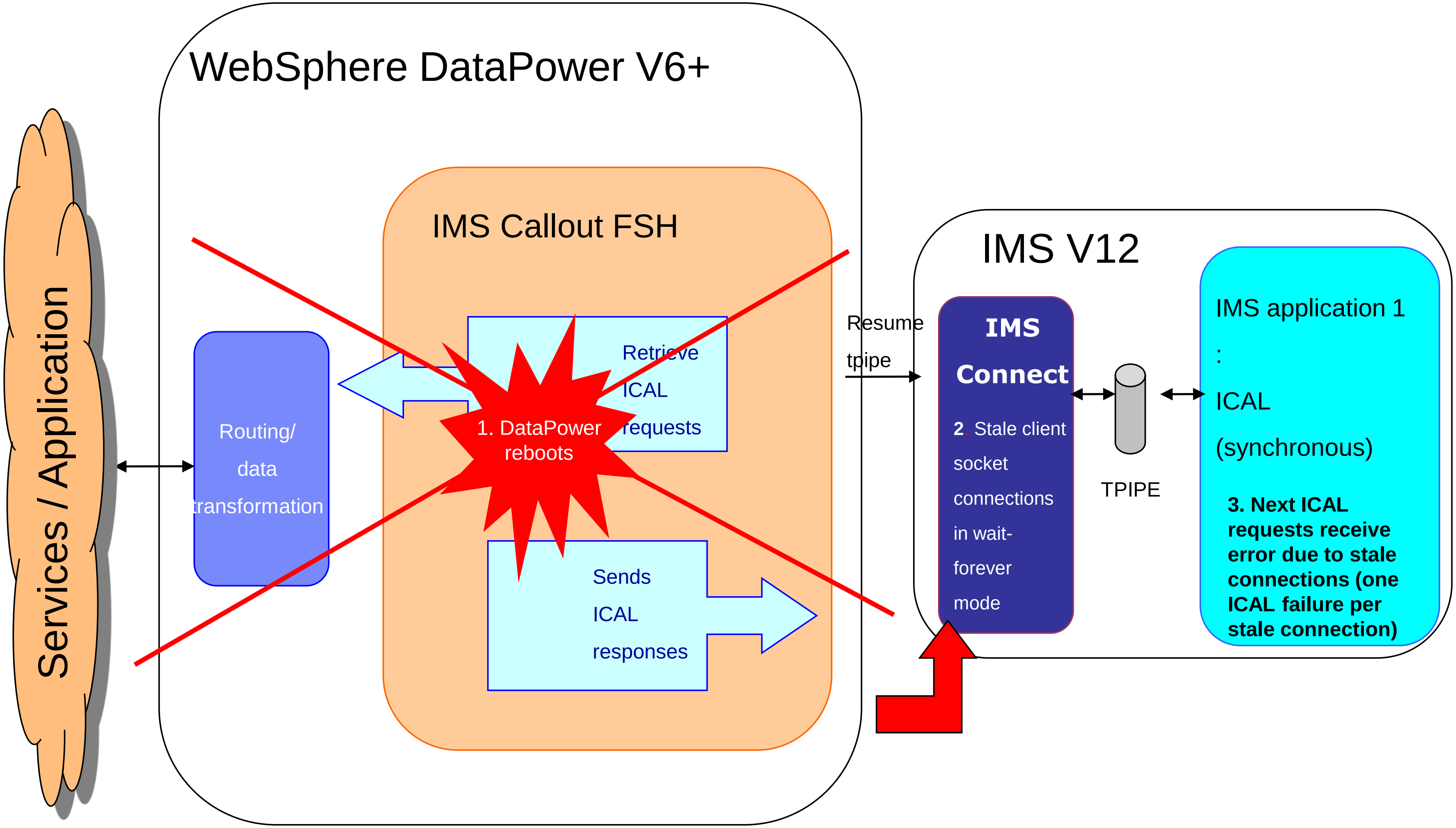
Prerequisites for IMS synchronous callout

- Software requirements
  - IMS V12 (IMS V13 is recommended)
    - – IMS Connect
    - – OTMA
  - DataPower Firmware 6.0.0.0 or higher
- Hardware requirements
  - WebSphere DataPower V6.0+ (XI52, XB62)
  - IBM DataPower Gateway
- Tooling
  - WebSphere Transformation Extender (WTX)
    Provides mapping between different data formats.
    - WTX maps can be built as deployable artifact for DataPower, providing data transformation between IMS callout bytes and XML data for web services.
    - A WTX map can be set using a DataPower-specified variable, then called within XSL code in a DataPower policy; or use GatewayScript

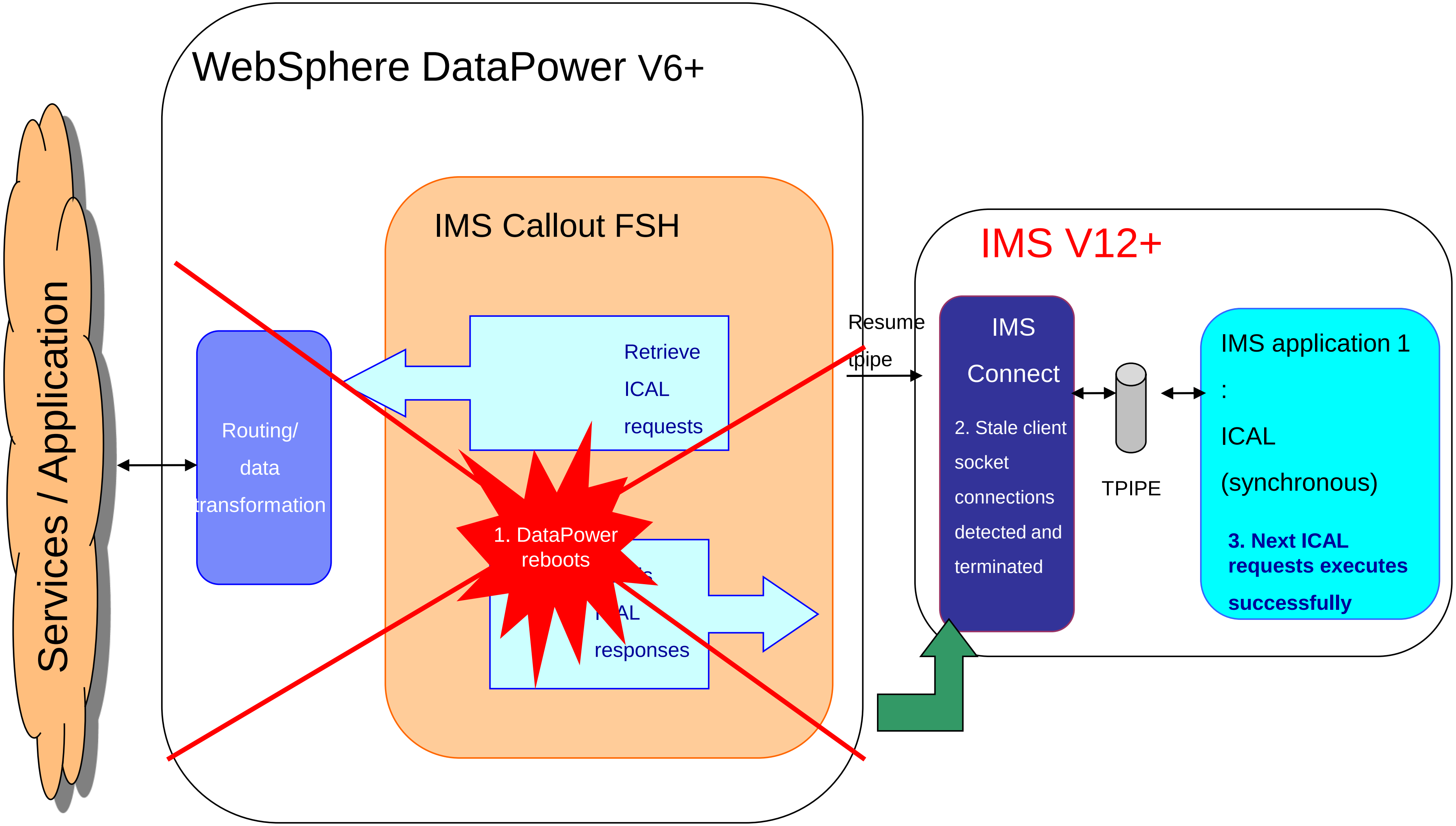
IMS Synchronous Callout DataPower & IMS Versions

- **IMS V12**
  - **IMS Connect**
    - DataPower User Exit Installation - Object Code Only user exit HWSDPWR1 (new)
      Specified in the EXIT= parameter of the TCP/IP statement in the IMS Connect configuration file (HWSCFGxx).
      - V13 PTF UK97704 & PTF UK97704
      - V12 PTF UK91544
  - **OTMA**
    - IMS Synch Callout user can specify a 1-to-8 byte mapname as the first 8 bytes in AIBUTKN so that this ID can be included in the OTMA state data in the callout message. The ID can be used as a unique service identifier for data transformation mapping and service routing
      - V13 (available as base code)
      - V12 PTF UK82636 (PM73135) AIB MAP name field
- **IMS V13 & V12**
  - **IMS Connect**: Socket listening redesign
    - V13 PTF UK95578 & PTF UK97704

IMS Connect V12 Requires Manual Cleanup on DataPower Failure/Restart



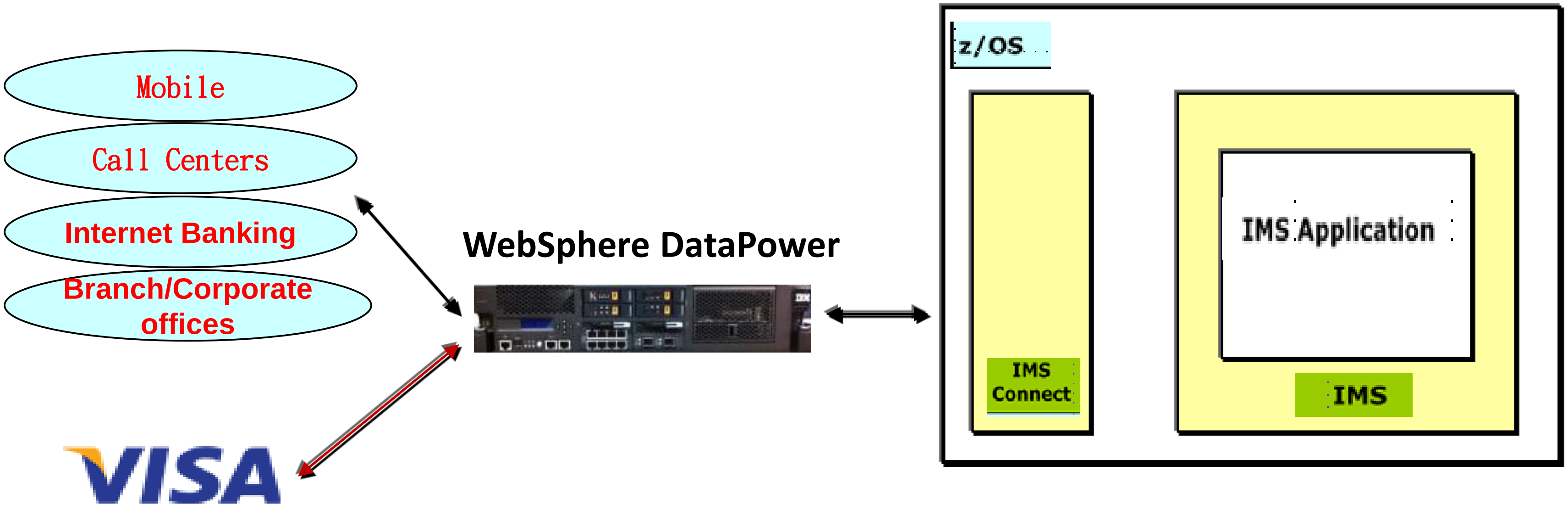
IMS Connect V12+ Socket Listening Redesign Function



Services / Application
WebSphere DataPower V6+
IMS Callout FSH
Routing/ data transformation
Retrieve ICAL requests
AL
responses
1. DataPower reboots
Resume tpipe
IMS V12+
IMS Connect
2. Stale client socket connections detected and terminated
TPIPE
IMS application 1 : ICAL (synchronous)
3. Next ICAL requests executes successfully

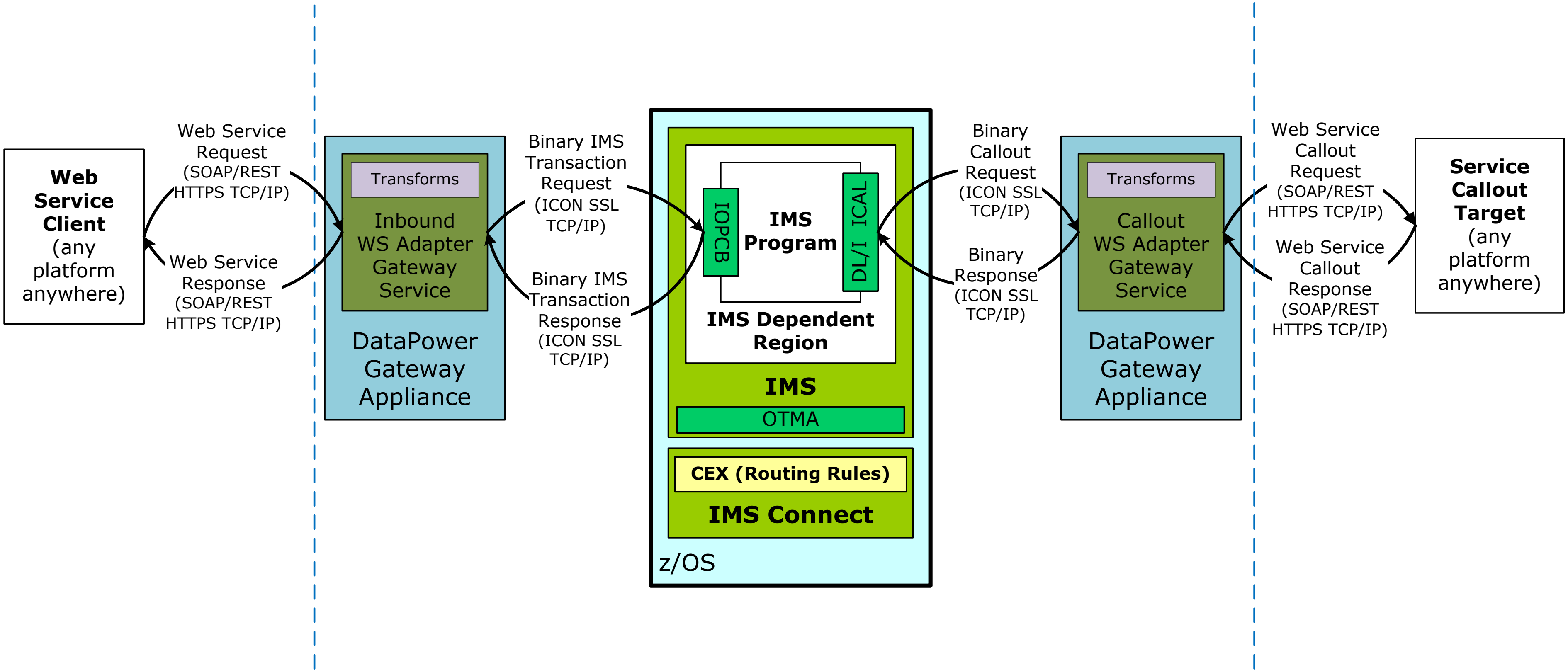
IMS & DataPower @Work

- A Banking system supports multiple solution delivery channels, e.g. Internet Banking, Mobile, Call Centers, Branch & Corporate offices, etc. for account balance, and fund transfer with Visa International
- In production in 2014



DataPower based WS Adapter Example:

z/OS IMS Application Programs as “First Class SOA Components”



Web Service Client (any platform anywhere)
Web Service Request (SOAP/REST HTTPS TCP/IP)
Web Service Response (SOAP/REST HTTPS TCP/IP)
Transforms
Inbound WS Adapter Gateway Service
DataPower Gateway Appliance
Binary IMS Transaction Request (ICON SSL TCP/IP)
Binary IMS Transaction Response (ICON SSL TCP/IP)
IOPCB
IMS Program
DL/I ICAL
IMS Dependent Region
IMS
OTMA
CEX (Routing Rules)
IMS Connect
z/OS
Binary Callout Request (ICON SSL TCP/IP)
Binary Response (ICON SSL TCP/IP)
Transforms
Callout WS Adapter Gateway Service
DataPower Gateway Appliance
Web Service Callout Request (SOAP/REST HTTPS TCP/IP)
Web Service Callout Response (SOAP/REST HTTPS TCP/IP)
Service Callout Target (any platform anywhere)

Thank You