Global Systems Integrator

Global   Trust   Leadership   Innovation

IBM WEBSPHERE DATAPOWER

MIRACLE MSS
SOFTWARE SYSTEMS, INC.

IBM

Agenda

- ❑   Quick Introduction to Miracle Software Systems

- ❑   What Is DataPower?

- ❑   DataPower Family

- ❑   DataPower as Security and Integration Solution

- ❑   Core Functions

- ❑   DataPower Services

- ❑   Right Fit and Red Flags

- ❑   Q & A

About Miracle Software Systems Inc

- Mid Sized Systems Integrator established in 1995
- Global Delivery Centers across USA,UK, India, Singapore & Australia
- Specialty in SOA Connectivity, B2B & Data Integration
- Major Partnerships with IBM & SAP
- USD 40 Million in revenues & 800 Employees Worldwide
- Financially Stable US Incorporated, Private Minority enterprise

MIRACLE **MSS**
SOFTWARE SYSTEMS, INC.

IBM

DataPower Appliances Overview

The IBM DataPower appliance formula for success

1) Take some characteristics from integration software stacks
- Programmability by developers
- Message level security and routing
- Integration with other SOA infrastructure & governance software
- Conditional Processing & Transformation of any-2-any formats
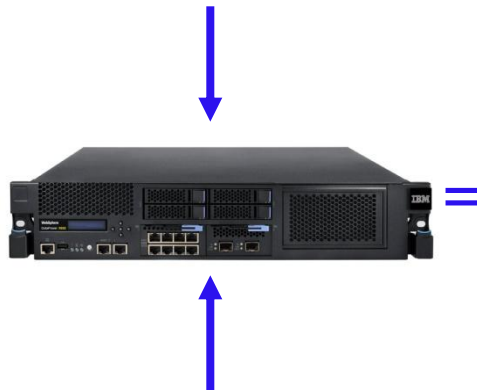
3) Combine them into a firmware-driven hardware device known as an "Appliance" that has the advantages of both software stacks and networking gear. Add to this some unique patented chip-based accelerators and you have a more efficient method for performing integration and security tasks.

2) Take some characteristics of networking & firewall devices
- High throughput
- Many concurrent connections
- IP level security and routing (can't see inside message but route by source and target)
- Simplified Management and reduced maintenance costs through firmware updates

What is IBM WebSphere DataPower?

❑ Purpose-built hardware provides physical security for every device

- ❖ Sealed, tamper-evident case with no external drives
- ❖ Default "locked-down" configuration
- ❖ Verbose audit logs

❑ Purpose-built & patented hardware accelerators in every device provide SLA friendly solutions that software-only solutions can't provide

What is IBM WebSphere DataPower?

- There is no well-known software stack. All the Data Power appliances run a single hardened firmware image that provides all the features
    - Signed and encrypted by IBM
    - Optimized DPOS operating system
    - Runs no arbitrary software or Java
    - Easily upgrade entire appliance in minutes
- Data Power has accreditation as fully DMZ-capable gateway device
    - Common Criteria EAL4
    - FIPS 140-2 Level 2 or Level 3 (with optional HSM device)
    - Drummond Group AS2

WebSphere DataPower Appliance Family

Smarter Business Agility with WebSphere DataPower Appliances

XG45

- Lightweight Gateway (HTTP,FTP,MQ,JMS)
- Any-to-Any conversion at near wire-speed
- Web Services security
- Rich authentication and authorization
- Centralized policy management

XI52

- Consumable full-function hardware based integration capable gateway
- "Any-to-any" conversion at wire-speed
- Dynamic routing; intelligent load distribution
- Rich set of security features
- Web Services security gateway
- Centralized policy management

XB62

- XI52 + B2B performance
- Secure B2B messaging (AS1, AS2, AS3)
- Trading partner profile management
- B2B Transaction Viewer
- Resend B2B transactions in or out

XC10

- Elastic Caching
- 240 GB of Cache
- Support for non-java applications
- Service Response Caching
- Caching across multiple data centers

MIRACLE MSS
SOFTWARE SYSTEMS, INC.

IBM

NEW Members to the WebSphere DataPower Appliance Family

XG45VE

- Lightweight Gateway (HTTP,FTP,MQ,JMS)
- Any-to-Any conversion at near wire-speed
- Web Services security
- Rich authentication and authorization
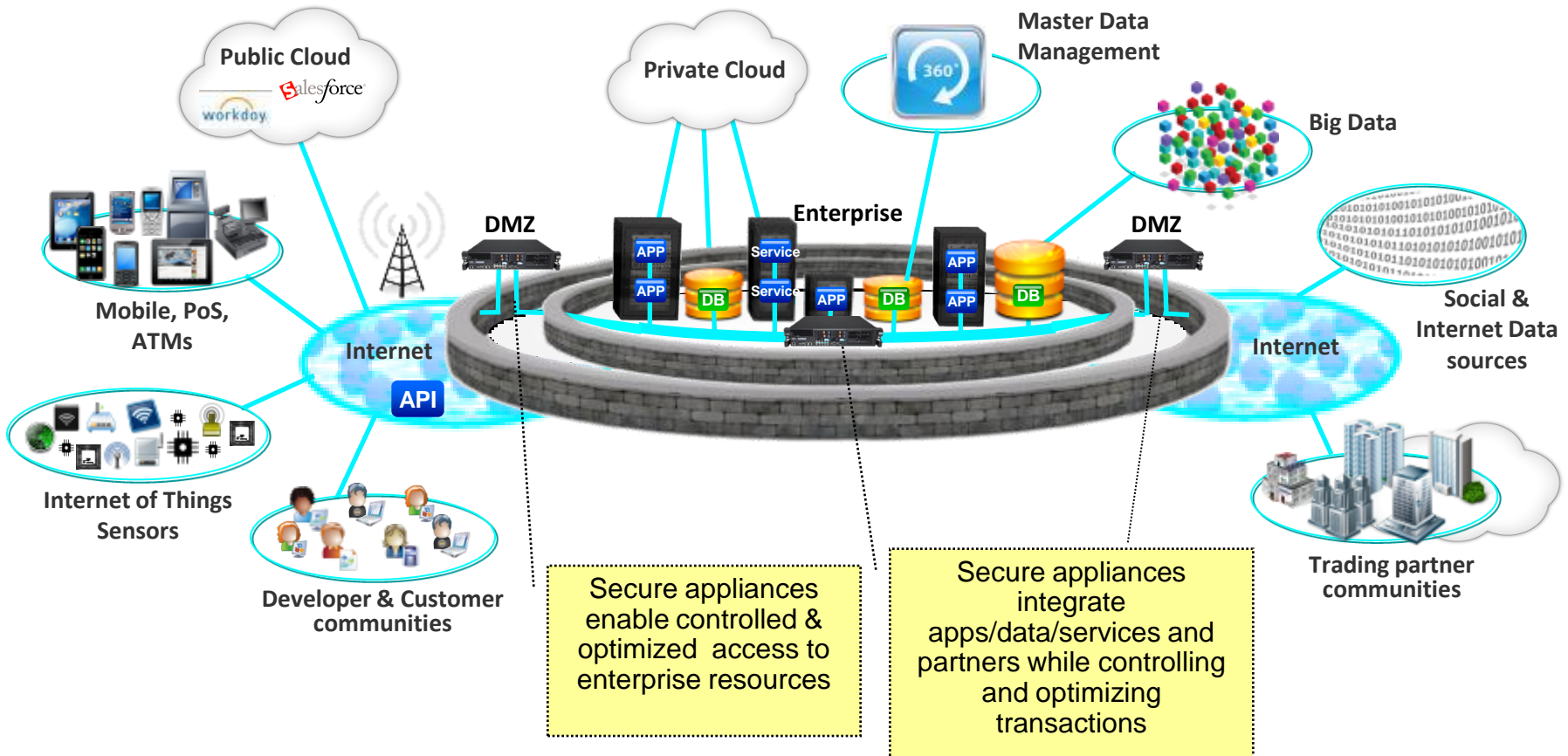- Centralized policy management

XI52VE

- Consumable full-function hardware based integration capable gateway
- "Any-to-any" conversion at wire-speed
- Dynamic routing; intelligent load distribution
- Rich set of security features
- Web Services security gateway
- Centralized policy management

- WebSphere DataPower XG45 and XI52 physical appliance functionality in a "virtual appliance" form-factor running on VMware hypervisor.
- Delivered as an Open Virtualization Archive (OVA) package targeted for VMware ESX or EXSi.
- Each "virtual appliance" is powered by the same purpose-built platform as the physical appliance model, and includes an embedded, optimized DataPower Operating System.
- Uses signed/encrypted firmware images like physical appliances, doesn't allow install of other software.
- Minimum configuration for each appliance is - 4 vCPU (i.e. virtual core) and 4GB RAM.

IBM Data Power's value as a Security & Integration Gateway

Public Cloud

Private Cloud

Master Data Management

Big Data

DMZ

Enterprise

DMZ

Mobile, PoS, ATMs

Internet

API

Social & Internet Data sources

Internet of Things Sensors

Internet

Developer & Customer communities

Trading partner communities

Secure appliances enable controlled & optimized access to enterprise resources

Secure appliances integrate apps/data/services and partners while controlling and optimizing transactions

Datapower Typical - Infrastructure
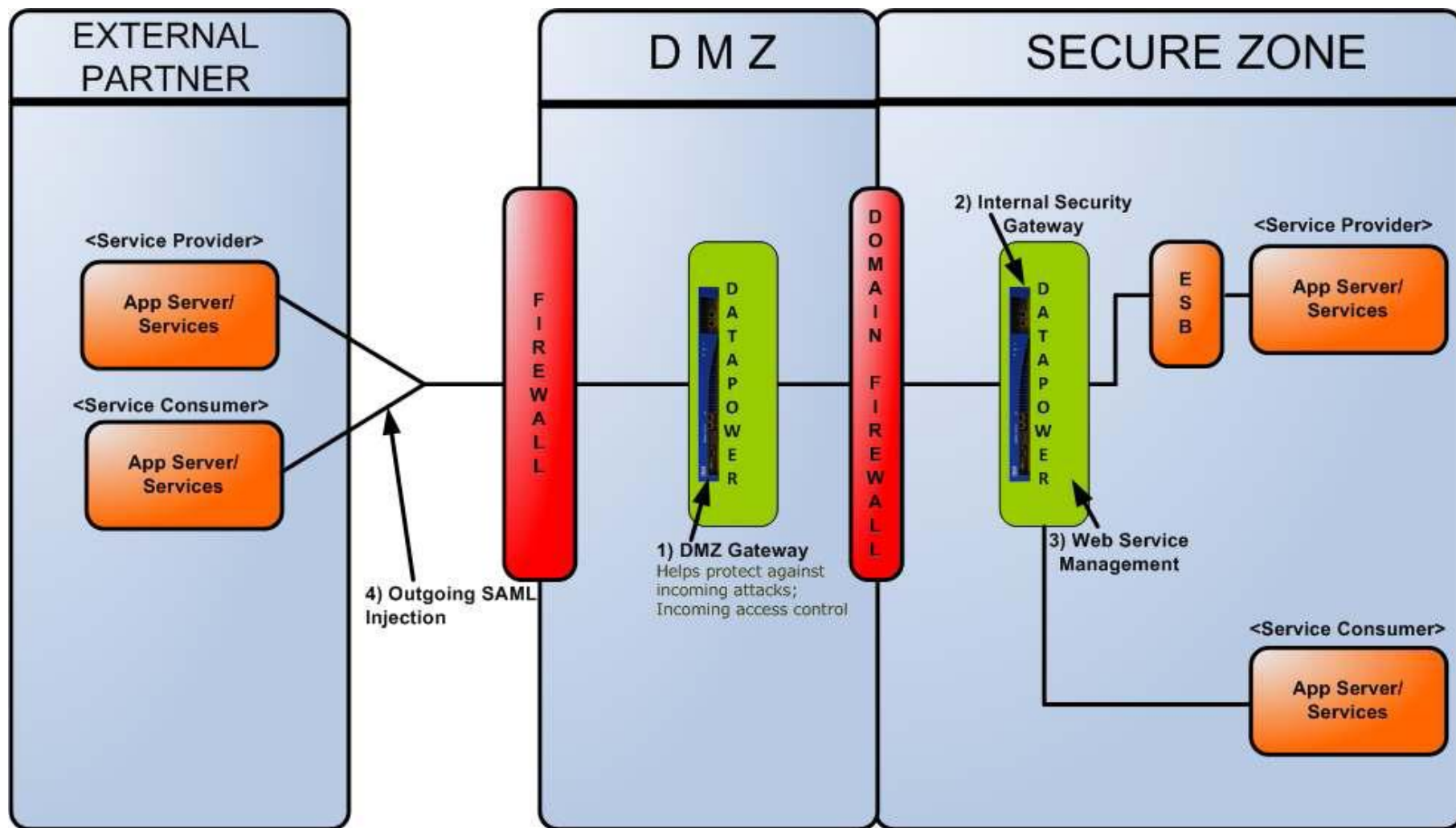
A smarter network is an appliance-based network

Internet

DMZ

Trusted Domain

4 Internal Security

5 Integration Gateway

XG45

XI52

XI52

Application

XB62

XI50B

Application

Consumer

XI50z

System z

1 Secure Gateway
*(Web Services,
Web Applications)*

2 Intelligent Load
Distribution

6 Runtime SOA Governance

3 B2B Partner Gateway

7 Web Service Management

8 Legacy Integration

MIRACLE MSS
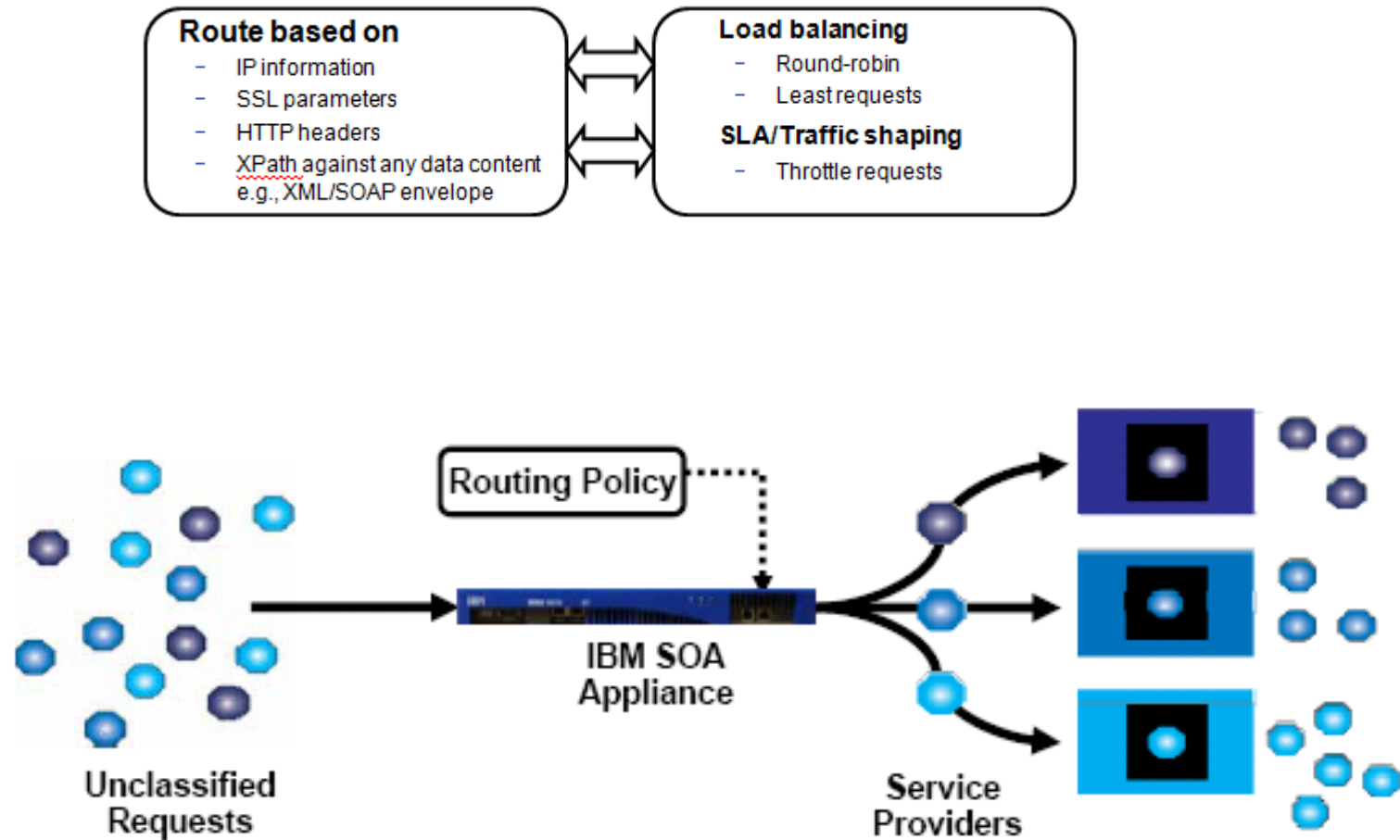SOFTWARE SYSTEMS, INC.

IBM.
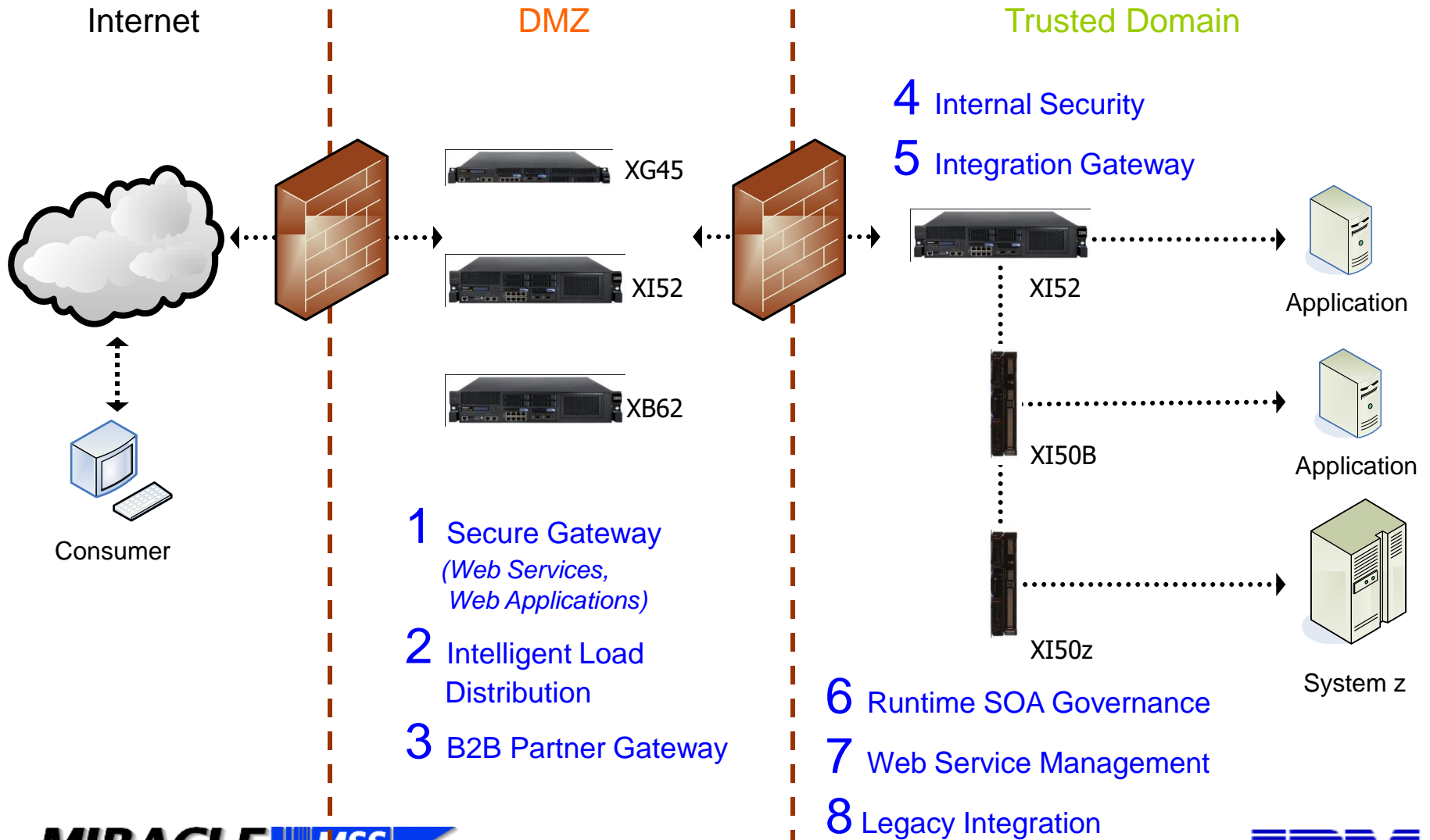
DataPower Core Processing Engine

- Wirespeed XML/XSLT/XPath Processing.

  - Accelerates XML processing, increasing throughput and decreasing latency for XML-based applications by offloading transformation and other resource-intensive functions.

- XML Schema Validation.

  - On all incoming/outgoing XML documents to ensure messages are legitimate and properly express your data's business rules.

- Support for popular XSLT extensions.

  - Some popular elements and functions supported by other engines, metadata extensions for accessing protocol data (e.g. <remove-http-request-header>); regular expressions for string processing; time/date and math functions.

- Customizable XML Caching for:

  - Frequently used XML documents.

  - XSL Style sheets.

  - URLs.

- XML Compression.

  - Standard compression negotiation with remote HTTP peer to reduce XML overhead.

XML 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.
- Access Control
- 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.
- Raw XML and SOAP message inspection (inbound and outbound)
- Well-formed XML validation
- SOAP protocol checks

Content-based Routing

Route based on
- IP information
- SSL parameters
- HTTP headers
- XPath against any data content
  e.g., XML/SOAP envelope

Load balancing
- Round-robin
- Least requests

SLA/Traffic shaping
- Throttle requests

Routing Policy

Unclassified Requests

IBM SOA Appliance

Service Providers

DataPower Services

- **XSL Proxy Service**
  - Used to off-load XSL transformation from general application servers.
  - Accelerates XML processing such as schema validation and XSL transformations

XSL Accelerator

- **XML Firewall Service**
  - Used for a wide variety of XML processing functions.
  - Supports XML encryption, XML signatures, and AAA

XML Firewall

- **Web Service Proxy**
  - Used when a WSDL is involved.
  - Virtualizes and secures back-end Web service applications
  - Provides web services management and monitoring capabilities.
  - Support for WS-Policy, WS-I, etc.

Web Service Proxy

DataPower Services

- **Multi-Protocol Gateway**
  - All the functionality of the XML Firewall.
  - Receives messages from clients using multiple protocols and sends messages to back-end services over many protocols
  - Used when mediating between dissimilar protocols (i.e. MQ and HTTP).

  Multi-Protocol Gateway

- **Web Application Firewall**
  - Used when protecting web applications.
  - Applies constraints on headers, cookies, HTTP methods, etc.

  Web Application Firewall

Use Cases - Right Fit

- **Security Gateway**
  - ❖ Datapower provides secure access to resources when integrating with third parties and integrating internal providers/consumers
  - ❖ Application Level Security and Threat Protection
    - Example – XML Denial-of-Service Protection, WS Security, AAA..

- **Monitoring and Managing**
  - ❖ Security Events log independently using syslogNG
  - ❖ Application transactional logging through enterprise monitoring
  - ❖ Tivoli using SNMP

- **Routing**

  Deep content routing - Content and Context

  Example: XPath (content) routing on Web Service parameters

- **Data Aggregation**
  - ❖ Aggregation and disaggregation: The ability to split or recombine messages

Use Cases - Right Fit continued ..

- ❑ • **Protocol Conversion**

  Service Proxy and Protocol Bridging

  ➢ Inbound Protocol – HTTP/HTTPS/SOAP/MQ/XML/JMS/FTP

  Outbound Protocol - HTTP/HTTPS/MQ/JMS/FTP

- ❑ • **Message Transformation**

  XML-to-XML transformation with XSLT

  HTML/SOAP to XML transformations

  Transformations – Convert WS to MQ

  Content enrichment and filtering

Use Cases - Red Flag

❑ **Long Lived Interactions**

Use Case caused by slowly responding service providers (e.g. human tasks or batch jobs)

Long Lived defined as latency greater than 2 sec

Recommendation – Avoid Long Live Interaction in Datapower

❑ **Large Buffered Payloads**

Use case which required transmission large payloads and

Transformation

Large Payload defined which are larger than 1 G

Recommendation: Use streaming or avoid large message   payloads

❑ **Composition Logic**

Use case which required excessive transformation

Recommendation: Avoid using datapower when application ESB

mediation forms of integration

Use Cases - Red Flag

❑ • **Event Sequencing**

Use case which required events that need to sequence

Recommendation – Avoid event sequencing in Datapower

❑ • **Persistence Requirements**

Use case which required payloads to be persisted when service

provider or service requestor is unavailable

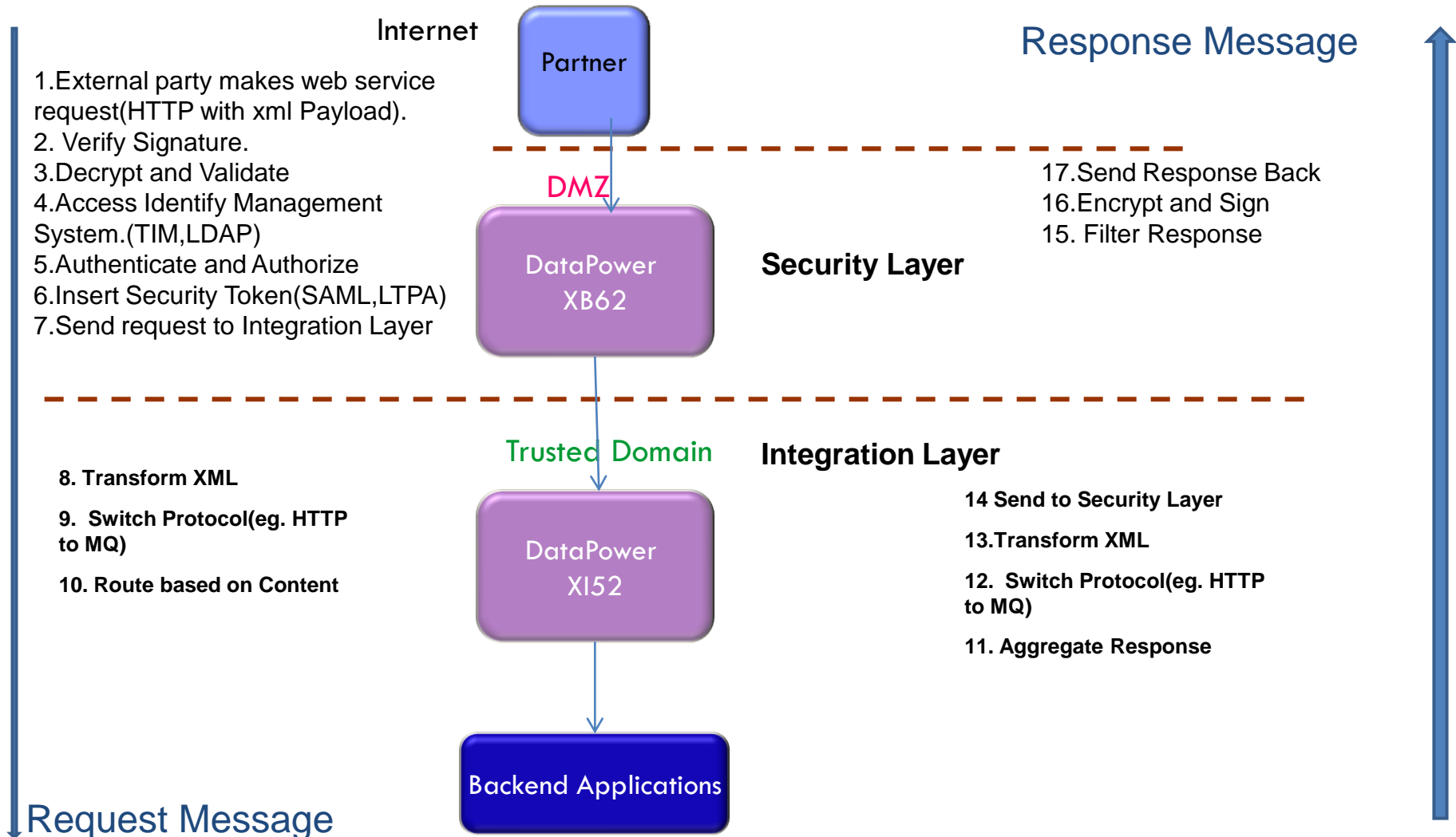Recommendation: Use WMQ if message persistence is required.

❑ • **Transactionality**

Use case which required transaction to be maintained

Recommendation: Datapower does not support transaction

coordination thus avoid any database interaction which need this

features

Datapower As a Security Gateway

Internet

Partner

Response Message

1.External party makes web service request(HTTP with xml Payload).
2. Verify Signature.
3.Decrypt and Validate
4.Access Identify Management System.(TIM,LDAP)
5.Authenticate and Authorize
6.Insert Security Token(SAML,LTPA)
7.Send request to Integration Layer

DMZ

DataPower XB62

Security Layer

17.Send Response Back
16.Encrypt and Sign
15. Filter Response

Trusted Domain

Integration Layer

8. Transform XML

9. Switch Protocol(eg. HTTP to MQ)

10. Route based on Content

DataPower XI52

14 Send to Security Layer

13.Transform XML

12. Switch Protocol(eg. HTTP to MQ)

11. Aggregate Response

Backend Applications

Request Message

MIRACLE MSS
SOFTWARE SYSTEMS, INC.

IBM

DataPower Service Governance Solutions

DataPower (XI52 and XB62) uses WSSR/UDDI subscriptions to retrieve the service WSDL/XSDs to build a web service proxy object.

SOAP/XML messages will be validated using validate action in the processing rule by retrieving the WSDL/XSD from WSRR/UDDI subscription in both web service proxy objects as well multi-protocol objects.

IBM Tivoli Composite Application Manager for SOA v6.1 includes a DataPower data collector that monitors Web services flows through a DataPower SOA appliance.
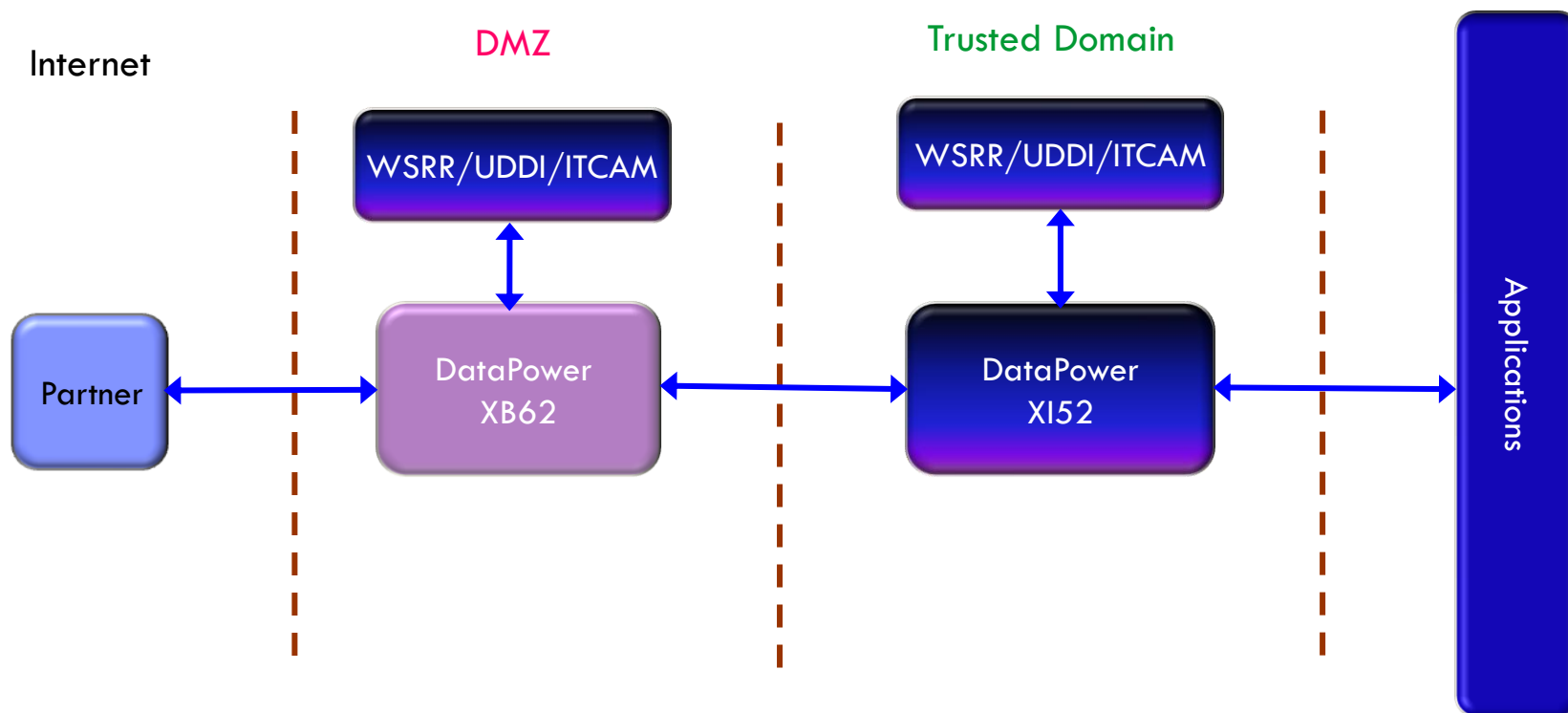
DataPower SLM

DataPower appliance allows elegant ways of implementing service level monitoring (SLM) as all messages entering and leaving the network may be monitored.

The SLM capabilities in the DataPower appliance offer the following benefits:

- **Avoid abuse and overuse of services and secure services from Denial of Service (DoS) attacks.**

- **Enforce service level agreements (SLAs).**

- **Differentiate between users with different needs for service quality.**

- **Define actions to be taken if thresholds for indicators are reached, such as sending notifications if there is a bad response time or too many error messages from the back end.**

Thank You