IBM DataPower Gateway Overview & What’s New in V7.5

Stefano Tosato, Offering Manager, Gateways

Aug 1, 2016
Agenda

- DataPower Gateway Overview
- Recent Releases
- What’s New in DataPower Gateway V7.5
IBM DataPower Gateways provide a low startup cost, helping clients increase ROI and reduce TCO with specialized, consumable, dedicated gateways that combine superior performance and hardened security in physical, virtual, cloud & Docker container form factors.
Secure, control & accelerate Digital workloads

**Mobile**
Simplify mobile security with single, purpose-built gateway; control mobile traffic and accelerate delivery

**SOA**
Secure, integrate, control & manage SOA workloads in the DMZ and Trusted zones

**API**
Easily secure, control, publish, monitor & manage your APIs

**Cloud**
Deploy in multiple hypervisor, cloud environments and enable hybrid & inter cloud connectivity

**Web**
Simplify web security with single, purpose-built gateway; control traffic and accelerate delivery for intranet and internet web applications

**B2B**
Extend Connectivity & Integration beyond the enterprise with DMZ-ready B2B edge capabilities
IBM DataPower Gateways are the industry-leading Security & Integration gateways that help provide security, integration, control and optimized access to a full range of Mobile, Web, API, SOA, B2B, & Cloud workloads.

1. API Gateway
2. Mobile Gateway
3. Web Gateway
4. B2B Partner Gateway
5. API & SOA Gateway
6. ESB / Integration Gateway
7. Internal Security Enforcement
8. Legacy Integration
**Single, modular & extensible Gateway platform**

### B2B Module
- B2B DMZ gateway
- EDIINT AS1, AS2, AS3, ebXML
- Partner profile management
- B2B transaction viewer
- Any-to-Any message transformation
- Database connectivity

### ISAM Proxy Module
- User access control, session management, web SSO enforcement
- Advanced mobile security: mobile SSO, context-based access, one-time password, multi-factor authn

### Application Optimization Module
- Frontend self-balancing
- Backend intelligent load distribution
- Session affinity
- z Sysplex Distributor integration

### Integration Module
- Any-to-Any message transformation
- Database connectivity
- Mainframe IMS connectivity

### TIBCO EMS Module
- Integrate with TIBCO EMS messaging middleware
- Support for queues & topics
- Load balancing & fault-tolerance

### IBM DataPower Gateway (Base)

#### Secure
- Authentication, authorization
- Security token translation
- Service / API virtualization
- Threat protection
- Message schema validation
- Message filtering
- Message digital signature
- Message encryption
- AV scanning integration

#### Integrate
- Transport protocol bridging
- Any-to-any message transformation
- Message enrichment
- Database connectivity
- Mainframe connectivity
- B2B partner connectivity
- Hybrid cloud connectivity

#### Control & Manage
- Quota & rate enforcement
- Content-based routing
- Message accounting
- B2B partner management
- Integration w/ governance, management & monitoring platforms including IBM API Connect & WSRR for policy enforcement

#### Optimize & Offload
- HTTP/2
- SSL / TLS offload
- Hardware accelerated crypto*
- JSON, XML offload
- JavaScript, JSONiq, XSLT, XQuery acceleration
- Local response caching
- Distributed caching with WX5
- Backend load balancing
Available Form Factors

Physical, Virtual, Cloud & Docker

- ISAM Proxy Module
- Integration Module
- B2B Module
- AO Module
- TIBCO EMS Module

All software modules are field upgradeable
Available Form Factors: Deploy Anywhere

### Physical
- **Gateway Image**
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Embedded OS
- **Hardware**
  - Trusted Platform Module
  - Hardware Security Module
- **Crypto Acceleration**

**All in one solution (HW / SW)**
- Physical security
- Drop-in deployment & mgmt
- Performance including HW crypto acceleration
- DMZ drop-in
- Embedded HSM option (FIPS 140-2 certified)

### Virtual**
- **Gateway Image**
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Embedded OS
- **Hypervisor**
  - Hardware
- **Software solution** (Virtual machine)
  - User responsible for providing & securing HW and Hypervisor
  - Flexible deployment
  - Flexible resource allocations
  - Prod, non-prod, dev editions

### Cloud**
- **Gateway Image**
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Application Layer
- **Operating System**
  - Cloud Virtual Server
- **Hypervisor**
  - Hardware
- **Software solution** (Application)
  - Cloud vendor responsible for securing HW and Hypervisor
  - User responsible for securing OS
  - Public Cloud deployments
  - Rapid scale up/down
  - First class Cloud citizen

### Docker**
- **Gateway Image**
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Application Layer
- **Docker Container**
- **Docker Engine**
- **Hypervisor / OS**
- **Hardware**

**Software solution (Container)**
- User responsible for providing & securing HW, Docker Host OS or hypervisor
- Docker optimized image
- Apply your DevOps tools & processes
- Provides ability to optionally store DP config externally in Docker Host filesystem

**1** Supported on VMware & Citrix XenServer hypervisors.
**2** Supported via RHEL & Ubuntu on Amazon EC2, Microsoft Azure, IBM SoftLayer.
**3** Supported on Docker Container based on RHEL & Ubuntu.
**4** Docker Image built using IBM provided packages.

"Once deployed, it’s DataPower Gateway"
Virtual Edition Benefits

- Seamless configuration migration
  - Easily move configuration between form factors

- Deployment flexibility and elasticity
  - “Right size” the deployment, quickly deploy where needed & rapidly scale

- Workload isolation
  - Projects can use their own instances

- Unbounded memory scalability
  - Memory can be added to instances without additional licensing

- Low cost for Dev & Test environments
  - Developers & Non-Production versions include add-on software modules at no additional charge

- Free disaster recovery
  - Warm or cold backup without additional licenses when licensed for Production

- Flexible licensing and entitlement
  - Sub-capacity licensing
  - Monthly licensing option
  - Entitlement to future product versions at no additional charge with active maintenance (S&S)
Non-blocking event-driven I/O architecture

- Architecture similar to Nginx & Node.js
- Continued enhancements since 2002

 Parses & compilers for JSON & XML processing written from ground-up with several patents

Secure and optimized JavaScript runtime called GatewayScript

Purpose-built, secure gateway image

- Single self-contained, signed & encrypted secure gateway image without external software dependencies
  - No arbitrary software
  - Security exposure minimized due to smaller vulnerability surface (few user-exposed and 3rd party components)
- High assurance, “locked-down” configuration
- Optimized, embedded operation system

Physical security via hardware

- Sealed, tamper-evident case
- No usable USB, VGA, other ports
- Customized intrusion detection switch
- Trusted Platform Module
- Encrypted flash drive
- Cryptographic acceleration card
- Optional FIPS 140-2 level 3 certified Hardware Security Module

Enterprise grade security requires a secure platform
Simple & Secure Architecture

- How is DataPower Gateway different? **Purpose-built, secure** gateway platform
  - Complete gateway platform delivered as hardened image
- Guiding philosophy is to centralize common security, traffic management, mediation, acceleration functions and optimize them in a security-hardened gateway stack delivered in physical, virtual, cloud & Docker container form factors

### DataPower Gateways
**Secure & Easy to Manage**

- DataPower Gateway Platform
  - Digitally Signed and Encrypted Image
- IBM Optimized Embedded Operating Environment
- Crypto Acceleration
- Flash Memory
- Hardware

### Commodity Gateways
**In-Secure & Hard to Manage**

- Proprietary Software
- JVM
- HTTP Server
- App Server
- Database
- libxml
- glibc
- JSP Engine
- Linux Daemons
- Full Linux OS (including shells and user accounts)
- Display Ports
- Bootable CDROM Drive
- Bootable USB Ports
- Hardware
GatewayScript™: Secure & optimized JavaScript runtime

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

- Security
  - Transaction isolation to prevent memory-based attacks
  - Code injection protection to prevent security exposures from malicious code

- Performance
  - Highly optimized JavaScript compiler
  - Built on intellectual capital and expertise from 10+ years securing and optimizing parsing/compiler technology
DataPower Gateways ....

Developer, Enterprise & DevOps Friendly

API, Mobile, Cloud, B2B
Built-in security, traffic mgmt, mediation, acceleration

Deploy Anywhere

Flexible & Extensible

Purpose-built, Secure Gateway

Operations Dashboard

JavaScript

Flexible & Extensible

DataPower Gateways
DataPower Gateways

*Over 15 years of innovation & 2000 global installations*

**Government**
- Agencies and ministries
- Defense and security organizations
- Crown corporations

**Banking**
- Majority of the big US and European banks
- All of the big 5 Canadian banks
- Numerous regional banks and credit unions

**Insurance**
- Used by 95% of top global insurance firms
- SaaS providers, ASPs, regulators, etc.

**Many, many, more**
- Healthcare
- Retailers
- Utilities, Power, Oil and Gas
- Telecom
- Airlines
- Others
**DataPower** has been trusted to be the exclusive **gateway** for **Bluemix**, IBM’s global Platform as a Service

---

**DataPower’ing** IBM Bluemix!!!

- Security
- Control
- Filtering
- Content-Based Routing
- Load balancing
- Monitoring and Logging
DataPower Gateway V7.5.1: Supported standards & protocols

- **Data format & language**
  - JavaScript
  - JSON
  - JSON Schema
  - 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, JSONiq

- **Security policy enforcement**
  - OAuth 2.0, OpenID Connect, Social Login
  - JWE, JWS, JWT, JWK
  - SAML 1.0/1.1/2.0, SAML Tkn Profile, SAML queries
  - XACML 2.0
  - Kerberos (including S4U2Self, S4U2Proxy)
  - SPNEGO
  - RADIUS, RSA SecurID OTP using RADIUS
  - LDAP versions 2 and 3
  - Lightweight Third-Party Authentication
  - 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, HTTP/2, HTTPS, WebSocket Proxy
  - FTP, FTPS, SFTP
  - WebSphere MQ
  - WebSphere MQ File Transfer Edition
  - TIBCO EMS
  - WebSphere Java Message Service
  - IBM IMS Connect, & IMS Callout
  - NFS
  - AS1, AS2, AS3, ebMS 2.0, CPPA 2.0, POP, SMTP (B2B Module)
  - DB2, Microsoft SQL Server, Oracle, Sybase, IMS

- **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
  - SYSLOG
  - IPv4, IPv6

- **Transport Layer Security**
  - TLS versions 1.0, 1.1, and 1.2
  - SSL versions 2 and 3
  - SNI, PFS, ECC Ciphers

- **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
  - WS-Management
  - WS-I Attachments Profile
  - SOAP Attachment Feature 1.2
  - SOAP with Attachments (SwA)
  - Direct Internet Message Encapsulation
  - Multipurpose Internet Mail Extensions
  - XML-binary Optimized Packaging (XOP)
  - Message Transmission Optimization Mechanism (MTOM)
  - WS-Mediation Policy (IBM standard)
  - Universal Description, Discovery, and Integration (UDDI versions 2 and 3), UDDI version 3 subscription
  - WebSphere Service Registry and Repository (WSRR)

[Link to Product Documentation]
See slide deck for Common Use Cases:
slideshare.net/ibmdatapower/data-power-common-use-cases
Agenda

- DataPower Gateway Overview
- Recent Releases
- What’s New in DataPower Gateway V7.5

### New Cloud Offerings
Deploy DataPower Gateways on **Amazon EC2**, **Microsoft Azure** and **SoftLayer CCI** to provide enhanced cloud elasticity for cloud workloads.

### Secure Gateway for Bluemix
Enhanced **hybrid cloud integration** to securely connect between **IBM Bluemix** applications and on-premise services protected using DataPower Gateways.

### Robust Platform Security
Protect mission-critical applications from security vulnerabilities with **enhanced TLS protocol** support using **Elliptic Curve Cryptography**, **Server Name Indication**, and **Perfect Forward Secrecy**.

### Enhanced Mobile and API security
Increased **mobile** and **API security** for protecting mission-critical transactions with **JSON Encryption**, **JSON Signature**, **JSON Key**, and **JSON Token**.

### GatewayScript Enhancements
Easily **transform between XML and JSON** messages to quickly integrate System of Records data sources with Systems of Engagement interfaces.

### Easier DevOps with new REST API
New **REST-based management API** to build deployment and automation scripts, enabling easier **devops** for continuous software delivery and quicker problem resolution.

**Released Jun 2015**
Agenda

- DataPower Gateway Overview
- Recent Releases
- What’s New in DataPower Gateway V7.5
New Cloud Offerings

Run DataPower as an **Red Hat Enterprise Linux (RHEL)** application on **cloud platforms** (Amazon/SoftLayer) for easier management using cloud management tools.

Deployment Flexibility using Docker

Deploy DataPower as a **Docker container** for enhanced portability, scalability and environment provisioning.

Network HSM Integration

Integrate with Gemalto (formerly Safenet) network HSM to provide secure key management and offload of crypto operations in cloud and virtual environments.

Built-in Policies on IBM API Connect

New API gateway policies for IBM API CONNECT to enable quick delivery of gateway capabilities without any custom policy authoring or coding.

Enhanced API Security

Flexible user authentication for Single Sign-On (SSO) to Web, mobile and API workloads using social (eg. Google) or enterprise identities based on OpenID Connect.

New Modernized User Experience

Modernized user experience to reduce complexity and allow quicker creation of gateway services.
DataPower V7.5 Offering Details (1 of 2)

- Run DataPower Gateways on cloud platforms (Amazon/SoftLayer) using Red Hat Enterprise Linux (RHEL) virtual server for increased deployment flexibility and security through implementation of RHEL best practices.
- Use DataPower Gateways on Microsoft Azure to secure and integrate services deployed on Azure Cloud.
- Deploy DataPower secure image in a Docker container for increased portability on bare-metal, virtual and cloud platforms, allowing DataPower to run on any Docker supported environment.
- Enhanced virtual and cloud platform security using Gemalto (formerly Safenet) network HSM (Certified FIPS 140-2 Level 3) to provide secure key management and offload of crypto operations.
- New modernized user experience to reduce complexity and allow quicker creation of gateways.
- Easily deploy gateway accelerators using Blueprints console and seamlessly customize to meet enterprise requirements.
DataPower V7.5 Offering Details (2 of 2)

- **Flexible user authentication** for Single Sign-On (SSO) to Web, mobile and API workloads using social (eg. Google) or enterprise identities based on OpenID connect.

- Out of the box API gateway policies for IBM API management to enable quick delivery of gateway capabilities without any custom policy authoring or coding.

- Use DataPower Gateways to enforce mobile and API security policies using **CA SSO** (formerly Siteminder) for increased security interoperability

- **Simplified packaging of ISAM module for DataPower** with entitlement to IBM Security Access Manager V9 virtual edition

- Enhanced mobile security to protect access to Mobile and API services managed from IBM MobileFirst Platform, enabling quicker time-to-market of mobile applications
Cloud
Deploy anywhere using Docker containers

- Perform regular Docker tasks (build, pull, and run) on any Docker supported hosts
- Pull DataPower images from Docker private registries
- Higher density to run multiple concurrent DataPower instances on a single machine
Quickly provision environments using DataPower Docker image

Private Registry

Docker Images

Multiple Containers for HA

Dev

Test

Prod

IBM DataPower Gateways

Containers

Containers

Containers
Quickly build and test gateway capabilities with shared volumes

- Map shared volume from host file system to Docker container to enable local development
  - Mapped to DataPower file system - local: and config: directories
- Enhanced development experience to quickly build and test changes
DataPower Cloud Gateway in public cloud platforms

- DataPower Gateways provide security and integration capabilities to protect and optimize cloud workloads on SoftLayer, **Microsoft Azure (new)**, and Amazon EC2 platforms.
- Deployed within the public cloud virtual server environment using either **Red Hat Enterprise Linux (new)** or Ubuntu.
Integration with SafeNet Network HSM

• **Current** - DataPower Gateways provide an embedded HSM for offload of secure crypto operations for enhanced security that is FIPS 140-2 Level 3 certified

• **New** – DataPower Gateways integrate with Gemalto (formerly SafeNet) **network** HSM to provide secure key management and offload of crypto operations in cloud and virtual environments.

• Enables secure key management and crypto offload in virtual and cloud environments

• The SafeNet Network HSM stores the keys and performs the cryptographic operations in the HSM partitions.
  – Cryptographic requests are sent over a network trust link (NTL).
Use DataPower Gateways to enable Hybrid cloud integration

Enhanced portability and scalability on public cloud platforms
API
What is API Connect?
An integrated creation, runtime, management, and security foundation for enterprise grade API’s and Microservices to power modern digital applications.

What does API Connect provide?
• Automated, visual and coding options for creating APIs
• Automated discovery of system of records APIs
• Node.js and Java support for creating Microservices
• Integrated enterprise grade clustering, management and security for Node.js and Java
• Lifecycle and governance for APIs, Products and Plans
• Access control over API’s, API Plans and API Products
• Advanced API usage analytics
• Customizable, self service developer portal for publishing APIs
• Policy enforcement, security and control
IBM API Connect: Capabilities Delivered

- Rapid model-driven API creation
- Datasource to API mapping automation
- Standards-based visual API spec creation in Swagger 2.0
- Local API creation and testing
- On-cloud & on-premises staging of APIs, Plans & Products

- Policy enforcement
- Enterprise security
- Quota management & rate limiting
- Content-based routing
- Response caching, load-balancing and offload processing
- Message format & transport protocol mediation

- Node.js & Java Microservice runtime
- Node.js & Java integrated runtime management
- Enterprise HA & scaling
- On-cloud & on-premises staging of Microservice applications

- API discovery
- API, Plan & Product policy creation
- API, Plan & Product lifecycle mgmt.
- Self-service, customizable, developer portal
- Advanced Analytics
- Subscription & community mgmt.
IBM API Connect: Additional built-in policies

- Built-in policies for IBM API Connect that are enforced on DataPower Gateway to quickly secure, control and optimize access to API services.
Mobile & Advanced Security
**DataPower Gateway**
High performance gateway to secure multi-channel traffic across mobile, IoT, cloud, web, B2B, SOA and APIs

**MobileFirst Platform Foundation**
Essential mobile backend services pre-integrated with advanced safeguards, management and analytics

**API Connect**
Create, Run, Manage & Secure new or existing APIs and Microservices in a hybrid deployment with Node.js and Java to power modern digital applications

Use one or all of these components together based on project needs
Integrating with IBM MobileFirst Platform

Secure & control Mobile apps

- Enforce security policies from IBM MobileFirst Platform using DataPower Gateways
- IBM MobileFirst Platform provides policy authoring & decision point (e.g., approved/rejected) with DataPower Gateways as the enforcement point

Diagram:
- Mobile devices
- Gateway connecting to IBM DataPower Gateways
- System of Record with components like MQ, IMS, CICS, DB2, z/OS Connect
  - P1: Application Authentication
  - P2: Step-up Authentication
  - A1: REST Adapter
  - A2: SOAP Adapter

API Policy = MFP (P1, P2)

MyAPI (Policy=MFP)
- GET A1
- POST A2
Integration with IBM Security Access Manager

Enforce “context-aware” API security to protect against fraud and security exposures
Recent API & Mobile security enhancements

- **OpenID Connect**: Flexible user authentication for Single Sign-On (SSO) to Web, mobile and API workloads using social (eg. Google) and enterprise identities
  - Use social provider to authenticate resource owner in an OAuth flow
  - Provide identity as-a-service for authentication users (OpenID Connect provider)

- **Stronger API security with JWT profile for OAuth** for protecting access to API resources

- **Enhanced interoperability across enterprise security products with JWT support in DataPower security framework (AAA)**

- **Dynamic security policy** support for enhanced authoring flexibility of user authentication, authorization and token management policies
Other enhancements

• Secure Backup/Restore scrypt between DataPower virtual editions
• Elliptical Curve Cryptography (ECC) enhancements in GatewayScript APIs and TLS protocols
• GatewayScript upgrade to ECMAScript 6.0 (Block scoping, promises, template strings, and more)
• Access control using IBM Security Access Manager (V8/V9) federated directories
UX
DataPower UX modernization

Modernized look and feel with updated theme and simplified navigation experience
Simplified navigation experience

List frequent tasks and search bar to find any tasks or configuration objects
Known as the ‘bible’ of DataPower planning, implementation, and usage.

New content to cover new products/features, including 9006/7.2!

**Volume 1** consists of *DataPower Intro, Setup Guide, Common Use Cases, Deployment Checklist*, new *Preface* and three invaluable new appendices for physical and virtual gateways.

**Volume II** is an in-depth coverage of DataPower networking topics, including VLAN, link aggregation, high availability.

**Volume III** is an in-depth coverage of DataPower development, including XSLT, EXSLT, JavaScript/GatewayScript, JSON, JSONiq, XQuery, binary/secondary data formats, and development tools.

**Volume IV** covers DataPower B2B processing and file transfer, including relevance of B2B in today’s API driven world.
Where can I learn more about IBM DataPower Gateway?

• Overview Video
  – youtube.com/watch?v=RqT3f_TmSMM
• Product Page
• Product Documentation
  – ibm.com/support/knowledgecenter/SS9H2Y
• Videos
  – youtube.com/channel/UCV2_gdea5LM58S-E3Wcqw
• Slide Decks
  – http://slideshare.net/ibmdatapower
• GitHub Repository
  – github.com/ibm-datapower/
• Twitter
  – twitter.com/IBMGateways
• LinkedIn
  – Private user group ‘IBM DataPower Gateway’
    – linkedin.com/groups?gid=4820454
• User Forum
  – ibm.biz/dpuserforum
Multi-Channel Gateway for Digital Edge Processing

Improve security & control while reducing cost

IBM DataPower Gateway: physical, virtual or cloud deployment
Policy-driven approach speeds time to market

- Uses **intuitive policy pipeline message processing** to secure, control, optimize, & integrate services and application traffic
- Enforce security standards with **zero coding**
- **Import/export** configurations between environments
- Transaction probe shows message content between actions for debugging
Over a 15+ years of innovation

- Optimal Interpreter and Compiler
- XA35
- XI50
- WebSphere Transformation Extender
- Model 9004
- XB60
- XI52 | XB62
- DataPower Virtual Edition
- DataPower Gateway
- Model 9005
- AO Self-Balancing and Intelligent Load Distribution
- Blade
- XG45
- IT CAM for SOA
- Model 9003
- XS40
- Gigabit/Sec OEM HW Solution
- IBM Acquisition
- DataPower Cloud Edition
- DataPower Docker
- Over a 15+ years of innovation